

payShield® 10K

Core Host Commands

007-001515-020



Date: April 2024

Rev: A

Doc. Number: 007-001515-020

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Copyright © 2018-2024 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Follow this link to find the End User Licensing Agreement: <https://cpl.thalesgroup.com/legal>

Contents

1 General	14
1.1 Local Master Keys (LMKs).....	14
1.2 Multiple LMKs.....	14
1.3 LMK Usage in Host Commands	15
2 Introduction.....	16
2.1 List of Host Commands (Alphabetical).....	17
2.2 List of Host Commands (Functional).....	25
2.3 General.....	35
3 Key Management Commands	36
3.1 Generic Key Management Commands	36
<i>Available Key Types/Usages</i>	<i>37</i>
<i>Interpretation of TR-31 Key Block Version ID Field</i>	<i>38</i>
<i>Generate a Key.....</i>	<i>39</i>
<i>Generate & Export a Key.....</i>	<i>42</i>
<i>Derive a Key.....</i>	<i>48</i>
<i>Derive & Export a Key.....</i>	<i>57</i>
<i>Generate and Print a Component</i>	<i>66</i>
<i>Generate and Print a Key as Split Components</i>	<i>70</i>
<i>Form a Key from Encrypted Components</i>	<i>73</i>
<i>Import a Key</i>	<i>75</i>
<i>Import a Key encrypted under a KTK</i>	<i>79</i>
<i>Export a Key</i>	<i>82</i>
<i>Translate Key Scheme.....</i>	<i>88</i>
<i>Translate ZMK from ZMK to LMK encryption</i>	<i>89</i>
3.2 LMK Translation Commands.....	92
<i>Translate a PIN and PIN Length</i>	<i>93</i>
<i>Translate Keys from Old LMK to New LMK and Migrate to New Key Type</i>	<i>94</i>
<i>Erase the Key Change Storage</i>	<i>98</i>
3.3 EMV Key Management Commands	99
<i>Derive Card Unique DES Keys</i>	<i>100</i>
<i>Export a Key under a KEK</i>	<i>106</i>
<i>Import an RSA Private Key</i>	<i>109</i>
<i>Export an RSA Private Key.....</i>	<i>113</i>
<i>Generate Digitized Card Single Use Keys.....</i>	<i>116</i>
<i>Generate Digitized Card Single Use Keys (Mode Flag '0': MCBP SUK Derivation; include PIN; output in legacy JSON format.)</i>	<i>117</i>

Generate Digitized Card Single Use Keys (Mode Flag '1': MCBP SUK Derivation; include PIN; output in MC SDK JSON format)	121
Generate Digitized Card Single Use Keys (Mode Flag '2': VCP LUK from Card Key).....	125
Generate Digitized Card Single Use Keys (Mode Flag '3': MCBP SK from MDES; add PIN; output encrypted SUK under KEK).....	127
Generate Digitized Card Single Use Keys (Mode Flag '4': MCBP SUK Derivation; output encrypted under KEK).....	129
Generate Digitized Card Single Use Keys (Mode Flag '5': LUK from Card Key with PIN).....	133
Generate Remote Management Session ID and Session Keys	135
3.4 Mastercard Key Management (OBKM) Commands.....	137
Generate an Issuer RSA Key Set.....	138
Validate a CA Self-Signed Certificate.....	140
Import Transport Key Set.....	141
Export Magnetic Stripe Card Key Set.....	143
Export Chip Card Key Set (2002 & 2003 Version).....	145
Export Chip Card Key Set (2007 Version).....	149
3.5 AS2805 Key Management Commands.....	153
Generate a Set of Zone Keys.....	154
Translate a Set of Zone Keys to Encryption under the LMK.....	156
Generate Initial Terminal Master Keys (AS2805 – 2001)	159
Update Terminal Master Key 1	161
Update Terminal Master Keys.....	163
Generate a Set of Terminal Keys.....	165
Generate an Acquirer Master Key Encrypting Key.....	168
Translate an Acquirer Master Key Encrypting Key.....	170
KEKGEN – 6.3.....	172
KEKREC – 6.3.....	174
Generate a KCA and KMACH.....	176
Generate a KEKs for use in Node to Node interchange using RSA.....	178
Receive a KEKr for use in Node to Node interchange using RSA	180
Decrypt a PIN Pad Public Key	182
Encrypt a Cross Acquirer Key Encrypting Key under an Initial Transport Key	184
Encrypt a Terminal Key under the LMK	186
3.6 Asymmetric Key Management Commands	188
Generate an RSA Public/Private Key Pair.....	189
Generate an ECC Public/Private Key Pair	193
Load a Private Key	195
Translate a Private Key.....	196
Import a Public Key.....	198
Validate a Public Key.....	201

Validate a Certificate and Import the Public Key	202
Translate a Public Key	205
Import Key or data under an RSA Public Key	207
Export Key under an RSA Public Key	214
Generate a Certificate Request.....	219
Key Derivation using Elliptic Curve Key Agreement	222
ECKA-EG Example.....	223
ECKA-DH Example.....	224
Key Derivation using ECKA-EG (Initiator: Derive Shared Secret)	225
Key Derivation using ECKA-EG (Recipient: Derive Shared Secret/Keys).....	227
Key Derivation using ECKA-EG/DH (Derive Shared Keys)	231
Key Derivation using ECKA-DH (Initiator: Create Ephemeral Keys).....	234
Key Derivation using ECKA-DH (Recipient: Derive Shared Secret/Keys).....	236
Key Derivation using ECKA-DH (Initiator: Derive Shared Keys).....	240
TR-34 Key Export	244
3.7 Bancontact Session Key Commands	249
Import Bancontact Session Key	251
Export Bancontact Session Key.....	256
4 Magnetic Stripe Issuing Commands.....	259
4.1 PIN and Offset Generation Commands.....	259
Derive a PIN and Optionally Generate Offset for New PVK Using the IBM Offset Method	260
Derive a PIN Using the Diebold Method.....	263
Generate a Random PIN	265
Generate an IBM PIN Offset (of an LMK encrypted PIN)	267
Generate an IBM PIN Offset (of a customer selected PIN).....	270
Generate a Diebold PIN Offset	273
Generate an ABA PVV (of an LMK encrypted PIN).....	275
Generate an ABA PVV (of a customer selected PIN).....	277
Load the Excluded PIN Table	280
4.2 PIN Mailer Printing Commands	281
Print PIN/PIN and Solicitation Data	282
Print a PIN Solicitation Mailer.....	284
Verify PIN/PIN and Solicitation Mailer Cryptography	286
Verify Solicitation Mailer Cryptography	287
4.3 PIN Solicitation Data Processing Commands	288
Load Solicitation Data to User Storage	289
Final Load of Solicitation Data to User Storage.....	290
4.4 Print Output Formatting Commands.....	292

<i>Load Formatting Data to HSM</i>	293
<i>Load Additional Formatting Data to HSM</i>	294
<i>Load a PIN Text String</i>	295
4.5 Clear PIN Commands	296
<i>Encrypt a Clear PIN</i>	297
<i>Decrypt an Encrypted PIN</i>	298
4.6 Card Verification Code/Value Generation Commands	299
<i>Generate a Card Verification Code/Value</i>	300
<i>Calculate Card Security Codes</i>	302
5 Magnetic Stripe Transaction Processing	304
5.1 PIN Change Commands	304
<i>Verify a PIN & Generate an IBM PIN Offset (of customer selected new PIN)</i>	305
<i>Verify a PIN & Generate an ABA PVV (of a customer selected PIN)</i>	309
5.2 PIN Verification Commands	312
<i>Verify a Terminal PIN Using the IBM Offset Method</i>	313
<i>Verify an Interchange PIN Using the IBM Offset Method</i>	316
<i>Verify a Terminal PIN Using the Diebold Method</i>	319
<i>Verify an Interchange PIN Using the Diebold Method</i>	321
<i>Verify a Terminal PIN Using the ABA PVV Method</i>	323
<i>Verify an Interchange PIN Using the ABA PVV Method</i>	325
<i>Verify a Terminal PIN Using the Comparison Method</i>	327
<i>Verify an Interchange PIN Using the Comparison Method</i>	329
5.3 PIN Translation Commands	331
<i>Translate a PIN from One ZPK to Another</i>	332
<i>Translate a PIN from TPK to ZPK/BDK Encryption (3DES DUKPT)</i>	335
<i>Translate a PIN from ZPK to LMK Encryption</i>	339
<i>Translate a PIN from TPK to LMK Encryption</i>	341
<i>Translate a PIN from LMK to ZPK Encryption</i>	343
<i>Translate PIN Algorithm</i>	345
<i>Translate Account Number for LMK-encrypted PIN</i>	346
<i>Translate an RSA-encrypted PIN to a ZPK or TPK-encrypted PIN</i>	348
<i>Load OPINPad to HSM Memory</i>	351
<i>Decode OPIN and translate to ZPK</i>	352
5.4 Card Verification Code/Value Commands	354
<i>Verify a Card Verification Code/Value</i>	355
<i>Generate a Dynamic CVV</i>	358
<i>Verify a Dynamic CVV/CVC</i>	360
<i>Verify Card Security Codes</i>	368

5.5 Racial Transaction Key Scheme (RTKS) Commands	370
<i>Transaction Request With a PIN (T/AQ Key) (when selected Transaction Key Scheme is Racial)</i>	371
<i>Transaction Request With a PIN (T/AQ Key) (when selected Transaction Key Scheme is Australian)</i>	373
<i>Transaction Request Without a PIN (when selected Transaction Key Scheme is Racial)</i>	374
<i>Transaction Request Without a PIN (when selected Transaction Key Scheme is Australian)</i> ..	376
<i>Transaction Request With a PIN (T/CI Key) (when selected Transaction Key Scheme is Racial)</i>	377
<i>Transaction Request With a PIN (T/CI Key) (when selected Transaction Key Scheme is Australian)</i>	379
<i>Translate KEYVAL (when selected Transaction Key Scheme is Racial)</i>	380
<i>Translate KEYVAL (when selected Transaction Key Scheme is Australian)</i>	382
<i>Administration Request Message (when selected Transaction Key Scheme is Racial)</i>	383
<i>Administration Request Message (when selected Transaction Key Scheme is Australian)</i>	385
<i>Transaction Response with Auth Para from Card Issuer (when selected Transaction Key Scheme is Racial)</i>	386
<i>Transaction Response with Auth Para from Card Issuer (when selected Transaction Key Scheme is Australian)</i>	388
<i>Generate Auth Para and Transaction Response (when selected Transaction Key Scheme is Racial)</i>	389
<i>Generate Auth Para and Transaction Response (when selected Transaction Key Scheme is Australian)</i>	391
<i>Confirmation (when selected Transaction Key Scheme is Racial)</i>	392
<i>Confirmation (when selected Transaction Key Scheme is Australian)</i>	394
5.6 DUKPT (X9.24) Transaction Processing Commands	395
<i>BDKs used with PIN encryption & MACing Commands</i>	396
<i>Translate a PIN from BDK to BDK or ZPK Encryption (3DES & AES DUKPT)</i>	398
<i>Verify a PIN Using the IBM Offset Method (3DES & AES DUKPT)</i>	402
<i>Verify a PIN Using the ABA PVV Method (3DES & AES DUKPT)</i>	406
<i>Verify a PIN Using the Diebold Method (3DES & AES DUKPT)</i>	410
<i>Verify a PIN Using the Encrypted PIN Method (3DES & AES DUKPT)</i>	413
<i>Generate/Verify a MAC (3DES & AES DUKPT)</i>	416
6 Data Protection Commands	419
6.1 Message Integrity Commands.....	419
<i>Generate MAC</i>	420
<i>Verify MAC</i>	423
<i>Verify and Translate MAC</i>	426
<i>Generate an RSA/ECC Signature</i>	430
<i>Validate an RSA/ECC Signature</i>	433
<i>Hash a Block of Data</i>	435

6.2 Message Encryption Commands	436
<i>Encrypt Data Block</i>	439
<i>Decrypt Data Block</i>	446
<i>Translate Data Block.....</i>	452
7 User Authentication Commands.....	459
7.1 HMAC Commands.....	459
<i>Generate an HMAC Secret Key</i>	460
<i>Generate an HMAC on a Block of Data</i>	463
<i>Verify an HMAC on a Block of Data</i>	465
<i>Import an HMAC key under a ZMK.....</i>	467
<i>Export an HMAC key under a ZMK.....</i>	471
<i>Translate a HMAC Key from Old LMK to New LMK</i>	474
7.2 WebPIN Commands	476
<i>Generate a Random Alphanumeric PIN.....</i>	477
<i>Print Alphanumeric PIN/Alphanumeric PIN and Solicitation Data</i>	478
<i>Translate Encrypted PIN to Encrypted Alphanumeric PIN.....</i>	480
<i>Translate an Alphanumeric PIN from old LMK to new LMK Encryption</i>	482
<i>Verify Alphanumeric PIN Block from Internet, return new encrypted PIN & Verify MAC</i>	483
8 HSM Management Commands	485
8.1 User Storage Commands.....	485
<i>Load Data to User Storage</i>	486
<i>Read Data from User Storage.....</i>	488
<i>Verify the Diebold Table in User Storage</i>	490
8.2 Miscellaneous Commands	491
<i>Echo Command.....</i>	492
<i>Cancel Authorized Activities.....</i>	493
<i>Generate a Key Check Value.....</i>	495
<i>Set HSM Response Delay</i>	498
<i>Translate Decimalization Table from Old to New LMK</i>	499
<i>Command Chaining</i>	500
<i>Modify Key Block Header.....</i>	502
<i>Generate a Random Value</i>	504
8.3 Diagnostic Commands	505
<i>Perform Diagnostics</i>	506
<i>HSM Status</i>	507
<i>Return Network Information</i>	509
<i>Get HSM Loading</i>	512
<i>Get Host Command Volumes</i>	513

Reset Utilization Statistics.....	514
Get Health Check Accumulated Counts.....	515
Reset Health Check Accumulated Counts	517
Get Instantaneous Health Check Status	518
8.4 Auditing Commands	521
Translate Audit Record MAC key.....	522
Retrieve Audit Record.....	523
Archive (Print) Audit Record.....	524
Delete Audit Record.....	525
Audit Record Verification	526
9 EMV Transaction Processing Commands.....	527
9.1 EMV Chip Card Commands	527
Key Naming Conventions	527
ARQC Verification and/or ARPC Generation (Using Static or Mastercard Proprietary SKD Method)	528
ARQC Verification and/or ARPC Generation (Using EMV or Cloud-Based SKD Methods)	533
Generate Secure Message (EMV 3.1.1)	537
Generate Secure Message (EMV 4.x)	542
Verify Truncated Application Cryptogram (Mastercard CAP).....	547
Data Authentication Code and Dynamic Number Verification (EMV 3.1.1).....	550
Decrypt Encrypted Counters (EMV 4.x)	552
10 EMV Chip, Contactless & Mobile Issuing	554
10.1 Contactless Cards Data Preparation Commands	554
Generate IVCVC3 and Static CVC3.....	555
10.2 EMV-based Cards Data Preparation Commands	557
Generate Issuer RSA Key Set and Public Key Certificate	558
Validate an Issuer Public Key Certificate.....	561
Generate Static Data Authentication Signature	564
Generate Card RSA Key Set and Public Key Certificate	566
Import a Certification Authority Self-Signed Certificate.....	571
EMV Sign Data	574
EMV Recover Data	576
10.3 MULTOS Card Data Preparation Commands	578
Import MULTOS Transport Key Certifying Key.....	579
Import MULTOS Hash Modulus Key.....	580
Translate MULTOS KTU.....	581
MULTOS ALU Generator – Allocate ALU Area	585
MULTOS ALU Generator – Load Block	586

MULTOS ALU Generator – Load Clear Data	587
MULTOS ALU Generator – Load Cipher Data	589
MULTOS ALU Generator – Generate Checksum.....	592
MULTOS ALU Generator – Encrypt Area.....	594
MULTOS ALU Generator – Generate Signature	596
MULTOS ALU Generator – Generate KTU.....	598
MULTOS ALU Generator – Return ALU.....	600
MULTOS ALU Generator – Release ALU.....	601
10.4 Chip Card Personalization Commands.....	602
<i>Establish Secure Session with Chip Card</i>	603
<i>Prepare Secure Message for Chip Card</i>	610
<i>Verify and Decrypt Response Secure Message from Chip Card</i>	617
10.5 Mobile Device Provisioning Commands.....	619
<i>Validate Authentication Code.....</i>	620
<i>Generate Remote Management Secure Message</i>	621
<i>Validate and Recover Remote Management Secure Message from the MPA</i>	627
10.6 JSON Web Token (JWT) Commands	630
<i>JWT Encode</i>	631
<i>JWT Decode</i>	635
11 AS2805 Transaction Processing.....	638
11.1 AS2805 Commands.....	638
<i>Generate a PIN Pad Acquirer Security Number</i>	640
<i>Translate a PIN Block to Encryption under a Zone PIN Key.....</i>	642
<i>Generate a Message Authentication Code AS2805.4 – 1985</i>	644
<i>Generate a Message Authentication Code (large messages)</i>	646
<i>Validate a Message Authentication Code AS2805.4 -1985</i>	648
<i>Verify a Message Authentication Code (large messages)</i>	650
<i>Encrypt Data</i>	652
<i>Decrypt Data</i>	654
<i>Translate a PIN Block to Encryption under a PIN Encryption Key</i>	656
<i>Generate a KEKs Validation Request</i>	658
<i>Generate a KEKr Validation Response</i>	660
<i>Verify a PIN Pad Proof of End Point</i>	662
<i>Verify a Terminal PIN using the IBM Method (AS2805 6.4).....</i>	664
<i>Verify a Terminal PIN using the VISA Method (AS2805 6.4).....</i>	666
<i>Calculate KMACI</i>	668
<i>Generate a Random Number.....</i>	670
<i>Generate a PIN Pad Authentication Code</i>	671

Encrypt a CPAT Authentication Value.....	672
Verify a PIN Pad Authentication Code	673
Generate a PIN Pad Proof of Endpoint (POEP)	674
Translate a PPASN from old to new LMK	675
Verify and Generate an IBM PIN Offset (of a customer selected PIN).....	676
Verify and Generate a VISA PVV (of a customer selected PIN).....	679
Generate a VISA PVV (of a customer selected PIN).....	682
Generate a Proof of Host value.....	685
Calculate a RSA Public Key Verification Code.....	686
11.2 AS2805.6.2 Support.....	687
Verify a Transaction Request, without PIN.....	692
Verify a Transaction Request, with PIN, when CD Field Available	694
Verify a Transaction Request, with PIN, when CD Field not Available (when selected Transaction Key Scheme is Australian)	696
Verify a Transaction Request, with PIN, when CD Field not Available (when selected Transaction Key Scheme is Racal)	698
Generate Transaction Response, with Auth Para Generated by Acquirer (when selected Transaction Key Scheme is Australian)	699
Generate Transaction Response, with Auth Para Generated by Acquirer (when selected Transaction Key Scheme is Racal)	701
Generate Transaction Response with Auth Para Generated by Card Issuer (when selected Transaction Key Scheme is Australian)	702
Generate Transaction Response with Auth Para Generated by Card Issuer (when selected Transaction Key Scheme is Racal)	704
Translate a PIN from PEK to ZPK Encryption (when selected Transaction Key Scheme is Australian)	705
Translate a PIN from PEK to ZPK Encryption (when selected Transaction Key Scheme is Racal)	707
Verify a Transaction Completion Confirmation (when selected Transaction Key Scheme is Australian)	708
Verify a Transaction Completion Confirmation (when selected Transaction Key Scheme is Racal)	710
Generate a Transaction Completion Response (when selected Transaction Key Scheme is Australian)	711
Generate a Transaction Completion Response (when selected Transaction Key Scheme is Racal)	713
Verify a PIN at Card Issuer using IBM Method	714
Verify a PIN at Card Issuer using the Diebold Method	716
Verify a PIN at Card Issuer using Visa Method	718
Verify a PIN at Card Issuer using the Comparison Method	720
Generate Auth Para at the Card Issuer (when selected Transaction Key Scheme is Australian)	722
Generate Auth Para at the Card Issuer (when selected Transaction Key Scheme is Racal) ...	724

Generate an Initial Terminal Key (when selected Transaction Key Scheme is Australian)	725
Generate an Initial Terminal Key (when selected Transaction Key Scheme is Racal)	726
Data Encryption Using a Derived Privacy Key.....	727
Data Decryption Using a Derived Privacy Key	729
12 Error Codes	731
13 Card Issuing Appendices	734
Card Issuing Appendix A – Self-Signed Issuer Public Key Certificate Format (Visa)	735
Card Issuing Appendix B – Self-Signed Issuer Public Key Certificate Format (Mastercard)	737
Card Issuing Appendix C – Self-Signed Issuer Public Key Certificate Format (American Express).....	739
Card Issuing Appendix D – Issuer Public Key Certificate Format (Visa).....	741
Card Issuing Appendix E – Issuer Public Key Certificate Format (Mastercard)	744
Card Issuing Appendix F – Issuer Public Key Certificate Format (American Express).....	746
Card Issuing Appendix G – Format of Card (ICC) Public Key Certificate.....	749
Card Issuing Appendix H – Private Key Encodings.....	751
Card Issuing Appendix I – MULTOS Card Public Key Certificate Format	755
Card Issuing Appendix J – MULTOS Transport Key Certifying Key File Format	758
Card Issuing Appendix K – MULTOS Hash Modulus File Format.....	759
Card Issuing Appendix L – Self Signed CA Public Key Certificate Format (Visa)	760
Card Issuing Appendix M – Self Signed CA Public Key Certificate Format (Mastercard) ...	762
Card Issuing Appendix N - Self Signed CA Public Key Certificate Format (American Express).....	764
Card Issuing Appendix O – DC_SUK block template.....	766
14 AS2805 Appendices	767
AS2805 Appendix A – One-Way Functions	767
OWF - 1988.....	767
OWF - 2000.....	767
AS2805 Appendix B – Derivation of the Privacy Key	768
AS2805 Appendix C – Key Check Value	769
Single Length Key.....	769
Double Length Key	769
AS2805 Appendix D – Key Encrypting Key Variants	770
Zone or Terminal Authentication keys.....	770
Zone or Terminal Encryption keys.....	771
Zone or Terminal PIN keys	772
AS2805 Appendix G – Definition of Card Values	773
AS2805 Appendix H – Generation of Initial Terminal Master Keys	774
AS2805 Appendix I – Terminal Master Key Update.....	775

AS2805 – 1988 Method	775
AS2805 – 2001 Method	775
AS2805 Appendix J – Derivation of the PIN Encryption Key.....	778
Single Length TPK.....	778
Double Length TPK	778
PIN enciphering key (KPE)	779
AS2805 Appendix K – AS2805.3 PIN block formats.....	780
AS2805 Format 1 PIN block.....	780
AS2805.3 Format 8 PIN block (format 46)	780
AS2805 Appendix L – Error messages	781
AS2805 Appendix M – Australian Key Schemes	783
AS2805 Appendix N – AS 2805.6.2 Support Appendices	786
AS2805 Appendix N – A: One-way Function.....	786
AS2805 Appendix N – B: Derivation of Data Values	787
AS2805 Appendix N – C: MAC Key Derivation	788
AS2805 Appendix N – D: PIN Encipherment Key Derivation.....	789
AS2805 Appendix N – E: Privacy Key Derivation.....	790
AS2805 Appendix N – F: Terminal Key Update (AS2805.6.2).....	791
AS2805 Appendix N – G: MAC and MAC Residue Calculation	792
AS2805 Appendix N – H: Authentication Parameter	793
AS2805 Appendix O – AS 2805.6.2 (Single DES) Support Appendices	794
AS2805 Appendix O – A: One-way Function	794
AS2805 Appendix O – B: Derivation of Card and Data Values.....	795
AS2805 Appendix O – C: MAC Key Derivation	796
AS2805 Appendix O – D: PIN Encipherment Key Derivation	797
AS2805 Appendix O – E: Terminal Key Update	797
AS2805 Appendix O – F: MAC and MAC Residue Calculation	798
AS2805 Appendix O – G: Card Key and Authentication Parameter	798
AS2805 Appendix S – APCA Functional Specification Comparison Guide	799
AS2805 Appendix T – Key Notation comparison table	802
AS2805 Appendix U – RSA Public Key Encoding	803
AS2805 Appendix U1 – DEA 2 Text Block - DFormat 1	803
AS2805 Appendix U2 – Public Key Encoding	804
AS2805 Appendix V – Plaintext Data Block Formats	805

1 General

1.1 Local Master Keys (LMKs)

For an introduction to LMKs (Local Master Keys) and information about LMKs, see the *payShield 10K Host Programmer's manual*. The *payShield 10K Host Programmer's manual* also documents changes made to key types for PCI HSM certification.

1.2 Multiple LMKs

It is possible to install multiple LMKs within a single payShield 10K. The precise details of the number and type of installed LMKs are controlled via the payShield 10K's license file:

License	Description
All packages	Two concurrent LMKs can be installed; however, one must be a Variant LMK, and the other a Key Block LMK.
PS10-LIC-LMKx2 (optional license)	Two concurrent LMKs can be installed; they can be any combination of Variant and Key Block LMKs.
PS10-LIC-LMKx5 (optional license)	Five concurrent LMKs can be installed; they can be any combination of Variant and Key Block LMKs.
PS10-LIC-LMKx10 (optional license)	Ten concurrent LMKs can be installed; they can be any combination of Variant and Key Block LMKs.
PS10-LIC-LMKx20 (optional license)	Twenty concurrent LMKs can be installed; they can be any combination of Variant and Key Block LMKs.

The basic mechanism for host commands to support multiple LMKs and LMK schemes is as follows:

Two additional (optional) fields are added to the end of each host command request message. These fields are:

Field	Length & Type	Details
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.

An additional mechanism has been introduced for Ethernet-attached host computers. The HSM can infer the LMK Identifier to use for a particular command from the TCP port on which the command is received. Historically, host commands sent via TCP/IP have been directed to the HSM's Well-Known Port, and this continues to be supported. However, host commands directed to [the Well-Known Port

+1] will automatically use LMK Id 00; host commands directed to [the Well-Known Port +2] will automatically use LMK Id 01; etc. The situation for an HSM using the default Well-Known Port value of 1500 is summarized in the table below:

Command received on TCP Port	LMK Used
1500	Default LMK Id (or %nn construct)
1501	LMK Id 00
1502	LMK Id 01
1503	LMK Id 02
...	...

1.3 LMK Usage in Host Commands

There are a total of five mechanisms that the HSM uses to determine which LMK Id to use with a host command.

The Management LMK is automatically used for command processing and the Delimiter and LMK Identifier fields should not be included in the command message. The only commands that belong in this category are the "Q0", "Q2", "Q4" and "Q8" commands.

For commands that use keyblocks, then the LMK that is identified in the key block header(s) will be used; if the Delimiter and LMK Identifier are present in the command message then all LMK identifiers must be in agreement.

If the Delimiter and LMK Identifier are present at the end of the command message, then the specified LMK will be used in the command processing.

For commands received via the Ethernet host port using TCP/IP, the HSM will infer the LMK Id to use based on the specific TCP port on which the command was received.

For all other commands where the Delimiter and LMK Identifier are not present in the command message then the Default LMK will be used in the command processing. This provides a backwards-compatible mode for the HSM.

2 Introduction

The payShield 10K provides a variety of functions to implement cryptographic functions to secure payment transactions.

This manual describes the primary set of payShield 10K commands, known as *core commands*. The payShield 10K provides other commands, known as *legacy commands*, which are described in the *payShield 10K Legacy Commands* manual.

The remainder of this manual describes the core commands, and is divided into the following groupings:

- Key Management Commands
- Magnetic Stripe Issuing Commands
- Magnetic Stripe Transaction Processing
- Data Protection Commands
- User Authentication Commands
- HSM Management Commands
- EMV Transaction Processing Commands
- EMV Chip, Contactless & Mobile Issuing
- AS2805 Transaction Processing

2.1 List of Host Commands (Alphabetical)

Command (Response)	Function	Page
A0 (A1)	<i>Generate a Key</i>	39
A0 (A1)	<i>Generate & Export a Key</i>	42
A0 (A1)	<i>Derive a Key</i>	48
A0 (A1)	<i>Derive & Export a Key</i>	57
A2 (A3, AZ)	<i>Generate and Print a Component</i>	66
A4 (A5)	<i>Form a Key from Encrypted Components</i>	72
A6 (A7)	<i>Import a Key</i>	75
A8 (A9)	<i>Export a Key</i>	82
AQ (AR)	<i>Translate an RSA-encrypted PIN to a ZPK or TPK-encrypted PIN</i>	348
B0 (B1)	<i>Translate Key Scheme</i>	87
B2 (B3)	<i>Echo Command</i>	492
B8 (B9)	<i>TR-34 Key Export</i>	244
BA (BB)	<i>Encrypt a Clear PIN</i>	297
BC (BD)	<i>Verify a Terminal PIN Using the Comparison Method</i>	327
BE (BF)	<i>Verify an Interchange PIN Using the Comparison Method</i>	329
BG (BH)	<i>Translate a PIN and PIN Length</i>	93
BK (BL)	<i>Generate an IBM PIN Offset (of a customer selected PIN)</i>	270
BM (BN)	<i>Load the Excluded PIN Table</i>	280
BQ (BR)	<i>Translate PIN Algorithm</i>	345
BS (BT)	<i>Erase the Key Change Storage</i>	98
BU (BV)	<i>Generate a Key Check Value</i>	495
BW (BX)	<i>Translate Keys from Old LMK to New LMK and Migrate to New Key Type</i>	94
BY (BZ)	<i>Translate ZMK from ZMK to LMK encryption</i>	88
C0 (C1)	<i>Generate Initial Terminal Master Keys (AS2805 – 2001)</i>	159
C2 (C3)	<i>Generate a Message Authentication Code (large messages)</i>	646
C4 (C5)	<i>Verify a Message Authentication Code (large messages)</i>	650
C6 (C7)	<i>Generate a Random Number</i>	670
C8 (C9)	<i>Generate an Acquirer Master Key Encrypting Key</i>	168
CA (CB)	<i>Translate a PIN from TPK to ZPK/BDK Encryption (3DES DUKPT)</i>	335
CC (CD)	<i>Translate a PIN from One ZPK to Another</i>	332
CE (CF)	<i>Generate a Diebold PIN Offset</i>	273
CG (CH)	<i>Verify a Terminal PIN Using the Diebold Method</i>	319
CS (CT)	<i>Modify Key Block Header</i>	502
CU (CV)	<i>Verify a PIN & Generate an ABA PVV (of a customer selected PIN)</i>	309

Command (Response)	Function	Page
CW (CX)	Generate a Card Verification Code/Value	300
CY (CZ)	Verify a Card Verification Code/Value	355
D0 (D1)	Generate a PIN Pad Authentication Code	671
D2 (D3)	Verify a PIN Pad Authentication Code	673
D4 (D5)	Translate a PIN Block to Encryption under a PIN Encryption Key	656
D6 (D7)	Translate an Acquirer Master Key Encrypting Key	170
D8 (D9)	Encrypt a CPAT Authentication Value	672
DA (DB)	Verify a Terminal PIN Using the IBM Offset Method	313
DC (DD)	Verify a Terminal PIN Using the ABA PVV Method	322
DE (DF)	Generate an IBM PIN Offset (of an LMK encrypted PIN)	267
DG (DH)	Generate an ABA PVV (of an LMK encrypted PIN)	275
DU (DV)	Verify a PIN & Generate an IBM PIN Offset (of customer selected new PIN)	305
E0 (E1)	Generate a KEKs Validation Request	658
E2 (E3)	Generate a KEKr Validation Response	660
E4 (E5)	Verify a PIN Pad Proof of End Point	662
E6 (E7)	Generate a PIN Pad Proof of Endpoint (POEP)	674
E8 (E9)	Generate a KCA and KMACH	176
EA (EB)	Verify an Interchange PIN Using the IBM Offset Method	316
EC (ED)	Verify an Interchange PIN Using the ABA PVV Method	325
EE (EF)	Derive a PIN and Optionally Generate Offset for New PVK Using the IBM Offset Method	260
EG (EH)	Verify an Interchange PIN Using the Diebold Method	321
EI (EJ)	Generate an RSA Public/Private Key Pair	188
EK (EL)	Load a Private Key	195
EM (EN)	Translate a Private Key	196
EO (EP)	Import a Public Key	197
EQ (ER)	Validate a Public Key	201
ES (ET)	Validate a Certificate and Import the Public Key	202
EU (EV)	Translate a Public Key	205
EW (EX)	Generate an RSA/ECC Signature	430
EY (EZ)	Validate an RSA/ECC Signature	433
F0 (F1)	Verify a Terminal PIN using the IBM Method (AS2805 6.4)	664
F2 (F3)	Verify a Terminal PIN using the VISA Method (AS2805 6.4)	666
F4 (F5)	Calculate KMACI	668
F6 (F7)	KEKGEN – 6.3	172

Command (Response)	Function	Page
F8 (F9)	<i>KEKREC – 6.3</i>	174
FW (FX)	<i>Generate an ABA PVV (of a customer selected PIN)</i>	277
FY (FZ)	<i>Generate an ECC Public/Private Key Pair</i>	193
G0 (G1)	<i>Translate a PIN from BDK to BDK or ZPK Encryption (3DES & AES DUKPT)</i>	398
GA (GB)	<i>Derive a PIN Using the Diebold Method</i>	263
GI (GJ)	<i>Import Key or data under an RSA Public Key</i>	207
GK (GL)	<i>Export Key under an RSA Public Key</i>	213
GM (GN)	<i>Hash a Block of Data</i>	435
GO (GP)	<i>Verify a PIN Using the IBM Offset Method (3DES & AES DUKPT)</i>	402
GQ (GR)	<i>Verify a PIN Using the ABA PVV Method (3DES & AES DUKPT)</i>	406
GS (GT)	<i>Verify a PIN Using the Diebold Method (3DES & AES DUKPT)</i>	410
GU (GV)	<i>Verify a PIN Using the Encrypted PIN Method (3DES & AES DUKPT)</i>	413
GW (GX)	<i>Generate/Verify a MAC (3DES & AES DUKPT)</i>	416
H0 (H1)	<i>Decrypt a PIN Pad Public Key</i>	182
H2 (H3)	<i>Calculate a RSA Public Key Verification Code</i>	686
H4 (H5)	<i>Generate a KEKs for use in Node to Node interchange using RSA</i>	178
H6 (H7)	<i>Receive a KEKr for use in Node to Node interchange using RSA</i>	180
H8 (H9)	<i>Encrypt a Cross Acquirer Key Encrypting Key under an Initial Transport Key</i>	184
HI (HJ)	<i>Transaction Request With a PIN (T/AQ Key) (when selected Transaction Key Scheme is Australian)</i>	373
HI (HJ)	<i>Verify a Transaction Request, with PIN, when CD Field not Available (when selected Transaction Key Scheme is Racal)</i>	698
HK (HL)	<i>Transaction Request Without a PIN (when selected Transaction Key Scheme is Australian)</i>	376
HK (HL)	<i>Generate Transaction Response, with Auth Para Generated by Acquirer (when selected Transaction Key Scheme is Racal)</i>	701
HM (HN)	<i>Administration Request Message (when selected Transaction Key Scheme is Australian)</i>	385
HM (HN)	<i>Generate Transaction Response with Auth Para Generated by Card Issuer (when selected Transaction Key Scheme is Racal)</i>	704
HO (HP)	<i>Transaction Response with Auth Para from Card Issuer (when selected Transaction Key Scheme is Australian)</i>	388
HO (HP)	<i>Translate a PIN from PEK to ZPK Encryption (when selected Transaction Key Scheme is Racal)</i>	707
HQ (HR)	<i>Generate Auth Para and Transaction Response (when selected Transaction Key Scheme is Australian)</i>	391

Command (Response)	Function	Page
HQ (HR)	<i>Verify a Transaction Completion Confirmation (when selected Transaction Key Scheme is Racal)</i>	710
HS (HT)	<i>Confirmation (when selected Transaction Key Scheme is Australian)</i>	394
HS (HT)	<i>Generate a Transaction Completion Response (when selected Transaction Key Scheme is Racal)</i>	713
HU (HV)	<i>Transaction Request With a PIN (T/CI Key) (when selected Transaction Key Scheme is Australian)</i>	379
HU (HV)	<i>Generate Auth Para at the Card Issuer (when selected Transaction Key Scheme is Racal)</i>	724
HW (HX)	<i>Translate KEYVAL (when selected Transaction Key Scheme is Australian)</i>	382
HW (HX)	<i>Generate an Initial Terminal Key (when selected Transaction Key Scheme is Racal)</i>	726
HY (HZ)	<i>Import a Key encrypted under a KTK</i>	79
I0 (I1)	<i>Encrypt a Terminal Key under the LMK</i>	186
I2 (I3)	<i>Import MULTOS Transport Key Certifying Key</i>	579
I4 (I5)	<i>Import MULTOS Hash Modulus Key</i>	580
I6 (I7)	<i>Translate MULTOS KTU</i>	581
I8 (I9)	<i>MULTOS ALU Generator – Allocate ALU Area</i>	585
I8 (I9)	<i>MULTOS ALU Generator – Load Block</i>	586
I8 (I9)	<i>MULTOS ALU Generator – Load Clear Data</i>	587
I8 (I9)	<i>MULTOS ALU Generator – Load Cipher Data</i>	589
I8 (I9)	<i>MULTOS ALU Generator – Generate Checksum</i>	592
I8 (I9)	<i>MULTOS ALU Generator – Encrypt Area</i>	594
I8 (I9)	<i>MULTOS ALU Generator – Generate Signature</i>	596
I8 (I9)	<i>MULTOS ALU Generator – Generate KTU</i>	598
I8 (I9)	<i>MULTOS ALU Generator – Return ALU</i>	600
I8 (I9)	<i>MULTOS ALU Generator – Release ALU</i>	601
IC (ID)	<i>Establish Secure Session with Chip Card</i>	603
IE (IF)	<i>Prepare Secure Message for Chip Card</i>	610
IG (IH)	<i>Key Derivation using Elliptic Curve Key Agreement</i>	222
II (IJ)	<i>Verify and Decrypt Response Secure Message from Chip Card</i>	617
IK (IL)	<i>EMV Sign Data</i>	574
IM (IN)	<i>EMV Recover Data</i>	576
IO (IP)	<i>Generate Remote Management Session ID and Session Keys</i>	135
IQ (IR)	<i>Validate Authentication Code</i>	620
IU (IV)	<i>Generate Remote Management Secure Message</i>	621

Command (Response)	Function	Page
IW (IX)	<i>Validate and Recover Remote Management Secure Message from the MPA</i>	627
IY (IZ)	<i>Generate Digitized Card Single Use Keys</i>	116
J0 (J1)	<i>Generate an Issuer RSA Key Set</i>	138
J2 (J3)	<i>Get HSM Loading</i>	512
J4 (J5)	<i>Get Host Command Volumes</i>	513
J6 (J7)	<i>Reset Utilization Statistics</i>	514
J8 (J9)	<i>Get Health Check Accumulated Counts</i>	515
JA (JB)	<i>Generate a Random PIN</i>	265
JC (JD)	<i>Translate a PIN from TPK to LMK Encryption</i>	341
JE (JF)	<i>Translate a PIN from ZPK to LMK Encryption</i>	339
JG (JH)	<i>Translate a PIN from LMK to ZPK Encryption</i>	343
JI (JJ)	<i>Reset Health Check Accumulated Counts</i>	517
JK (JL)	<i>Get Instantaneous Health Check Status</i>	518
JO (JP)	<i>Validate a CA Self-Signed Certificate</i>	140
JW (JX)	<i>JWT Encode</i>	631
JY (JZ)	<i>JWT Decode</i>	635
K0 (K1)	<i>Decrypt Encrypted Counters (EMV 4.x)</i>	552
K2 (K3)	<i>Verify Truncated Application Cryptogram (Mastercard CAP)</i>	547
K4 (K5)	<i>ARQC Generation</i>	531
K8 (K9)	<i>Export a Key under a KEK</i>	106
KE (KF)	<i>Generate Issuer RSA Key Set and Public Key Certificate</i>	558
KG (KH)	<i>Validate an Issuer Public Key Certificate</i>	561
KI (KJ)	<i>Derive Card Unique DES Keys</i>	100
KK (KL)	<i>Import a Certification Authority Self-Signed Certificate</i>	571
KM (KN)	<i>Generate Static Data Authentication Signature</i>	564
KO (KP)	<i>Generate Card RSA Key Set and Public Key Certificate</i>	566
KQ (KR)	<i>ARQC Verification and/or ARPC Generation (Using Static or Mastercard Proprietary SKD Method)</i>	528
KS (KT)	<i>Data Authentication Code and Dynamic Number Verification (EMV 3.1.1)</i>	550
KU (KV)	<i>Generate Secure Message (EMV 3.1.1)</i>	537
KW (KX)	<i>ARQC Verification and/or ARPC Generation (Using EMV or Cloud-Based SKD Methods)</i>	533
KY (KZ)	<i>Generate Secure Message (EMV 4.x)</i>	542
L0 (L1)	<i>Generate an HMAC Secret Key</i>	460
L6 (L7)	<i>Import an RSA Private Key</i>	109
L8 (L9)	<i>Export an RSA Private Key</i>	113

Command (Response)	Function	Page
LA (LB)	<i>Load Data to User Storage</i>	486
LC (LD)	<i>Verify the Diebold Table in User Storage</i>	490
LE (LF)	<i>Read Data from User Storage</i>	488
LG (LH)	<i>Set HSM Response Delay</i>	498
LI (LJ)	<i>Load a PIN Text String</i>	295
LO (LP)	<i>Translate Decimalization Table from Old to New LMK</i>	499
LQ (LR)	<i>Generate an HMAC on a Block of Data</i>	463
LS (LT)	<i>Verify an HMAC on a Block of Data</i>	465
LU (LV)	<i>Import an HMAC key under a ZMK</i>	467
LW (LX)	<i>Export an HMAC key under a ZMK</i>	471
LY (LZ)	<i>Translate a HMAC Key from Old LMK to New LMK</i>	474
M0 (M1)	<i>Encrypt Data Block</i>	439
M2 (M3)	<i>Decrypt Data Block</i>	446
M4 (M5)	<i>Translate Data Block</i>	452
M6 (M7)	<i>Generate MAC</i>	420
M8 (M9)	<i>Verify MAC</i>	423
MY (MZ)	<i>Verify and Translate MAC</i>	426
N0 (N1)	<i>Generate a Random Value</i>	504
N6 (N7)	<i>Import Bancontact Session Key</i>	251
N8 (N9)	<i>Export Bancontact Session Key</i>	256
NC (ND)	<i>Perform Diagnostics</i>	506
NE (NF, NZ)	<i>Generate and Print a Key as Split Components</i>	69
NG (NH)	<i>Decrypt an Encrypted PIN</i>	298
NI (NJ)	<i>Return Network Information</i>	509
NK (NL)	<i>Command Chaining</i>	500
NO (NP)	<i>HSM Status</i>	507
NY (NZ)	<i>Generate IVCVC3 and Static CVC3</i>	555
OA (OB, OZ)	<i>Print a PIN Solicitation Mailer</i>	284
OI (OJ)	<i>Generate a Set of Zone Keys</i>	154
OK (OL)	<i>Translate a Set of Zone Keys to Encryption under the LMK</i>	156
OU (OV)	<i>Update Terminal Master Key 1</i>	161
OW (OX)	<i>Update Terminal Master Keys</i>	163
P0 (P1)	<i>Verify and Generate a VISA PVV (of a customer selected PIN)</i>	679
P2 (P3)	<i>Generate a VISA PVV (of a customer selected PIN)</i>	682
P4 (P5)	<i>Generate a Proof of Host value</i>	685
P6 (P7)	<i>Load OPINPad to HSM Memory</i>	351

Command (Response)	Function	Page
P8 (P9)	<i>Decode OPIN and translate to ZPK</i>	352
PA (PB)	<i>Load Formatting Data to HSM</i>	293
PC (PD)	<i>Load Additional Formatting Data to HSM</i>	294
PE (PF, PZ)	<i>Print PIN/PIN and Solicitation Data</i>	282
PG (PH)	<i>Verify PIN/PIN and Solicitation Mailer Cryptography</i>	286
PI (PJ)	<i>Generate a Set of Terminal Keys</i>	165
PK (PL)	<i>Generate a PIN Pad Acquirer Security Number</i>	640
PM (PN)	<i>Verify a Dynamic CVV/CVC</i>	360
PO (PP)	<i>Translate a PIN Block to Encryption under a Zone PIN Key</i>	642
PQ (PR)	<i>Generate a Message Authentication Code AS2805.4 – 1985</i>	644
PS (PT)	<i>Validate a Message Authentication Code AS2805.4 -1985</i>	648
PU (PV)	<i>Encrypt Data</i>	652
PW (PX)	<i>Decrypt Data</i>	654
PY (PZ)	<i>Verify and Generate an IBM PIN Offset (of a customer selected PIN)</i>	676
Q0 (Q1)	<i>Translate Audit Record MAC key</i>	522
Q2 (Q3)	<i>Retrieve Audit Record</i>	523
Q4 (Q5)	<i>Archive (Print) Audit Record</i>	524
Q6 (Q7)	<i>Delete Audit Record</i>	525
Q8 (Q9)	<i>Audit Record Verification</i>	526
QA (QB)	<i>Load Solicitation Data to User Storage</i>	289
QC (QD)	<i>Final Load of Solicitation Data to User Storage</i>	290
QE (QF)	<i>Generate a Certificate Request</i>	219
QI (QJ)	<i>Translate a PPASN from old to new LMK</i>	675
QK (QL)	<i>Translate Account Number for LMK-encrypted PIN</i>	346
QM (QN)	<i>Data Encryption Using a Derived Privacy Key</i>	727
QO (QP)	<i>Data Decryption Using a Derived Privacy Key</i>	729
QQ (QR)	<i>Verify a PIN at Card Issuer using IBM Method</i>	714
QS (QT)	<i>Verify a PIN at Card Issuer using the Diebold Method</i>	716
QU (QV)	<i>Verify a PIN at Card Issuer using Visa Method</i>	718
QW (QX)	<i>Verify a PIN at Card Issuer using the Comparison Method</i>	720
QY (QZ)	<i>Generate a Dynamic CVV</i>	358
R4 (R5)	<i>Export Chip Card Key Set (2002 & 2003 Version)</i>	145
R4 (R5)	<i>Export Chip Card Key Set (2007 Version)</i>	149
R6 (R7)	<i>Export Magnetic Stripe Card Key Set</i>	143
R8 (R9)	<i>Import Transport Key Set</i>	141
RA (RB)	<i>Cancel Authorized Activities</i>	493

Command (Response)	Function	Page
RC (RD)	<i>Verify Solicitation Mailer Cryptography</i>	287
RE (RF)	<i>Verify a Transaction Request, without PIN</i>	692
RG (RH)	<i>Verify a Transaction Request, with PIN, when CD Field Available</i>	694
RI (RJ)	<i>Transaction Request With a PIN (T/AQ Key) (when selected Transaction Key Scheme is Racal)</i>	371
RI (RJ)	<i>Verify a Transaction Request, with PIN, when CD Field not Available (when selected Transaction Key Scheme is Australian)</i>	696
RK (RL)	<i>Transaction Request Without a PIN (when selected Transaction Key Scheme is Racal)</i>	374
RK (RL)	<i>Generate Transaction Response, with Auth Para Generated by Acquirer (when selected Transaction Key Scheme is Australian)</i>	699
RM (RN)	<i>Administration Request Message (when selected Transaction Key Scheme is Racal)</i>	383
RM (RN)	<i>Generate Transaction Response with Auth Para Generated by Card Issuer (when selected Transaction Key Scheme is Australian)</i>	702
RO (RP)	<i>Transaction Response with Auth Para from Card Issuer (when selected Transaction Key Scheme is Racal)</i>	386
RO (RP)	<i>Translate a PIN from PEK to ZPK Encryption (when selected Transaction Key Scheme is Australian)</i>	705
RQ (RR)	<i>Generate Auth Para and Transaction Response (when selected Transaction Key Scheme is Racal)</i>	389
RQ (RR)	<i>Verify a Transaction Completion Confirmation (when selected Transaction Key Scheme is Australian)</i>	708
RS (RT)	<i>Confirmation (when selected Transaction Key Scheme is Racal)</i>	392
RS (RT)	<i>Generate a Transaction Completion Response (when selected Transaction Key Scheme is Australian)</i>	711
RU (RV)	<i>Transaction Request With a PIN (T/CI Key) (when selected Transaction Key Scheme is Racal)</i>	377
RU (RV)	<i>Generate Auth Para at the Card Issuer (when selected Transaction Key Scheme is Australian)</i>	722
RW (RX)	<i>Translate KEYVAL (when selected Transaction Key Scheme is Racal)</i>	380
RW (RX)	<i>Generate an Initial Terminal Key (when selected Transaction Key Scheme is Australian)</i>	725
RY (RZ)	<i>Calculate Card Security Codes</i>	302
RY (RZ)	<i>Verify Card Security Codes</i>	368
ZA (ZB)	<i>Generate a Random Alphanumeric PIN</i>	477
ZE (ZF, ZZ)	<i>Print Alphanumeric PIN/Alphanumeric PIN and Solicitation Data</i>	478
ZK (ZL)	<i>Translate an Alphanumeric PIN from old LMK to new LMK Encryption</i>	480
ZM (ZN)	<i>Translate Encrypted PIN to Encrypted Alphanumeric PIN</i>	482
ZU (ZW)	<i>Verify Alphanumeric PIN Block from Internet, return new encrypted PIN & Verify MAC</i>	483

2.2 List of Host Commands (Functional)

Function	Command (Response)	Page
<i>Key Management Commands</i>		
Generic Key Management Commands		36
Generate a Key	A0 (A1)	39
Generate & Export a Key	A0 (A1)	42
Derive a Key	A0 (A1)	48
Derive & Export a Key	A0 (A1)	57
Generate and Print a Component	A2 (A3, AZ)	66
Generate and Print a Key as Split Components	NE (NF, NZ)	69
Form a Key from Encrypted Components	A4 (A5)	72
Import a Key	A6 (A7)	75
Import a Key encrypted under a KTK	HY (HZ)	79
Export a Key	A8 (A9)	82
Translate Key Scheme	B0 (B1)	87
Translate ZMK from ZMK to LMK encryption	BY (BZ)	88
LMK Translation Commands		92
Translate a PIN and PIN Length	BG (BH)	93
Translate Keys from Old LMK to New LMK and Migrate to New Key Type	BW (BX)	94
Erase the Key Change Storage	BS (BT)	98
EMV Key Management Commands		99
Derive Card Unique DES Keys	KI (KJ)	100
Export a Key under a KEK	K8 (K9)	106
Import an RSA Private Key	L6 (L7)	109
Export an RSA Private Key	L8 (L9)	113
Generate Digitized Card Single Use Keys	IY (IZ)	116
Generate Remote Management Session ID and Session Keys	IO (IP)	135
Mastercard Key Management (OBKM) Commands		137
Generate an Issuer RSA Key Set	J0 (J1)	138
Validate a CA Self-Signed Certificate	JO (JP)	140
Import Transport Key Set	R8 (R9)	141
Export Magnetic Stripe Card Key Set	R6 (R7)	143
Export Chip Card Key Set (2002 & 2003 Version)	R4 (R5)	145

Function	Command (Response)	Page
<i>Export Chip Card Key Set (2007 Version)</i>	R4 (R5)	149
AS2805 Key Management Commands		153
Generate a Set of Zone Keys	OI (OJ)	154
Translate a Set of Zone Keys to Encryption under the LMK	OK (OL)	156
Generate Initial Terminal Master Keys (AS2805 – 2001)	C0 (C1)	159
Update Terminal Master Key 1	OU (OV)	161
Update Terminal Master Keys	OW (OX)	163
Generate a Set of Terminal Keys	PI (PJ)	165
Generate an Acquirer Master Key Encrypting Key	C8 (C9)	168
Translate an Acquirer Master Key Encrypting Key	D6 (D7)	170
KEKGEN – 6.3	F6 (F7)	172
KEKREC – 6.3	F8 (F9)	174
Generate a KCA and KMACH	E8 (E9)	176
Generate a KEKs for use in Node to Node interchange using RSA	H4 (H5)	178
Receive a KEKr for use in Node to Node interchange using RSA	H6 (H7)	180
Decrypt a PIN Pad Public Key	H0 (H1)	182
Encrypt a Cross Acquirer Key Encrypting Key under an Initial Transport Key	H8 (H9)	184
Encrypt a Terminal Key under the LMK	I0 (I1)	186
Asymmetric Key Management Commands		188
Generate an RSA Public/Private Key Pair	EI (EJ)	188
Generate an ECC Public/Private Key Pair	FY (FZ)	193
Load a Private Key	EK (EL)	195
Translate a Private Key	EM (EN)	196
Import a Public Key	EO (EP)	197
Validate a Public Key	EQ (ER)	201
Validate a Certificate and Import the Public Key	ES (ET)	202
Translate a Public Key	EU (EV)	205
Import Key or data under an RSA Public Key	GI (GJ)	207
Export Key under an RSA Public Key	GK (GL)	213
Generate a Certificate Request	QE (QF)	219
Key Derivation using Elliptic Curve Key Agreement	IG (IH)	222
TR-34 Key Export	B8 (B9)	244
Bancontact Session Commands		249
Import Bancontact Session Key	N6 (N7)	251
Export Bancontact Session Key	N8 (N9)	256

Function	Command (Response)	Page
Magnetic Stripe Issuing Commands		
PIN and Offset Generation Commands		259
Derive a PIN and Optionally Generate Offset for New PVK Using the IBM Offset Method	EE (EF)	260
Derive a PIN Using the Diebold Method	GA (GB)	263
Generate a Random PIN	JA (JB)	265
Generate an IBM PIN Offset (of an LMK encrypted PIN)	DE (DF)	267
Generate an IBM PIN Offset (of a customer selected PIN)	BK (BL)	270
Generate a Diebold PIN Offset	CE (CF)	273
Generate an ABA PVV (of an LMK encrypted PIN)	DG (DH)	275
Generate an ABA PVV (of a customer selected PIN)	FW (FX)	277
Load the Excluded PIN Table	BM (BN)	280
PIN Mailer Printing Commands		281
Print PIN/PIN and Solicitation Data	PE (PF, PZ)	282
Print a PIN Solicitation Mailer	OA (OB, OZ)	284
Verify PIN/PIN and Solicitation Mailer Cryptography	PG (PH)	286
Verify Solicitation Mailer Cryptography	RC (RD)	287
PIN Solicitation Data Processing Commands		288
Load Solicitation Data to User Storage	QA (QB)	289
Final Load of Solicitation Data to User Storage	QC (QD)	290
Print Output Formatting Commands		292
Load Formatting Data to HSM	PA (PB)	293
Load Additional Formatting Data to HSM	PC (PD)	294
Load a PIN Text String	LI (LJ)	295
Clear PIN Commands		296
Encrypt a Clear PIN	BA (BB)	297
Decrypt an Encrypted PIN	NG (NH)	298
Card Verification Code/Value Generation Commands		299
Generate a Card Verification Code/Value	CW (CX)	300
Calculate Card Security Codes	RY (RZ)	302
Magnetic Stripe Transaction Processing		
PIN Change Commands		304
Verify a PIN & Generate an IBM PIN Offset (of customer selected new PIN)	DU (DV)	305

Function	Command (Response)	Page
<i>Verify a PIN & Generate an ABA PVV (of a customer selected PIN)</i>	CU (CV)	309
PIN Verification Commands		312
<i>Verify a Terminal PIN Using the IBM Offset Method</i>	DA (DB)	313
<i>Verify an Interchange PIN Using the IBM Offset Method</i>	EA (EB)	316
<i>Verify a Terminal PIN Using the Diebold Method</i>	CG (CH)	319
<i>Verify an Interchange PIN Using the Diebold Method</i>	EG (EH)	321
<i>Verify a Terminal PIN Using the ABA PVV Method</i>	DC (DD)	322
<i>Verify an Interchange PIN Using the ABA PVV Method</i>	EC (ED)	325
<i>Verify a Terminal PIN Using the Comparison Method</i>	BC (BD)	327
<i>Verify an Interchange PIN Using the Comparison Method</i>	BE (BF)	329
PIN Translation Commands		331
<i>Translate a PIN from One ZPK to Another</i>	CC (CD)	332
<i>Translate a PIN from TPK to ZPK/BDK Encryption (3DES DUKPT)</i>	CA (CB)	335
<i>Translate a PIN from ZPK to LMK Encryption</i>	JE (JF)	339
<i>Translate a PIN from TPK to LMK Encryption</i>	JC (JD)	341
<i>Translate a PIN from LMK to ZPK Encryption</i>	JG (JH)	343
<i>Translate PIN Algorithm</i>	BQ (BR)	345
<i>Translate Account Number for LMK-encrypted PIN</i>	QK (QL)	346
<i>Translate an RSA-encrypted PIN to a ZPK or TPK-encrypted PIN</i>	AQ (AR)	348
<i>Load OPINPad to HSM Memory</i>	P6 (P7)	351
<i>Decode OPIN and translate to ZPK</i>	P8 (P9)	352
Card Verification Code/Value Commands		354
<i>Verify a Card Verification Code/Value</i>	CY (CZ)	355
<i>Generate a Dynamic CVV</i>	QY (QZ)	358
<i>Verify a Dynamic CVV/CVC</i>	PM (PN)	360
<i>Verify Card Security Codes</i>	RY (RZ)	368
Racal Transaction Key Scheme (RTKS) Commands		370
<i>Transaction Request With a PIN (T/AQ Key) (when selected Transaction Key Scheme is Racal)</i>	RI (RJ)	371
<i>Transaction Request With a PIN (T/AQ Key) (when selected Transaction Key Scheme is Australian)</i>	HI (HJ)	373
<i>Transaction Request Without a PIN (when selected Transaction Key Scheme is Racal)</i>	RK (RL)	374
<i>Transaction Request Without a PIN (when selected Transaction Key Scheme is Australian)</i>	HK (HL)	376
<i>Transaction Request With a PIN (T/CI Key) (when selected Transaction Key Scheme is Racal)</i>	RU (RV)	377

Function	Command (Response)	Page
<i>Transaction Request With a PIN (T/CI Key) (when selected Transaction Key Scheme is Australian)</i>	HU (HV)	379
<i>Translate KEYVAL (when selected Transaction Key Scheme is Racal)</i>	RW (RX)	380
<i>Translate KEYVAL (when selected Transaction Key Scheme is Australian)</i>	HW (HX)	382
<i>Administration Request Message (when selected Transaction Key Scheme is Racal)</i>	RM (RN)	383
<i>Administration Request Message (when selected Transaction Key Scheme is Australian)</i>	HM (HN)	385
<i>Transaction Response with Auth Para from Card Issuer (when selected Transaction Key Scheme is Racal)</i>	RO (RP)	386
<i>Transaction Response with Auth Para from Card Issuer (when selected Transaction Key Scheme is Australian)</i>	HO (HP)	388
<i>Generate Auth Para and Transaction Response (when selected Transaction Key Scheme is Racal)</i>	RQ (RR)	389
<i>Generate Auth Para and Transaction Response (when selected Transaction Key Scheme is Australian)</i>	HQ (HR)	391
<i>Confirmation (when selected Transaction Key Scheme is Racal)</i>	RS (RT)	392
<i>Confirmation (when selected Transaction Key Scheme is Australian)</i>	HS (HT)	394
DUKPT (X9.24) Transaction Processing Commands		395
<i>Translate a PIN from BDK to BDK or ZPK Encryption (3DES & AES DUKPT)</i>	G0 (G1)	398
<i>Verify a PIN Using the IBM Offset Method (3DES & AES DUKPT)</i>	GO (GP)	402
<i>Verify a PIN Using the ABA PVV Method (3DES & AES DUKPT)</i>	GQ (GR)	406
<i>Verify a PIN Using the Diebold Method (3DES & AES DUKPT)</i>	GS (GT)	410
<i>Verify a PIN Using the Encrypted PIN Method (3DES & AES DUKPT)</i>	GU (GV)	413
<i>Generate/Verify a MAC (3DES & AES DUKPT)</i>	GW (GX)	416
Data Protection Commands		
Message Integrity Commands		419
<i>Generate MAC</i>	M6 (M7)	420
<i>Verify MAC</i>	M8 (M9)	423
<i>Verify and Translate MAC</i>	MY (MZ)	426
<i>Generate an RSA/ECC Signature</i>	EW (EX)	430
<i>Validate an RSA/ECC Signature</i>	EY (EZ)	433
<i>Hash a Block of Data</i>	GM (GN)	435

Function	Command (Response)	Page
Message Encryption Commands		436
Encrypt Data Block	M0 (M1)	439
Decrypt Data Block	M2 (M3)	446
Translate Data Block	M4 (M5)	452
User Authentication Commands		
HMAC Commands		459
Generate an HMAC Secret Key	L0 (L1)	460
Generate an HMAC on a Block of Data	LQ (LR)	463
Verify an HMAC on a Block of Data	LS (LT)	465
Import an HMAC key under a ZMK	LU (LV)	467
Export an HMAC key under a ZMK	LW (LX)	471
Translate a HMAC Key from Old LMK to New LMK	LY (LZ)	474
WebPIN Commands		476
Generate a Random Alphanumeric PIN	ZA (ZB)	477
Print Alphanumeric PIN/Alphanumeric PIN and Solicitation Data	ZE (ZF, ZZ)	478
Translate an Alphanumeric PIN from old LMK to new LMK Encryption	ZK (ZL)	480
Translate Encrypted PIN to Encrypted Alphanumeric PIN	ZM (ZN)	482
Verify Alphanumeric PIN Block from Internet, return new encrypted PIN & Verify MAC	ZU (ZW)	483
HSM Management Commands		
User Storage Commands		485
Load Data to User Storage	LA (LB)	486
Read Data from User Storage	LE (LF)	488
Verify the Diebold Table in User Storage	LC (LD)	490
Miscellaneous Commands		491
Echo Command	B2 (B3)	492
Cancel Authorized Activities	RA (RB)	493
Generate a Key Check Value	BU (BV)	495
Set HSM Response Delay	LG (LH)	498
Translate Decimalization Table from Old to New LMK	LO (LP)	499
Command Chaining	NK (NL)	500
Modify Key Block Header	CS (CT)	502
Generate a Random Value	N0 (N1)	504

Function	Command (Response)	Page
Diagnostic Commands		505
Perform Diagnostics	NC (ND)	506
HSM Status	NO (NP)	507
Return Network Information	NI (NJ)	509
Get HSM Loading	J2 (J3)	512
Get Host Command Volumes	J4 (J5)	513
Reset Utilization Statistics	J6 (J7)	514
Get Health Check Accumulated Counts	J8 (J9)	515
Reset Health Check Accumulated Counts	JI (JJ)	517
Get Instantaneous Health Check Status	JK (JL)	518
Auditing Commands		521
Translate Audit Record MAC key	Q0 (Q1)	522
Retrieve Audit Record	Q2 (Q3)	523
Archive (Print) Audit Record	Q4 (Q5)	524
Delete Audit Record	Q6 (Q7)	525
Audit Record Verification	Q8 (Q9)	526
EMV Transaction Processing Commands		
EMV Chip Card Commands		527
ARQC Verification and/or ARPC Generation (Using Static or Mastercard Proprietary SKD Method)	KQ (KR)	528
ARQC Verification and/or ARPC Generation (Using EMV or Cloud-Based SKD Methods)	KW (KX)	533
ARQC Generation	K4 (K5)	531
Generate Secure Message (EMV 3.1.1)	KU (KV)	537
Generate Secure Message (EMV 4.x)	KY (KZ)	542
Verify Truncated Application Cryptogram (Mastercard CAP)	K2 (K3)	547
Data Authentication Code and Dynamic Number Verification (EMV 3.1.1)	KS (KT)	550
Decrypt Encrypted Counters (EMV 4.x)	K0 (K1)	552
EMV Chip, Contactless & Mobile Issuing		
Contactless Cards Data Preparation Commands		554
Generate IVCVC3 and Static CVC3	NY (NZ)	555

Function	Command (Response)	Page
EMV-based Cards Data Preparation Commands		557
Generate Issuer RSA Key Set and Public Key Certificate	KE (KF)	558
Validate an Issuer Public Key Certificate	KG (KH)	561
Generate Static Data Authentication Signature	KM (KN)	564
Generate Card RSA Key Set and Public Key Certificate	KO (KP)	566
Import a Certification Authority Self-Signed Certificate	KK (KL)	571
EMV Sign Data	IK (IL)	574
EMV Recover Data	IM (IN)	576
MULTOS Card Data Preparation Commands		578
Import MULTOS Transport Key Certifying Key	I2 (I3)	579
Import MULTOS Hash Modulus Key	I4 (I5)	580
Translate MULTOS KTU	I6 (I7)	581
MULTOS ALU Generator – Allocate ALU Area	I8 (I9)	585
MULTOS ALU Generator – Load Block	I8 (I9)	586
MULTOS ALU Generator – Load Clear Data	I8 (I9)	587
MULTOS ALU Generator – Load Cipher Data	I8 (I9)	589
MULTOS ALU Generator – Generate Checksum	I8 (I9)	592
MULTOS ALU Generator – Encrypt Area	I8 (I9)	594
MULTOS ALU Generator – Generate Signature	I8 (I9)	596
MULTOS ALU Generator – Generate KTU	I8 (I9)	598
MULTOS ALU Generator – Return ALU	I8 (I9)	600
MULTOS ALU Generator – Release ALU	I8 (I9)	601
Chip Card Personalization Commands		602
Establish Secure Session with Chip Card	IC (ID)	603
Prepare Secure Message for Chip Card	IE (IF)	610
Verify and Decrypt Response Secure Message from Chip Card	II (IJ)	617
Mobile Device Provisioning Commands		619
Validate Authentication Code	IQ (IR)	620
Generate Remote Management Secure Message	IU (IV)	621
Validate and Recover Remote Management Secure Message from the MPA	IW (IX)	627
JSON Web Token (JWT) Commands		630
JWT Encode	JW (JX)	631
JWT Decode	JY (JZ)	635

Function	Command (Response)	Page
<i>AS2805 Transaction Processing</i>		
AS2805 Commands		638
Generate a PIN Pad Acquirer Security Number	PK (PL)	640
Translate a PIN Block to Encryption under a Zone PIN Key	PO (PP)	642
Generate a Message Authentication Code AS2805.4 – 1985	PQ (PR)	644
Generate a Message Authentication Code (large messages)	C2 (C3)	646
Validate a Message Authentication Code AS2805.4 -1985	PS (PT)	648
Verify a Message Authentication Code (large messages)	C4 (C5)	650
Encrypt Data	PU (PV)	652
Decrypt Data	PW (PX)	654
Translate a PIN Block to Encryption under a PIN Encryption Key	D4 (D5)	656
Generate a KEKs Validation Request	E0 (E1)	658
Generate a KEKr Validation Response	E2 (E3)	660
Verify a PIN Pad Proof of End Point	E4 (E5)	662
Verify a Terminal PIN using the IBM Method (AS2805 6.4)	F0 (F1)	664
Verify a Terminal PIN using the VISA Method (AS2805 6.4)	F2 (F3)	666
Calculate KMACI	F4 (F5)	668
Generate a Random Number	C6 (C7)	670
Generate a PIN Pad Authentication Code	D0 (D1)	671
Encrypt a CPAT Authentication Value	D8 (D9)	672
Verify a PIN Pad Authentication Code	D2 (D3)	673
Generate a PIN Pad Proof of Endpoint (POEP)	E6 (E7)	674
Translate a PPASN from old to new LMK	QI (QJ)	675
Verify and Generate an IBM PIN Offset (of a customer selected PIN)	PY (PZ)	676
Verify and Generate a VISA PVV (of a customer selected PIN)	P0 (P1)	679
Generate a VISA PVV (of a customer selected PIN)	P2 (P3)	682
Generate a Proof of Host value	P4 (P5)	685
Calculate a RSA Public Key Verification Code	H2 (H3)	686

Function	Command (Response)	Page
AS2805.6.2 Support		687
Verify a Transaction Request, without PIN	RE (RF)	692
Verify a Transaction Request, with PIN, when CD Field Available	RG (RH)	694
Verify a Transaction Request, with PIN, when CD Field not Available (when selected Transaction Key Scheme is Australian)	RI (RJ)	696
Verify a Transaction Request, with PIN, when CD Field not Available (when selected Transaction Key Scheme is Racal)	HI (HJ)	698
Generate Transaction Response, with Auth Para Generated by Acquirer (when selected Transaction Key Scheme is Australian)	RK (RL)	699
Generate Transaction Response, with Auth Para Generated by Acquirer (when selected Transaction Key Scheme is Racal)	HK (HL)	701
Generate Transaction Response with Auth Para Generated by Card Issuer (when selected Transaction Key Scheme is Australian)	RM (RN)	702
Generate Transaction Response with Auth Para Generated by Card Issuer (when selected Transaction Key Scheme is Racal)	HM (HN)	704
Translate a PIN from PEK to ZPK Encryption (when selected Transaction Key Scheme is Australian)	RO (RP)	705
Translate a PIN from PEK to ZPK Encryption (when selected Transaction Key Scheme is Racal)	HO (HP)	707
Verify a Transaction Completion Confirmation (when selected Transaction Key Scheme is Australian)	RQ (RR)	708
Verify a Transaction Completion Confirmation (when selected Transaction Key Scheme is Racal)	HQ (HR)	710
Generate a Transaction Completion Response (when selected Transaction Key Scheme is Australian)	RS (RT)	711
Generate a Transaction Completion Response (when selected Transaction Key Scheme is Racal)	HS (HT)	713
Verify a PIN at Card Issuer using IBM Method	QQ (QR)	714
Verify a PIN at Card Issuer using the Diebold Method	QS (QT)	716
Verify a PIN at Card Issuer using Visa Method	QU (QV)	718
Verify a PIN at Card Issuer using the Comparison Method	QW (QX)	720
Generate Auth Para at the Card Issuer (when selected Transaction Key Scheme is Australian)	RU (RV)	722
Generate Auth Para at the Card Issuer (when selected Transaction Key Scheme is Racal)	HU (HV)	724
Generate an Initial Terminal Key (when selected Transaction Key Scheme is Australian)	RW (RX)	725
Generate an Initial Terminal Key (when selected Transaction Key Scheme is Racal)	HW (HX)	726
Data Encryption Using a Derived Privacy Key	QM (QN)	727
Data Decryption Using a Derived Privacy Key	QO (QP)	729

2.3 General

This section details all the commands available with their responses and possible error codes.

A number of abbreviations are used throughout. They are:

L	:	Encrypted PIN length. Set at installation.
m	:	Message header length. Set at installation.
n	:	Variable length field.
A	:	Alphanumeric (can include any non-control type) characters.
H	:	Hexadecimal character ('0'...'9', 'A'...'F').
N	:	Numeric Field ('0'...'9').
C	:	Control character.
B	:	Binary data (byte) (X'00...X'FF).
D	:	Binary coded decimal (BCD) character ('0'...'9').

For example:

32 H : Indicates that thirty-two hexadecimal characters are required.

m A : Indicates the string of "message header length" alphanumeric characters.

In a command to the payShield 10K, any key can be replaced by a reference to internal user storage. In the details that follow, a key is always shown as if it is to be sent with each command; in every case the key can be replaced by the index flag "K" and a three-hexadecimal-digit pointer value: the value of "K" for the index flag is used irrespective of the index flag used when storing the key in User Storage using the *LA* host command.

The payShield 10K can be used in systems where there may be Atalla security equipment at other network nodes. This is achieved by the inclusion of an Atalla variant in those commands that translate a key from/to encryption under a ZMK. This has the effect of modifying the ZMK before it is used to decrypt/encrypt in accordance with the method used by the Atalla equipment. The payShield 10K can support 1 or 2 digit Atalla variants.

When a disabled host command is invoked, the error code 68 is returned.

3 Key Management Commands

3.1 Generic Key Management Commands

The payShield 10K provides the following host commands to support generic key management operations:

Function	Command	Page
<i>Generate a Key</i>	A0 (A1)	39
<i>Generate & Export a Key</i>	A0 (A1)	42
<i>Derive a Key</i>	A0 (A1)	48
<i>Derive & Export a Key</i>	A0 (A1)	57
<i>Generate and Print a Component</i>	A2 (A3, AZ)	66
<i>Generate and Print a Key as Split Components</i>	NE (NF, NZ)	69
<i>Form a Key from Encrypted Components</i>	A4 (A5)	72
<i>Import a Key</i>	A6 (A7)	75
<i>Import a Key encrypted under a KTK</i>	HY (HZ)	79
<i>Export a Key</i>	A8 (A9)	82
<i>Translate Key Scheme</i>	B0 (B1)	87
<i>Translate ZMK from ZMK to LMK encryption</i>	BY (BZ)	88

Available Key Types/Usages

The generic key management commands A0, A6 and A8 can use keys/keyblocks with the following types/usages:

Variant LMK

Type	Key Name
000	Zone Master Key, ZMK
200	VisaCash Master Key, KML
001	Zone PIN encryption, ZPK
002	PIN Verification Key, PVK
002*	Terminal Master Key, TMK
002*	Terminal PIN Key, TPK
302	DUKPT Initial Key, IKEY [◊]
402	Card Verification Key, CVK, CSCK
003	Terminal Authentication Key, TAK
006	Watchword key, WWK
008	Zone authentication key, ZAK
009	DUKPT Base Derivation Key, BDK-1
609	DUKPT Base Derivation Key, BDK-2
809	DUKPT Base Derivation Key, BDK-3
909	DUKPT Base Derivation Key, BDK-4
109	EMV Key, MK-AC
209	EMV Key, MK-SMI
309	EMV Key, MK-SMC
409	EMV Key, MK-DAC
509	EMV Key, MK-DN
709	DCVV Master Key, MK-CVC3
00A	Data Encryption Key, ZEK
00B	Data Encryption Key, DEK
30B	Data Encryption Key, TEK
70D [◊]	Terminal PIN Key, TPK
80D [◊]	Terminal Master Key, TMK
607	ZKA Master Key, ZKA-MK

* Applies if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N".

[◊] Applies if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y".

[◊] IKEY is also known as IPEK.

Note: Refer to the Key Type Table (see the *payShield 10K Host Programmer's manual*) for generation/import/export permissions.

Key Block LMK

Usage	Key Name
01	WatchWord Key, WWK
B0	DUKPT Base Derivation Key, BDK-1
41	DUKPT Base Derivation Key, BDK-2
42	DUKPT Base Derivation Key, BDK-3
43	DUKPT Base Derivation Key, BDK-4
44	DUKPT Base Derivation Key, BDK-5
B1	DUKPT Initial Key, IKEY [◊]
C0	Card verification (generic)
11	Card verification (American Express CSC)
12	Card verification (Mastercard CVC)
13	Card verification (Visa CVV)
D0	Data encryption (generic)
21	Data encryption using a DEK
22	Data encryption using a ZEK
23	Data encryption using a TEK
E0	EMV Master Key: Application Cryptogram (MK _{AC})
E1	EMV Master Key: Secure Messaging for Confidentiality (MK _{SMC})
E2	EMV Master Key: Secure Messaging for Integrity (MK _{SMI})
E3	EMV Master Key: Data Authentication Code (MK _{DAC})
E4	EMV Master Key: Dynamic Numbers (MK _{DN})
E5	EMV Master Key: Card Personalization
E6	EMV Master Key: Other
31	VisaCash Master Load Key, KML
32	Dynamic CVV Master Key, MK-CVC3
K0	Key encryption or wrapping (generic)
K1	Key encryption of wrapping (TR-31)
51	Terminal key encryption, TMK
52	Zone key encryption, ZMK
53	ZKA Master Key, ZKA-MK
56	MKPKC Master Key (Italian Standard)
57	MKPOS/MKSER Master Key (Italian Standard)
58	SPKC Session Key (Italian Standard)
M1	ISO 9797-1 MAC algorithm 1 (using DES/3DES)
M3	ISO 9797-1 MAC algorithm 3 (using 3DES)
M5	CBC-MAC (using AES)
M6	CMAC (using AES)
P0	PIN encryption (generic)
71	Terminal PIN encryption, TPK
72	Zone PIN encryption, ZPK
73	Transaction key scheme Terminal Key Register, TKR
V0	PIN verification, KPV, other algorithm
V1	PIN verification using the IBM 3624 method
V2	PIN verification using the ABA PVV method

[◊] IKEY is also known as IPEK.

Interpretation of TR-31 Key Block Version ID Field

The first byte of a TR-31 key block contains a Key Block Version ID field, which identifies the format of the key block, and the process used to protect it. The table below describes the different possible values for the Key Block Version ID.

Key Block Version ID	Description
'A'	The MACing and encryption keys are derived from the Key Block Protection Key using a simple XOR process. Refer to TR-31:2005 for details.
'B'	The MACing and encryption keys are derived from the Key Block Protection Key using a CMAC process. Refer to TR-31:2010 §5.3.2.1 for details.
'C'	This is essentially identical to Version 'A'. The MACing and encryption keys are derived from the Key Block Protection Key using the same XOR process as used with Key Block Version ID = 'A'. Refer to TR-31:2010 §5.3.3.1 for details.
'D'	The encryption key and Authentication key are derived from the Key Block Protection Key using CMAC as a pseudorandom function to produce 16-byte MAC values. Key Blocks constructed using AES KBPKs will only use version "D". Refer to TR-31:2018 §5.3.2.3 for details.

Generate a Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Variant LMK	Authorization: Determined by KTT(G) Activity: generate.{key}.host
Key Block LMK	Authorization: Not Required

Function: To generate a random key and return it encrypted under the LMK.

Variant LMK	Key Block LMK
Authorization: This command examines the 'Generate' flag of the given key type within the Key Type Table (see the <i>payShield 10K Host Programmer's manual</i>) to determine the authorization requirement. If the flag is 'A', the HSM must either be in the Authorized State, or the activity generate.{key}.host must be authorized, where 'key' is the key type code of the key being generated.	When using a Key Block LMK, no specific authorization is required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'A0'.
Mode	1 H	Indicates the operation of the function: '0': Generate key
Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be generated. A list of possible values is shown in <i>Available Key Types/Usages</i> (p.37). For a Key Block LMK: This field is ignored; should be set to 'FFF'.
Key Scheme (LMK)	1 A	Indicates the scheme for encrypting the output key under the LMK. For a list of key schemes, see the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> .
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
The following section applies only when generating in key block format		
Delimiter	1 A	Value '#'. Required when generating a key block. If present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the key block header; must be present if the above Delimiter is present. For a list of possible values, see <i>Available Key Types/Usages</i> (p.37).
Algorithm	2 A	Algorithm and key length; the first character will be included in the algorithm field in the key block header (byte 7); must be present if the above Delimiter is present; permitted values: 'D1' – single length DES key 'T2' – double length DES key 'T3' – triple length DES key 'A1' – 128-bit AES key 'A2' – 192-bit AES key 'A3' – 256-bit AES key '11' – 128-bit AES key for FF1 only '12' – 192-bit AES key for FF1 only '13' – 256-bit AES key for FF1 only
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in the <i>payShield 10K Host Programmer's manual</i> .
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'A1'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
Key (under LMK)	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The new key, encrypted under the LMK. For a Variant LMK, the 'Key (under LMK)' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'. For a Key Block LMK, the 'Key (under LMK)' will be encrypted under the LMK.
Key Check Value	6 H	The key check value.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate & Export a Key

Variant LMK	Key Block LMK
Available in package(s): Classic & Premium	
Variant LMK	Authorization: Determined by KTT(G&E) Activities: generate.{key}.host and export.{key}.host
Key Block LMK	Authorization: If export to non-KB Activity: export.{key}.host

Function:

To generate a random key and return it encrypted under the LMK and under a ZMK or TMK (for transmission to another party).

Variant LMK	Key Block LMK										
<p>Authorization:</p> <p>This command examines the 'Generate' flag of the given key type within the Key Type Table (see the <i>payShield 10K Host Programmer's manual</i>) to determine the authorization requirement. If the flag is 'A', the HSM must either be in the Authorized State, or the activity generate.{key}.host must be authorized, where 'key' is the key type code of the key being generated.</p> <p>This command also examines the 'Export' flag of the given key type within the Key Type Table (see the <i>payShield 10K Host Programmer's manual</i>). If the flag is 'A', the HSM must either be in the Authorized State, or the activity export.{key}.host must be authorized, where 'key' is the key usage code of the key being exported.</p>	<p>The authorization requirement for this command depends solely on the type of export being requested:</p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="background-color: #f2e0e0;">"Key Scheme (ZMK)"</th><th style="background-color: #d9eaf7;">Authorization</th></tr> </thead> <tbody> <tr> <td>'S' (Thales Key Block)</td><td>None</td></tr> <tr> <td>'R' (TR-31 Key Block)</td><td>None</td></tr> <tr> <td>'U', 'T' (Variant)</td><td>Required</td></tr> <tr> <td>'Z', 'X', 'Y' (X9.17)</td><td>Required</td></tr> </tbody> </table> <p>If authorization is required, the HSM must either be in the Authorized State, or the activity export.{key}.host must be authorized, where 'key' is the key usage code of the key being exported.</p>	"Key Scheme (ZMK)"	Authorization	'S' (Thales Key Block)	None	'R' (TR-31 Key Block)	None	'U', 'T' (Variant)	Required	'Z', 'X', 'Y' (X9.17)	Required
"Key Scheme (ZMK)"	Authorization										
'S' (Thales Key Block)	None										
'R' (TR-31 Key Block)	None										
'U', 'T' (Variant)	Required										
'Z', 'X', 'Y' (X9.17)	Required										

<p>Notes:</p> <p>A TMK can only export the following key types:</p> <p>If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N":</p> <ul style="list-style-type: none"> 002 (TPK or TMK) 003 (TAK) 30B (TEK) 302 (IKEY) <p>If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y":</p> <ul style="list-style-type: none"> 70D (TPK) 80D (TMK) 003 (TAK) 30B (TEK) 302 (IKEYφ) 	<p>A TMK with Key Usage = '51' can only export keyblocks with the following Key Usage values:</p> <ul style="list-style-type: none"> 'P0', '71' (TPK) 'M1', 'M3', 'M5', 'M6' (TAK) '23' (TEK) '51' (TMK) 'B1' (IKEY) <p>When exporting the new key, the ZMK (or TMK) key block must have the following field values:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #d9e1f2;">"ZMK" KB Header</th><th style="background-color: #d9e1f2;">Value(s)</th></tr> </thead> <tbody> <tr> <td>Key Usage</td><td>'K0', 'K1', '51', or '52'</td></tr> <tr> <td>Algorithm</td><td>'D'*', 'T' or 'A'</td></tr> <tr> <td>Mode of Use</td><td>'B', 'E', or 'N'</td></tr> </tbody> </table> <p>* Note: Exporting to a key block format is not permitted with a single-length ZMK or TMK.</p>	"ZMK" KB Header	Value(s)	Key Usage	'K0', 'K1', '51', or '52'	Algorithm	'D'*', 'T' or 'A'	Mode of Use	'B', 'E', or 'N'
"ZMK" KB Header	Value(s)								
Key Usage	'K0', 'K1', '51', or '52'								
Algorithm	'D'*', 'T' or 'A'								
Mode of Use	'B', 'E', or 'N'								

- Further Notes:
- Exporting to a key block format requires the ZMK/TMK to be one of the following:
 - Double or triple length DES key
 - Any size AES key

For security reasons, when using a Key Block LMK, this command will not support the export of a DEK (Key Usage = "D0" or "21") to encryption under a ZMK in variant or X9.17 format.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'A0'.
Mode	1 H	Indicates the operation of the function: '1': Generate key and encrypt under ZMK (or TMK or Current BDK)
Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be generated. A list of possible values is shown in <i>Available Key Types/Usages</i> (p.37). For a Key Block LMK: This field is ignored; should be set to 'FFF'.
Key Scheme (LMK)	1 A	Indicates the scheme for encrypting the output key under the LMK. For a list of key schemes, see the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> .
Delimiter	1 A	Value ';'. Optional. If present, the following field must also be present.
ZMK/TMK Flag	1 N	Optional. Only present if the above delimiter is present. '0': ZMK (default value if these fields are not present) '1': TMK

Field	Length & Type	Details
ZMK (or TMK or Current BDK)	16 / 32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The Zone Master Key (or Terminal Master Key or Current Base Derivation Key). For a ZMK, the length of the key must correspond to the ZMK key length as defined in the Security Settings. For a Variant LMK, the 'ZMK' is encrypted under LMK pair 04-05. The 'TMK' is encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 8 if the setting has the value "Y". For a Key Block LMK, the 'ZMK (or TMK)' must comply with the following:
Key Scheme (ZMK or TMK or Current BDK)	1 A	Indicates the scheme for encrypting the key under the ZMK (or TMK or Current BDK). For a list of key schemes, see the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> .
Atalla Variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.

Field	Length & Type	Details
The following section applies only when generating and exporting in key block format		
Delimiter	1 A	Value '#'. Required when generating a key block. If present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the key block header; must be present if the above Delimiter is present. For a list of possible values, see <i>Available Key Types/Usages</i> (p.37).
Algorithm	2 A	Algorithm and key length; the first character will be included in the algorithm field in the key block header (byte 7); must be present if the above Delimiter is present; permitted values: 'D1' – single length DES key 'T2' – double length DES key 'T3' – triple length DES key 'A1' – 128-bit AES key 'A2' – 192-bit AES key 'A3' – 256-bit AES key
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in the <i>payShield 10K Host Programmer's manual</i> .
This section specifies the optional blocks to be included in both the generated key block and the exported key block.		
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier. Valid values include: 'KS', 'KV', '00' – '05'
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04' to X'FF'; if value = X'04', then the following field is not present.
Optional Block Data	n A	Optional block data.
This section specifies the optional blocks to be included in the exported TR-31 key block (only).		
Delimiter	1 A	Value '\$'. Optional; only present if exporting in TR-31 format.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; must be present if the above Delimiter is present. Permitted values: '00' to '99'. Note this is reduced if Optional Blocks KS and/or KV are specified to be included as given above.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; to be included only in the exported TR-31 key block header. Valid values include: 'KS', 'KV', 'KC', 'KP', 'IK', 'TS' and '00' – '99'. Note: 'KS' and 'KV' can only be added if they are not already included in Thales Key Block - otherwise a "Repeated optional block ID" error is given.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04' to X'FF'; if value = X'04', then the following field is not present.
Optional Block Data	n A	Optional block data.
Delimiter	1 A	Value '&'. Optional; can only be present when the generated key is to be exported; if present, the following field must also be present.
Modified Export Value	1 A	Character to be placed in the exportability field (byte 11) of the exported key; only permitted value = 'N'; must be present if the above Delimiter is present.

Delimiter	1 A	Value '!'. Optional; can only be present when the generated key is to be exported in TR-31 key block format. If present, the following field must be present.
Key Block Version ID	1 A	Key Block Version ID: 'A': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'B': Key block protected using the Key Derivation Binding Method (see Ref 8 §5.3.2.1) 'C': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'D': Key block protected using the AES Key Derivation Binding Method (see Ref 8 §5.3.2.3).
The following section applies only when generating a variant key, and exporting to TR-31 format		
Delimiter	1 A	Value '&'. Optional; can only be present when the generated key is to be exported; if present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the key block header; must be present if the above Delimiter is present. May be any TR-31 permitted value for the key type; For a list of possible values, see the <i>payShield 10K Host Programmer's manual</i> .
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present.
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; only permitted value is 'N' or 'S'; must be present if the above Delimiter is present.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '99'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier. Valid values include: 'KS', 'KV', 'KC', 'KP', 'IK', 'TS' and '00' – '99'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04' to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
Delimiter	1 A	Value '!'. Optional; can only be present when the generated key is to be exported to TR-31 key block format. If present, the following field must also be present.
Key Block Version ID	1 A	Key Block Version ID: 'A': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'B': Key block protected using the Key Derivation Binding Method (see Ref 8 §5.3.2.1) 'C': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1)
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'A1'.
Error Code	2 A	'00': No error '07': Invalid ZKA Master Key Type '10': ZMK or TMK Parity error 'BC': Repeated optional block ID '68': Command disabled or a standard error code.
Key (under LMK)	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The new key, encrypted under the LMK. For a Variant LMK, the 'Key (under LMK)' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'.
Key (under ZMK or TMK or Current BDK)	16 H or 'U' + 32 H or 'T' + 48 H or 'R' + n A or 'S' + n A	For a Key Block LMK, the 'Key (under LMK)' will be encrypted under the LMK. The new key, encrypted under the supplied ZMK (or TMK or Current BDK).
Key Check Value	6 H	The key check value.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Derive a Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Variant LMK	Authorization: Determined by KTT(G) Activities: generate.{key}.host
Key Block LMK	Authorization: Not required

Function: To derive a key and return it encrypted under the LMK.

The following derivation methods are supported:

- Derivation of an Initial Key (IKEY) for the DUKPT scheme.
- Derivation of a ZPK/ZAK/ZEK for the ZKA scheme.
- Derivation of a TEK for the Italian scheme.

Notes for DUKPT derivation

If the BDK is a BDK1, BDK2 or BDK4, then it can be a double-length DES key or a 128/192/256-bit AES key.

If the BDK is a BDK3 or BDK5, then it must be a double-length DES key.

When specifying Key Block fields for the derived key, the following values should be used:

Field	Value
Key Usage	'B1': IKEY – DUKPT Initial Key.
Algorithm	'T2': double length DES key. 'A1': 128-bit AES key. 'A2': 192-bit AES key. 'A3': 256-bit AES key.
Mode of Use	'B': Both encrypt and decrypt operations. 'D': Decrypt operations only. 'E': Encrypt operations only. 'N': No special restrictions apply.
Key Version Number	'00' – '99'.
Exportability	'N': Non-exportable by the receiver of the key block, or from storage. 'E': Exportable under a KEK in a form meeting the requirements of X9.24 Parts 1 or 2. 'S': Exportable under a KEK in a form not necessarily meeting the requirements of X9.24 Parts 1 or 2.

Notes for ZKA
derivation

The ZKA Master Key must be a double-length DES key or a 256-bit AES key, and any derived key will be of the same algorithm & size as the master key. The derived key may be a ZPK, ZAK or ZEK.

When specifying Key Block fields for the derived key, the following values should be used, but refer to the "ZKA Option" field for full details.

Field	Value
Key Usage	'72': ZPK – Zone PIN Key '22': ZEK – Zone Encryption Key 'M3', 'M6': ZAK – Zone Authentication Key
Algorithm	'T2': double length DES key 'A3': 256-bit AES key
Mode of Use	If RNDI is supplied: For a ZPK: 'D': Decrypt operations only For a ZEK: 'D': Decrypt operations only For a ZAK: 'V': Verify operations only If RNDI is not supplied: For a ZPK: 'E': Encrypt operations only For a ZEK: 'E': Encrypt operations only For a ZAK: 'G': Generate operations only
Key Version Number	'00' – '99'.
Exportability	'N': Non-exportable by the receiver of the key block, or from storage. 'E': Exportable under a KEK in a form meeting the requirements of X9.24 Parts 1 or 2. 'S': Exportable under a KEK in a form not necessarily meeting the requirements of X9.24 Parts 1 or 2.

Notes for Italian derivation

This scheme is only compatible with a Key Block LMK. Both the master key and the derived key will use the DES/3DES algorithm. The length of the master key can be single, double or triple length. The length of the derived key can be single, double or triple length, but must not be greater than the length of the master key. The length of the Derivation Data fields depend on the length of the key being derived and the Derivation Mode, as shown in the two tables below:

ECB	Derivation Data Length #1	Derivation Data Length #2	Derivation Data Length #3
Single	8	0	0
Double	8	8	0
Triple	8	8	8

CBC	Derivation Data Length #1	Derivation Data Length #2	Derivation Data Length #3
Single	Multiple of 8	0	0
Double	Multiple of 8	Multiple of 8	0
Triple	Multiple of 8	Multiple of 8	Multiple of 8

When specifying Key Block fields for the derived key, the following values should be used:

Field	Value
Key Usage	'23': TEK – Data Encryption Key '58': SPKC – Session PKC
Algorithm	'D1': single length DES key. 'T2': double length DES key. 'T3': triple length DES key.
Mode of Use	'B': Both encrypt and decrypt operations. 'D': Decrypt operations only. 'E': Encrypt operations only.
Key Version Number	'00' – '99'.
Exportability	'N': Non-exportable by the receiver of the key block, or from storage. 'E': Exportable under a KEK in a form meeting the requirements of X9.24 Parts 1 or 2.

Variant LMK	Key Block LMK
Authorization: This command examines the 'Generate' flag of the given key type within the Key Type Table (see the <i>payShield 10K Host Programmer's manual</i>) to determine the authorization requirement. If the flag is 'A', the HSM must either be in the Authorized State, or the activity generate.{key}.host must be authorized, where 'key' is the key type code of the key being generated.	When using a Key Block LMK, no specific authorization is required.

Field	Length & Type	Details															
COMMAND MESSAGE																	
Message Header	m A	Subsequently returned to the Host unchanged.															
Command Code	2 A	Value 'A0'.															
Mode	1 H	Indicates the operation of the function: 'A': Derive key															
Key Type	3 H	<p>For a Variant LMK:</p> <p>Indicates the key type of the key to be derived.</p> <p>A list of possible values is listed below:</p> <table border="1"> <thead> <tr> <th>Key Type</th> <th>Description</th> <th>Derive Key Mode</th> </tr> </thead> <tbody> <tr> <td>302</td> <td>IKEY</td> <td>0 (DUKPT)</td> </tr> <tr> <td>001</td> <td>ZPK</td> <td>1 (ZKA)</td> </tr> <tr> <td>008</td> <td>ZAK</td> <td>1 (ZKA)</td> </tr> <tr> <td>00A</td> <td>ZEK</td> <td>1 (ZKA)</td> </tr> </tbody> </table>	Key Type	Description	Derive Key Mode	302	IKEY	0 (DUKPT)	001	ZPK	1 (ZKA)	008	ZAK	1 (ZKA)	00A	ZEK	1 (ZKA)
Key Type	Description	Derive Key Mode															
302	IKEY	0 (DUKPT)															
001	ZPK	1 (ZKA)															
008	ZAK	1 (ZKA)															
00A	ZEK	1 (ZKA)															
Key Scheme (LMK)	1 A	<p>For a Key Block LMK:</p> <p>This field is ignored; should be set to 'FFF'.</p>															
Derive Key Mode	1 A	<p>Indicates the operation to derive an encryption key:</p> <p>'0': DUKPT - Derive IKEY from DUKPT Master Key Type '1': ZKA – Derive ZKA key from ZKA Master Key '2': Italian – Derive TEK from MKPOS/MKSER Master Key</p>															
This section applies only when Derive Key Mode = '0':																	
DUKPT Master Key Type	1 H	<p>Only present if Derive Key Mode = '0'.</p> <p>For a Variant LMK:</p> <p>This field indicates the DUKPT Master Key Type for deriving the initial device key:</p> <p>'1': BDK-1 '2': BDK-2 '3': BDK-3 '4': BDK-4 '5': BDK-5</p>															
DUKPT Master Key	'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>For a Key Block LMK:</p> <p>This field is ignored, but must be set to '1' – '5'.</p> <p>Only present if Derive Key Mode = '0'.</p> <p>The DUKPT Master Key (BDK).</p> <p>For a Variant LMK:</p> <p>If DUKPT Master Key Type = '1': BDK-1 encrypted under LMK 28/29</p> <p>If DUKPT Master Key Type = '2': BDK-2 encrypted under LMK 28/29 variant 6</p> <p>If DUKPT Master Key Type = '3': BDK-3 encrypted under LMK 28/29 variant 8</p> <p>If DUKPT Master Key Type = '4': BDK-4 encrypted under LMK 28/29 variant 9</p> <p>If DUKPT Master Key Type = '5': BDK-5 not supported using a Variant LMK</p> <p>For a Key Block LMK, the BDK must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'B0', '41', '42', '43', '44'</td> <td>'T', 'A'</td> <td>'X', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'B0', '41', '42', '43', '44'	'T', 'A'	'X', 'N'									
Key Usage	Algorithm	Mode of Use															
'B0', '41', '42', '43', '44'	'T', 'A'	'X', 'N'															
KSN	15 H or 16 H	<p>Only be present if Derive Key Mode = '0'.</p> <p>A Key Set Identifier and Device ID for deriving the Initial Key. Right justified and padded with 'F's. (NOTE: there is no Transaction Counter, as there would be with a KSN sent in transaction data from a terminal.)</p> <p>For a 3DES BDK except BDK5, the KSN is 15 H.</p> <p>Example: For a KSI + DID of 303950 + 12342468 (14 hex characters), the KSN field would be "F30395012342468". The last hex character (8) must be even.</p>															

Field	Length & Type	Details
		For an AES BDK and a 3DES BDK5, the KSN is 16 H. AES Example: For BDK ID + DID of 30395059 + 12345678 (16 hex characters), the KSN field would be 3039505912345678. There is no need for the last character to be even. See the <i>Host Programmer's manual</i> for further information.
This section applies only when Derive Key Mode = '1':		
ZKA Master Key Type	3 H	Only present if Derive Key Mode = '1'. For a Variant LMK: Indicates the LMK pair/variant under which the ZKA Master Key is encrypted: 607 : Master Key is encrypted under LMK pair 24-25/6
		For a Key Block LMK: This field is ignored; should be set to 'FFF'
ZKA Master Key	32 H or 'U' + 32 H	Only present if Derive Key Mode = '1'. The ZKA Master Key must either be a double-length DES key or a 256-bit AES key. For the Acquirer, this is the Acquirer Master Key. For the NSP, this is the Communication Link Key.
	or 'S' + n A	For a Variant LMK, the ZKA Master Key is encrypted under the LMK pair/variant indicated by the ZKA Master Key Type field.
ZKA Option	1 H	Only present if Derive Key Mode = '1'. <u>Options for NSP when using TDES:</u> '0': Derive one of the following NSP TDES "receive" keys using supplied RNDI : <ul style="list-style-type: none">• PIN Decryption Key (Key Usage="72", Mode Of Use="D")• Data Decryption Key (Key Usage="22", Mode Of Use="D")• MAC Verification Key (Key Usage="M3", Mode Of Use="V") '1': Derive one of the following NSP TDES "send" keys using new RNDI: <ul style="list-style-type: none">• PIN Encryption Key (Key Usage="72", Mode Of Use="E")• Data Encryption Key (Key Usage="22", Mode Of Use="E")• MAC Generation Key (Key Usage="M3", Mode Of Use="G") <u>Options for the Acquirer when using AES:</u> <i>Note that for these options:</i> <ul style="list-style-type: none">• the Acquirer is restricted to supporting "receive request" messages and "send response" messages only.• for the "send response" message, derivation of a PIN Encryption Key is NOT permitted.• the Network Operator IDNO is required to be supplied for these options. '2': Derive one of the following Acquirer AES "receive request" keys using Network Operator ID _{NO} and supplied RNDI: <ul style="list-style-type: none">• PIN Decryption Key (Key Usage="72", Mode Of Use="D")• Data Decryption Key (Key Usage="22", Mode Of Use="D")• MAC Verification Key (Key Usage="M6", Mode Of Use="V") '5': Derive one of the following Acquirer AES "send response" keys using Network Operator ID _{NO} and new RNDI: <ul style="list-style-type: none">• Data Encryption Key (Key Usage="22", Mode Of Use="E")• MAC Generation Key (Key Usage="M6", Mode Of Use="G") <u>Options for the NSP when using AES:</u> <i>Note that for these options:</i> <ul style="list-style-type: none">• the NSP is restricted to supporting "send request" messages and "receive response" messages only.• derivation of a PIN decryption key is NOT permitted for "receive response" messages.• the Network Operator IDNO is NOT required to be supplied for these options. '7': Derive one of the following NSP AES "send request" keys using new RNDI: <ul style="list-style-type: none">• PIN Encryption Key (Key Usage="72", Mode Of Use="E")• Data Encryption Key (Key Usage="22", Mode Of Use="E")• MAC Generation Key (Key Usage="M6", Mode Of Use="G")

Field	Length & Type	Details						
ZKA RNDI	32 H	'8': Derive one of the following NSP AES "receive response" keys using supplied RNDI: <ul style="list-style-type: none"> • Data Decryption Key (Key Usage="22", Mode Of Use="D") • MAC Verification Key (Key Usage="M6", Mode Of Use="V") Only present for "receive" key operations i.e. if ZKA Option = '0', '2' or '8'. Random Number Input used to derive the PAC/MAC/DE key from the ZKA Master Key.						
Network Operator ID _{NO}	32 H	Only present for the Acquirer i.e. if ZKA Option = '2' or '5'. Network Operator ID _{NO} padded to 16 bytes.						
This section applies only when Derive Key Mode = '2'.								
Derivation Mode	1 N	Derivation mode: '0': ECB mode '1': CBC mode						
MKPOS/MKSER	'S' + n A	For a Key Block LMK, the 'MKPOS/MKSER' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'56', '57'</td> <td>'D', 'T'</td> <td>'X', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'56', '57'	'D', 'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'56', '57'	'D', 'T'	'X', 'N'						
Derivation Data Length #1	3 N	Length of following field. Must be > 0. If Derivation Mode = '0' (ECB), this field must = '008' If Derivation Mode = '1' (CBC), this field must be divisible by 8.						
Derivation Data #1	n B	Derivation data #1.						
IV #1	8 B	Only present if Derivation Mode = '1' (CBC). Initialisation vector #1.						
Derivation Data Length #2	3 N	Length of following field. If '000', the following two fields should not be present. If Derivation Mode = '0' (ECB), this field must = '008' If Derivation Mode = '1' (CBC), this field must be divisible by 8.						
Derivation Data #2	n B	Derivation data #2.						
IV #2	8 B	Only present if Derivation Mode = '1' (CBC). Initialisation vector #2.						
Derivation Data Length #3	3 N	Length of following field. If '000', the following two fields should not be present. If Derivation Mode = '0' (ECB), this field must = '008' If Derivation Mode = '1' (CBC), this field must be divisible by 8.						
Derivation Data #3	n B	Derivation data #3.						
IV #3	8 B	Only present if Derivation Mode = '1' (CBC). Initialisation vector #3.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						

Field	Length & Type	Details
The following section applies only when deriving a key in key block format		
Delimiter	1 A	Value '#'. Required when generating a key block. If present, the following fields must also be present.
Key Usage	2 A	<p>Key Usage field, to be included in the key block header; must be present if the above Delimiter is present. For a list of possible values, see <i>Available Key Types/Usages</i> (p.37).</p> <p>Permitted values for deriving keys from a DUKPT Master Key (BDK) are: 'B1' (IKEY)</p> <p>Permitted values for deriving keys from a ZKA Master Key are: '72' (ZPK) 'M3', 'M6' (ZAK) '22' (ZEK)</p> <p>Permitted values for deriving keys from an Italian Master Encryption Derivation Key (MKPOS/MKSER) are: '23' (TEK)</p> <p>Permitted values for deriving keys from an Italian Master PIN Derivation Key (MKPKC) are: '58' (SPKO)</p>
Algorithm	2 A	<p>Algorithm and key length; the first character will be included in the algorithm field in the key block header (byte 7); must be present if the above Delimiter is present; permitted values:</p> <p>'D1' – single length DES key 'T2' – double length DES key 'T3' – triple length DES key 'A1' – 128-bit AES key 'A2' – 192-bit AES key 'A3' – 256-bit AES key</p> <p>Note: Refer to the tables at the start of this command description for the appropriate values.</p>
Mode of Use	1 A	<p>Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i>.</p> <p>Note: Refer to the tables at the start of this command description for the appropriate values.</p>
Key Version Number	2 N	<p>Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.</p> <p>Note: Refer to the tables at the start of this command description for the appropriate values.</p>
Exportability	1 A	<p>Exportability field, to be included in the key block header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in the <i>payShield 10K Host Programmer's manual</i>.</p> <p>Note: Refer to the tables at the start of this command description for the appropriate values.</p>
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04' to X'FF'; if value = X'04', then the following field is not present.
Optional Block Data	n A	Optional block data.
The following section applies only when generating a variant key, and exporting to TR-31 format		
Delimiter	1 A	Value '&'. Optional; can only be present when the generated key is to be exported; if present, the following fields must also be present.
Key Usage	2 A	Key Usage field, to be included in the key block header; must be present if the above Delimiter is present. May be any TR-31 permitted value for the key type; For a list of possible values, see the <i>payShield 10K Host Programmer's manual</i> .
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present.

Field	Length & Type	Details
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; only permitted value is "N" or "S"; must be present if the above Delimiter is present.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '02'; must be present if the above Delimiter is present. (Note: only "KS" and "KV" Optional Blocks are valid.)
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'A1'.
Error Code	2 A	'00': No error '07': Invalid ZKA Master Key Type '10': ZMK or TMK Parity error '52': Invalid Derivation Mode '55': Invalid Derivation Data Length #1 '56': Invalid Derivation Data Length #2 '57': Invalid Derivation Data Length #3 '68': Command disabled or a standard error code.
Key (under LMK)	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The new key, encrypted under the LMK. For a Variant LMK, the 'Key (under LMK)' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'. For a Key Block LMK, the 'Key (under LMK)' will be encrypted under the LMK.
Key Check Value	6 H	The key check value.
ZKA RNDI	32 H	Only present if ZKA Option = '1', '5' and '7'. Newly generated RNDI which was used to derive the PAC/MAC/DE key from the ZKA Master Key
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Derive & Export a Key

Variant LMK	Key Block LMK
Available in package(s): Classic & Premium	
Variant LMK	Authorization: Determined by KTT(G&E) Activities: generate.{key}.host and export.{key}.host
Key Block LMK	Authorization: If export to non-KB Activity: export.{key}.host

Function:

To derive a key and return it encrypted under the LMK and under a ZMK or TMK (for transmission to another party) or encrypted under the Update Key of a BDK (for transmission to a terminal).

The following derivation methods are supported:

- Derivation of an Initial Key (IKEY) for the DUKPT scheme.
- Derivation of a ZPK/ZAK/ZEK for the ZKA scheme.

Notes for DUKPT derivation

If the BDK is a BDK1, BDK2 or BDK4, then it can be a double-length DES key or a 128/192/256-bit AES key.

If the BDK is a BDK3 or BDK5, then it must be a double-length DES key.

When specifying Key Block fields for the derived key, the following values should be used:

Field	Value
Key Usage	'B1': IKEY – DUKPT Initial Key.
Algorithm	'T2': double length DES key. 'A1': 128-bit AES key. 'A2': 192-bit AES key. 'A3': 256-bit AES key.
Mode of Use	'B': Both encrypt and decrypt operations. 'D': Decrypt operations only. 'E': Encrypt operations only. 'N': No special restrictions apply.
Key Version Number	'00' – '99'.
Exportability	'N': Non-exportable by the receiver of the key block, or from storage. 'E': Exportable under a KEK in a form meeting the requirements of X9.24 Parts 1 or 2. 'S': Exportable under a KEK in a form not necessarily meeting the requirements of X9.24 Parts 1 or 2.

Notes for ZKA derivation

The ZKA Master Key must be a double-length DES key or a 256-bit AES key, and any derived key will be of the same algorithm & size as the master key. The derived key may be a ZPK, ZAK or ZEK.

When specifying Key Block fields for the derived key, the following values should be used, but refer to the "ZKA Option" field for full details.

Field	Value
Key Usage	'72': ZPK – Zone PIN Key '22': ZEK – Zone Encryption Key 'M3', M6: ZAK – Zone Authentication Key
Algorithm	'T2': double length DES key 'A3': 256-bit AES key
Mode of Use	If RNDI is supplied: For a ZPK: 'D': Decrypt operations only For a ZEK: 'D': Decrypt operations only For a ZAK: 'V': Verify operations only If RNDI is not supplied: For a ZPK: 'E': Encrypt operations only For a ZEK: 'E': Encrypt operations only For a ZAK: 'G': Generate operations only
Key Version Number	'00' – '99'.
Exportability	'N': Non-exportable by the receiver of the key block, or from storage. 'E': Exportable under a KEK in a form meeting the requirements of X9.24 Parts 1 or 2. 'S': Exportable under a KEK in a form not necessarily meeting the requirements of X9.24 Parts 1 or 2.

Variant LMK	Key Block LMK										
<p>Authorization:</p> <p>This command examines the 'Generate' flag of the given key type within the Key Type Table (see the <i>payShield 10K Host Programmer's manual</i>) to determine the authorization requirement. If the flag is 'A', the HSM must either be in the Authorized State, or the activity generate.{key}.host must be authorized, where 'key' is the key type code of the key being generated.</p> <p>This command also examines the 'Export' flag of the given key type within the Key Type Table (see the <i>payShield 10K Host Programmer's manual</i>). If the flag is 'A', the HSM must either be in the Authorized State, or the activity export.{key}.host must be authorized, where 'key' is the key type code of the key being exported.</p>	<p>The authorization requirement for this command depends solely on the type of export being requested:</p> <table border="1"> <thead> <tr> <th>"Key Scheme (ZMK)"</th><th>Authorization</th></tr> </thead> <tbody> <tr> <td>'S' (Thales Key Block)</td><td>None</td></tr> <tr> <td>'R' (TR-31 Key Block)</td><td>None</td></tr> <tr> <td>'U', 'T' (Variant)</td><td>Required</td></tr> <tr> <td>'Z', 'X', 'Y' (X9.17)</td><td>Required</td></tr> </tbody> </table> <p>If authorization is required, the HSM must either be in the Authorized State, or the activity export.{key}.host must be authorized, where 'key' is the key usage code of the key being exported.</p>	"Key Scheme (ZMK)"	Authorization	'S' (Thales Key Block)	None	'R' (TR-31 Key Block)	None	'U', 'T' (Variant)	Required	'Z', 'X', 'Y' (X9.17)	Required
"Key Scheme (ZMK)"	Authorization										
'S' (Thales Key Block)	None										
'R' (TR-31 Key Block)	None										
'U', 'T' (Variant)	Required										
'Z', 'X', 'Y' (X9.17)	Required										

<p>Notes:</p> <p>A TMK can only export the following key types:</p> <p>If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N":</p> <ul style="list-style-type: none"> 002 (TPK or TMK) 003 (TAK) 30B (TEK) 302 (IKEY) <p>If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y":</p> <ul style="list-style-type: none"> 70D (TPK) 80D (TMK) 003 (TAK) 30B (TEK) 302 (IKEYφ) 	<p>A TMK with Key Usage = '51' can only export keyblocks with the following Key Usage values:</p> <ul style="list-style-type: none"> 'P0', '71' (TPK) 'M1', 'M3', 'M5', 'M6' (TAK) '23' (TEK) '51' (TMK) 'B1' (IKEY) <p>When exporting the new key, the ZMK (or TMK) key block must have the following field values:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #d9e1f2;">"ZMK" KB Header</th><th style="background-color: #d9e1f2;">Value(s)</th></tr> </thead> <tbody> <tr> <td>Key Usage</td><td>'K0', 'K1', '51', or '52'</td></tr> <tr> <td>Algorithm</td><td>'D'*', 'T' or 'A'</td></tr> <tr> <td>Mode of Use</td><td>'B', 'E', or 'N'</td></tr> </tbody> </table> <p>* Note: Exporting to a key block format is not permitted with a single-length ZMK or TMK.</p>	"ZMK" KB Header	Value(s)	Key Usage	'K0', 'K1', '51', or '52'	Algorithm	'D'*', 'T' or 'A'	Mode of Use	'B', 'E', or 'N'
"ZMK" KB Header	Value(s)								
Key Usage	'K0', 'K1', '51', or '52'								
Algorithm	'D'*', 'T' or 'A'								
Mode of Use	'B', 'E', or 'N'								

- Further Notes:
- Exporting to a key block format requires the ZMK/TMK to be one of the following:
 - Double or triple length DES key
 - Any size AES key

For security reasons, when using a Key Block LMK, this command will not support the export of a DEK (Key Usage = "D0" or "21") to encryption under a ZMK in variant or X9.17 format.

Field	Length & Type	Details															
COMMAND MESSAGE																	
Message Header	m A	Subsequently returned to the Host unchanged.															
Command Code	2 A	Value 'A0'.															
Mode	1 H	Indicates the operation of the function: 'B': Derive key and encrypt under ZMK (or TMK or Current BDK)															
Key Type	3 H	<p>For a Variant LMK:</p> <p>Indicates the key type of the key to be generated/derived. A list of possible values is listed below:</p> <table border="1" style="margin-left: auto; margin-right: auto; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #d9e1f2;">Key Type</th><th style="background-color: #d9e1f2;">Description</th><th style="background-color: #d9e1f2;">Derive Key Mode</th></tr> </thead> <tbody> <tr> <td>302</td><td>IKEY</td><td>0 (DUKPT)</td></tr> <tr> <td>001</td><td>ZPK</td><td>1 (ZKA)</td></tr> <tr> <td>008</td><td>ZAK</td><td>1 (ZKA)</td></tr> <tr> <td>00A</td><td>ZEK</td><td>1 (ZKA)</td></tr> </tbody> </table> <p>For a Key Block LMK:</p> <p>This field is ignored; should be set to 'FFF'.</p>	Key Type	Description	Derive Key Mode	302	IKEY	0 (DUKPT)	001	ZPK	1 (ZKA)	008	ZAK	1 (ZKA)	00A	ZEK	1 (ZKA)
Key Type	Description	Derive Key Mode															
302	IKEY	0 (DUKPT)															
001	ZPK	1 (ZKA)															
008	ZAK	1 (ZKA)															
00A	ZEK	1 (ZKA)															
Key Scheme (LMK)	1 A	Indicates the scheme for encrypting the output key under the LMK. For a list of key schemes, see the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> .															

Field	Length & Type	Details						
Derive Key Mode	1 A	Indicates the operation to derive an encryption key: '0': DUKPT - Derive IKEY from DUKPT Master Key Type '1': ZKA – Derive ZKA key from ZKA Master Key						
This section applies only when Derive Key Mode = '0':								
DUKPT Master Key Type	1 H	<p>Only present if Derive Key Mode = '0'.</p> <p>This field indicates the DUKPT Master Key Type for deriving the initial device key:</p> <ul style="list-style-type: none"> '1': BDK-1 '2': BDK-2 '3': BDK-3 '4': BDK-4 '5': BDK-5 <p>For a Key Block LMK:</p> <p>This field is ignored, but must be set to '1' – '5'.</p>						
DUKPT Master Key	'U' + 32 H or 'T' + 48 H	<p>Only present if Derive Key Mode = '0'.</p> <p>The DUKPT Master Key (BDK).</p> <p>For a Variant LMK:</p> <p>If DUKPT Master Key Type = '1': BDK-1 encrypted under LMK 28/29</p> <p>If DUKPT Master Key Type = '2': BDK-2 encrypted under LMK 28/29 variant 6</p> <p>If DUKPT Master Key Type = '3': BDK-3 encrypted under LMK 28/29 variant 8</p> <p>If DUKPT Master Key Type = '4': BDK-4 encrypted under LMK 28/29 variant 9</p> <p>If DUKPT Master Key Type = '5': BDK-5 not supported using a Variant LMK</p>						
	or 'S' + n A	<p>For a Key Block LMK, the BDK must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'B0', '41', '42', '43', '44'</td> <td>'T', 'A'</td> <td>'X', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'B0', '41', '42', '43', '44'	'T', 'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'B0', '41', '42', '43', '44'	'T', 'A'	'X', 'N'						
KSN	15 H or 16 H	<p>Only be present if Derive Key Mode = '0'.</p> <p>A Key Set Identifier and Device ID for deriving the Initial Key. Right justified and padded with 'F's. (NOTE: there is no Transaction Counter, as there would be with a KSN sent in transaction data from a terminal.)</p> <p>For a 3DES BDK except BDK5, the KSN is 15 H.</p> <p>Example: For a KSI + DID of 303950 + 12342468 (14 hex characters), the KSN field would be "F30395012342468". The last hex character (8) must be even.</p> <p>For an AES BDK and a 3DES BDK5, the KSN is 16 H.</p> <p>AES Example: For BDK ID + DID of 30395059 + 12345678 (16 hex characters), the KSN field would be 3039505912345678. There is no need for the last character to be even.</p> <p>See the <i>Host Programmer's manual</i> for further information.</p>						
This section applies only when Derive Key Mode = '1':								
ZKA Master Key Type	3 H	<p>Only present if Derive Key Mode = '1'.</p> <p>For a Variant LMK:</p> <p>Indicates the LMK pair/variant under which the ZKA Master Key is encrypted: 607 : Master Key is encrypted under LMK pair 24-25/6</p>						
ZKA Master Key	32 H or 'U' + 32 H	<p>For a Key Block LMK:</p> <p>This field is ignored; should be set to 'FFF'</p> <p>Only present if Derive Key Mode = '1'.</p> <p>The ZKA Master Key must either be a double-length DES key or a 256-bit AES key.</p> <p>For the Acquirer, this is the Acquirer Master Key.</p> <p>For the NSP, this is the Communication Link Key.</p> <p>For a Variant LMK, the ZKA Master Key is encrypted under the LMK pair/variant indicated by the ZKA Master Key Type field.</p>						
	or 'S' + n A	<p>For a Key Block LMK, the ZKA Master Key must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'53'</td> <td>'T', 'A'</td> <td>'X'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'53'	'T', 'A'	'X'
Key Usage	Algorithm	Mode of Use						
'53'	'T', 'A'	'X'						

Field	Length & Type	Details
ZKA Option	1 H	<p>Only present if Derive Key Mode = '1'.</p> <p><u>Options for NSP when using TDES:</u></p> <p>'0': Derive one of the following NSP TDES "receive" keys using supplied RNDI :</p> <ul style="list-style-type: none"> • PIN Decryption Key (Key Usage="72", Mode Of Use="D") • Data Decryption Key (Key Usage="22", Mode Of Use="D") • MAC Verification Key (Key Usage="M3", Mode Of Use="V") <p>'1': Derive one of the following NSP TDES "send" keys using new RNDI:</p> <ul style="list-style-type: none"> • PIN Encryption Key (Key Usage="72", Mode Of Use="E") • Data Encryption Key (Key Usage="22", Mode Of Use="E") • MAC Generation Key (Key Usage="M3", Mode Of Use="G") <p><u>Options for the Acquirer when using AES:</u></p> <p><i>Note that for these options:</i></p> <ul style="list-style-type: none"> • <i>the Acquirer is restricted to supporting "receive request" messages and "send response" messages only.</i> • <i>for the "send response" message, derivation of a PIN Encryption Key is NOT permitted.</i> • <i>the Network Operator IDNO is required to be supplied for these options.</i> <p>'2': Derive one of the following Acquirer AES "receive request" keys using Network Operator ID_{NO} and supplied RNDI:</p> <ul style="list-style-type: none"> • PIN Decryption Key (Key Usage="72", Mode Of Use="D") • Data Decryption Key (Key Usage="22", Mode Of Use="D") • MAC Verification Key (Key Usage="M6", Mode Of Use="V") <p>'5': Derive one of the following Acquirer AES "send response" keys using Network Operator ID_{NO} and new RNDI:</p> <ul style="list-style-type: none"> • Data Encryption Key (Key Usage="22", Mode Of Use="E") • MAC Generation Key (Key Usage="M6", Mode Of Use="G") <p><u>Options for the NSP when using AES:</u></p> <p><i>Note that for these options:</i></p> <ul style="list-style-type: none"> • <i>the NSP is restricted to supporting "send request" messages and "receive response" messages only.</i> • <i>derivation of a PIN decryption key is NOT permitted for "receive response" messages.</i> • <i>the Network Operator IDNO is NOT required to be supplied for these options.</i> <p>'7': Derive one of the following NSP AES "send request" keys using new RNDI:</p> <ul style="list-style-type: none"> • PIN Encryption Key (Key Usage="72", Mode Of Use="E") • Data Encryption Key (Key Usage="22", Mode Of Use="E") • MAC Generation Key (Key Usage="M6", Mode Of Use="G") <p>'8': Derive one of the following NSP AES "receive response" keys using supplied RNDI:</p> <ul style="list-style-type: none"> • Data Decryption Key (Key Usage="22", Mode Of Use="D") • MAC Verification Key (Key Usage="M6", Mode Of Use="V") <p>Only present for "receive" key operations i.e. if ZKA Option = '0', '2' or '8'. Random Number Input used to derive the PAC/MAC/DE key from the ZKA Master Key.</p>
Network Operator ID _{NO}	32 H	Only present for the Acquirer i.e. if ZKA Option = '2' or '5'. Network Operator ID _{NO} padded to 16 bytes.
Delimiter	1 A	Value ';'. Optional. If present, the following field must also be present.
ZMK/TMK Flag	1 N	Optional. Only present if the above delimiter is present. '0': ZMK (default value if these fields are not present) '1': TMK

Field	Length & Type	Details									
ZMK (or TMK or Current BDK)		<p>The Zone Master Key (or Terminal Master Key or Current Base Derivation Key). For a ZMK, the length of the key must correspond to the ZMK key length as defined in the Security Settings.</p> <p>If Derive Key Mode = '0' (DUKPT – Derive IPEK from DUKPT Master Key), then this field may be used to supply the terminal's Current BDK. In this case, this command will encrypt the IPEK derived from the DUKPT Master Key under the Update Key derived from the Current BDK (as defined in X9.24-3).</p>									
	16 / 32 H or 'U' + 32 H or 'T' + 48 H	For a Variant LMK, the 'ZMK' is encrypted under LMK pair 04-05. The 'TMK' is encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 8 if the setting has the value "Y".									
	or 'S' + n A	For a Key Block LMK, the 'ZMK (or TMK)' must comply with the following:									
		<table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'K0', 'K1', '51', '52'</td><td>'D', 'T', 'A'</td><td>'B', 'E', 'N'</td></tr> <tr> <td>'B0', '41', '43'</td><td>'A'</td><td>'X', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'K0', 'K1', '51', '52'	'D', 'T', 'A'	'B', 'E', 'N'	'B0', '41', '43'	'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use									
'K0', 'K1', '51', '52'	'D', 'T', 'A'	'B', 'E', 'N'									
'B0', '41', '43'	'A'	'X', 'N'									
Current BDK's Initial Key Serial Number	16 H	The key serial number of the current BDK. Only present if using a current BDK.									
Key Scheme (ZMK or TMK or Current BDK)	1 A	Indicates the scheme for encrypting the key under the ZMK (or TMK or Current BDK). For a list of key schemes, see the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> .									
Atalla Variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.									
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.									
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.									

Field	Length & Type	Details
The following section applies only when deriving & exporting in key block format		
Delimiter	1 A	Value '#'. Required when generating a key block. If present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the key block header; must be present if the above Delimiter is present. For a list of possible values, see <i>Available Key Types/Usages</i> (p.37). Permitted values for deriving keys from a ZKA Master Key are: '72' (ZPK) 'M3', 'M6' (ZAK) '22' (ZEK)
Algorithm	2 A	Algorithm and key length; the first character will be included in the algorithm field in the key block header (byte 7); must be present if the above Delimiter is present; permitted values: 'D1' – single length DES key 'T2' – double length DES key 'T3' – triple length DES key 'A1' – 128-bit AES key 'A2' – 192-bit AES key 'A3' – 256-bit AES key Note: for keys derived using the ZKA process, this field must match the algorithm & size of the ZKA Master Key.
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in the <i>payShield 10K Host Programmer's manual</i> .
This section specifies the optional blocks to be included in both the derived key block and the exported key block.		
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier. Valid values include: 'KS', 'KV', '00' – '05'
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
This section specifies the optional blocks to be included in the exported TR-31 key block (only).		
Delimiter	1 A	Value '\$'. Optional; only present if exporting in TR-31 format.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; must be present if the above Delimiter is present. Permitted values: '00' to '99'. Note this is reduced if Optional Blocks KS and/or KV are specified to be included as given above.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; to be included only in the exported TR-31 key block header. Valid values include: 'KS', 'KV', 'KC', 'KP', 'IK', 'TS' and '00' – '99'. Note: 'KS' and 'KV' can only be added if they are not already included in Thales Key Block - otherwise a "Repeated optional block ID" error is given.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
Delimiter	1 A	Value '&'. Optional; can only be present when the generated key is to be exported; if present, the following field must also be present.
Modified Export Value	1 A	Character to be placed in the exportability field (byte 11) of the exported key; only permitted value = "N"; must be present if the above Delimiter is present.

Delimiter	1 A	Value '!'. Optional; can only be present when the generated key is to be exported in TR-31 key block format. If present, the following field must be present.
Key Block Version ID	1 A	<p>Key Block Version ID:</p> <p>'A': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'B': Key block protected using the Key Derivation Binding Method (see Ref 8 §5.3.2.1) 'C': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'D': Key block protected using the AES Key Derivation Binding Method (see Ref 8 §5.3.2.3).</p>
The following section applies only when generating a variant key, and exporting to TR-31 format		
Delimiter	1 A	Value '&'. Optional; can only be present when the generated key is to be exported; if present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the key block header; must be present if the above Delimiter is present. May be any TR-31 permitted value for the key type; For a list of possible values, see the <i>payShield 10K Host Programmer's manual</i> .
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present.
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; only permitted value is "N" or "S"; must be present if the above Delimiter is present.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '99'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier. Valid values include: 'KS', 'KV', 'KC', 'KP', 'IK', 'TS' and '00' – '99'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
Delimiter	1 A	Value '!'. Optional; can only be present when the generated key is to be exported to TR-31 key block format. If present, the following field must be present.
Key Block Version ID	1 A	<p>Key Block Version ID:</p> <p>'A': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'B': Key block protected using the Key Derivation Binding Method (see Ref 8 §5.3.2.1) 'C': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'D': Key block protected using the AES Key Derivation Binding Method (see Ref 8 §5.3.2.3).</p>
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'A1'.
Error Code	2 A	'00': No error '07': Invalid ZKA Master Key Type '10': ZMK or TMK Parity error 'BC': Repeated optional block ID '68': Command disabled or a standard error code.
Key (under LMK)	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The new key, encrypted under the LMK. For a Variant LMK, the 'Key (under LMK)' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'.
Key (under ZMK or TMK or Current BDK)	16 H or 'U' + 32 H or 'T' + 48 H or 'R' + n A or 'S' + n A	For a Key Block LMK, the 'Key (under LMK)' will be encrypted under the LMK. The new key, encrypted under the supplied ZMK (or TMK or Current BDK).
Key Check Value	6 H	The key check value.
ZKA RNDI	32 H	Only present if ZKA Option = '1', '5' and '7'. Newly generated RNDI which was used to derive the PAC/MAC/DE key from the ZKA Master Key
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate and Print a Component

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Required	
Activity: genprint.{key}.host	

Function:

Generate a random component, print it at the HSM attached printer and return the encrypted value to the host.

	Variant LMK	Key Block LMK
Authorization:	The HSM must either be in the Authorized State, or the activity genprint.{key}.host must be authorized, where 'key' is the key type code of the key component being generated. For a list of possible values, see <i>Available Key Types/Usages</i> (p.37).	The HSM must either be in the Authorized State, or the activity genprint.{key}.host must be authorized, where 'key' is the key usage of the key block component being generated. For a list of possible values, see <i>Available Key Types/Usages</i> (p.37).
Notes:		In practice, the Number of Optional Blocks field in the component key block should be set to '00', since any such fields are discarded when the key block is formed (e.g. using command 'A4').

A printer must be attached to one of the USB ports on the payShield 10K. Serial-to-USB and parallel-to-USB cables are available from Thales, on request.

The HSM must have a Print Format already defined. Refer to the section on Key Component Printing in the *payShield 10K Host Programmer's Manual* for more details.

The sequence "**^P**" (without quotes) specifies the location of where the plaintext component should be printed.

^T in the Print Format denotes a key check value.

This command supports printing key components on a single line, or on multiple lines, as controlled by the Print Option field.

Print Option	Format of printed output
Not specified	All key component hex characters on a single line
'01'	Up to 16 hex characters per line
'02'	Up to 32 hex characters per line

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'A2'.
Key Type	3 H	For a Variant LMK: Indicates the key type of the component to be generated. For a list of possible values, see Key Type Codes in the <i>payShield 10K Host Programmer's manual</i> and <i>Available Key Types/Usages</i> (p. 37).

Field	Length & Type	Details
Component Check Flag	1 A	For a Key Block LMK: This field is ignored; should be set to 'FFF'. Optional. If present, indicates whether the response should include a check value for the component: '1': Do not return component check value. '2': Return component check value. If not present, this field assumes the value of '1'.
Delimiter	1 A	Value '\$'. Optional; if present, the Print Options field below must be specified.
Print Options	2 A	'01' - Print component with a maximum of 16 hex characters per line, representing 8 bytes / 64 bits '02' - Print component with a maximum of 32 hex characters per line, representing 16 bytes / 128 bits
Key Scheme (LMK)	1 A	Indicates the scheme for encrypting the key under the LMK. For a list of key schemes, see the Key Scheme Table can be found in the <i>payShield 10K Host Programmer's manual</i> .
Print Field 0	n A	The print field defined as Print Field 0 in the print format definition (must not contain a ';' character).
Delimiter	1 A	Value ':'.
Print Field 1	n A	The print field defined as Print Field 1 in the print format definition (must not contain a ';' character).
...
...
Last print field	n A	The last print field defined in the print format definition (must not contain a ';' or '~' character).
Delimiter	1 A	Value '~'. Value must be present if either the '%' or '#' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.

The following section applies only when generating components in key block format

Delimiter	1 A	Value '#'. Required when generating a key block component. If present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the key block header; must be present if the above Delimiter is present. For a list of possible values, see the <i>payShield 10K Host Programmer's manual</i> .
Algorithm	2 A	Algorithm and key length; the first character will be included in the algorithm field in the key block header (byte 7); must be present if the above Delimiter is present; permitted values: 'D1' – single length DES key 'T2' – double length DES key 'T3' – triple length DES key 'A1' – 128-bit AES key 'A2' – 192-bit AES key 'A3' – 256-bit AES key
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: 'c0' to 'c9'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in the <i>payShield 10K Host Programmer's manual</i> .
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '06'; must be present if the above Delimiter is present.

For each optional block, the following three fields must be specified.

Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.

Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except '03', '04' and 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19'.

payShield 10K Core Host Commands

Field	Length & Type	Details
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (before printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'A3'.
Error Code	2 A	'00': No Error '68': Command disabled or a standard error code.
Component	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The new component, encrypted under the LMK. For a Variant LMK, the 'Component' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'. For a Key Block LMK, the 'Component' will be encrypted under the LMK.
Component Check Value	6 H	The check value of the component. Present only if Component Check Flag = '2'.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (after printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'AZ'.
Error Code	2 A	'00': No error '16': Printer not ready/disconnected '41': Internal hardware/software error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.

Generate and Print a Key as Split Components

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Required	
Activity: genprint.{key}.host	

Function:

Generate a random key, print it as two half components or three third components at the HSM attached printer, and return it encrypted under the appropriate LMK.

Variant LMK	Key Block LMK
Authorization: The HSM must either be in the Authorized State, or the activity genprint.{key}.host must be authorized, where 'key' is the key type code of the key/component being generated. For a list of possible values, see <i>Available Key Types/Usages</i> (p.37).	The HSM must either be in the Authorized State, or the activity genprint.{key}.host must be authorized, where 'key' is the key usage of the key block/component being generated. For a list of possible values, see <i>Available Key Types/Usages</i> (p.37).

Notes:

A printer must be attached to one of the USB ports on the payShield 10K, Serial-to-USB and parallel-to-USB cables are available from Thales, on request.

The HSM must have a print format already defined.

For a single length key, the key is split into two 8 character values. ^P and ^Q in the print format denote the left and right halves respectively.

For a double length key, ^P and ^Q in the print format denote the first and second key respectively.

For a triple length key, ^P, ^Q and ^R in the print format denote the first, second and third key respectively.

^T in the print format denotes a key check value.

payShield 10K Core Host Commands

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'NE'.
Key Type	3 H	<p>For a Variant LMK:</p> <p>Indicates the key type of the key to be generated. For a list of possible values, see Key Type Codes in the <i>payShield 10K Host Programmer's manual</i> and <i>Available Key Types/Usages</i> (p. 37).</p> <p>For a Key Block LMK:</p> <p>This field is ignored; should be set to 'FFF'.</p>
Key Scheme (LMK)	1 A	Indicates the scheme for encrypting the key under the LMK. For a list of key schemes, see the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> .
Print Field 0	n A	The print field defined as Print Field 0 in the print format definition (must not contain a ';' character).
Delimiter	1 A	Value '~'.
Print Field 1	n A	The print field defined as Print Field 1 in the print format definition (must not contain a ';' character).
...
Last print field	n A	The last print field defined in the print format definition (must not contain a ';' or '~' character).
Delimiter	1 A	Value '~'. Optional; must be present if either the '%' or '#' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
The following section applies only when generating components in key block format		
Delimiter	1 A	Value '#'. Required when generating a key block. If present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the key block header; must be present if the above Delimiter is present. For a list of possible values, see the <i>payShield 10K Host Programmer's manual</i> .
Algorithm	2 A	Algorithm and key length; the first character will be included in the algorithm field in the key block header (byte 7); must be present if the above Delimiter is present; permitted values: 'D1' – single length DES key 'T2' – double length DES key 'T3' – triple length DES key 'A1' – 128-bit AES key 'A2' – 192-bit AES key 'A3' – 256-bit AES key
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the key block header; any permitted values; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in the <i>payShield 10K Host Programmer's manual</i> .
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (before printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'NF'.
Error Code	2 A	'00': No error '16': Printer not ready/not connected '18': Format definition not loaded '68': Command disabled or a standard error code.
Key	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The new key, encrypted under the LMK. For a Variant LMK, the 'Key' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'. For a Key Block LMK, the 'Key' will be encrypted under the LMK.
Key Check Value	6 H	The key check value.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (after printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'NZ'.
Error Code	2 A	'00': No error '16': Printer not ready/disconnected '41': Internal hardware/software error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.

Form a Key from Encrypted Components

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Required	
Activity: component.{key}.host	

Function:

To form a key from encrypted components.

	Variant LMK	Key Block LMK
Authorization:	The HSM must either be in the Authorized State, or the activity component.{key}.host must be authorized, where 'key' is the key type code of the key being formed. For a list of possible values, see <i>Available Key Types/Usages</i> (p.37).	The HSM must either be in the Authorized State, or the activity component.{key}.host must be authorized, where 'key' is the key usage of the key block being formed. For a list of possible values, see <i>Available Key Types/Usages</i> (p.37).
Notes:		<p>The Key Usage, Mode of Use, Algorithm and Exportability fields specified after the '#' delimiter must match the corresponding values in all component keyblocks.</p> <p>Any optional blocks specified after the '#' delimiter will be used in constructing the new key. Optional blocks contained in the component keyblocks will be discarded.</p>

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'A4'.
Number of components	1 N	The number of supplied components. Range: '2' – '9'.
Key Type	3 H	<p>For a Variant LMK:</p> <p>Indicates the key type of the key to be generated. For a list of possible values, see <i>Key Type Codes</i> in the <i>payShield 10K Host Programmer's manual</i> and <i>Available Key Types/Usages</i>.</p> <p>For a Key Block LMK:</p> <p>This field is ignored; should be set to 'FFF'.</p>
Key Scheme (LMK)	1 A	Indicates the scheme for encrypting the key under the LMK. For a list of key schemes, see the <i>Key Scheme Table</i> in the <i>payShield 10K Host Programmer's manual</i> .
Key Component 1	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	Encrypted key component 1.
Key Component 2	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	Encrypted key component 2.
...

payShield 10K Core Host Commands

Key Component n	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	Encrypted key component n.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
The following section applies only when combining components in key block format		
Delimiter	1 A	Value '#'. Required when forming a key block. If present, the following fields must be present.
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'A5'.
Error Code	2 A	'00': No error '03': Invalid number of components '10': Component parity error '68': Command disabled or a standard error code.
Key (under LMK)	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The formed key, encrypted under the LMK. For a Variant LMK, the 'Key (under LMK)' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'.
Key Check Value	6 H	The key check value.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Import a Key

Variant LMK	Key Block LMK
Available in package(s): Classic & Premium	
Variant LMK	Authorization: Determined by KTT(I) Activities: import.{key}.host
Key Block LMK	Authorization: If import from non-KB Activity: import.{key}.host

Function: To import a key encrypted under a ZMK.

Variant LMK	Key Block LMK												
Authorization: This command examines the 'Import' flag of the given key type within the Key Type Table (see the <i>payShield 10K Host Programmer's manual</i>) to determine the authorization requirement. If the flag is 'A', the HSM must either be in the Authorized State, or the activity import.{key}.host must be authorized, where 'key' is the key type code of the key being imported.	The authorization requirement for this command depends on the type of import being requested: <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #d9eaf7;">Scheme of "Key (ZMK)"</th><th style="background-color: #d9eaf7;">Auth</th></tr> </thead> <tbody> <tr> <td>'S' (Thales Key Block)</td><td>None</td></tr> <tr> <td>'R' (TR-31 Key Block)</td><td>None</td></tr> <tr> <td>'U', 'T' (Variant)</td><td>Required</td></tr> <tr> <td>'Z', 'X', 'Y' (X9.17)</td><td>Required</td></tr> <tr> <td>'M', 'O' (CBC mode)</td><td>Required</td></tr> </tbody> </table> If authorization is required, the HSM must either be in the Authorized State, or the activity import.{key}.host must be authorized, where 'key' is the key usage code of the key being imported.	Scheme of "Key (ZMK)"	Auth	'S' (Thales Key Block)	None	'R' (TR-31 Key Block)	None	'U', 'T' (Variant)	Required	'Z', 'X', 'Y' (X9.17)	Required	'M', 'O' (CBC mode)	Required
Scheme of "Key (ZMK)"	Auth												
'S' (Thales Key Block)	None												
'R' (TR-31 Key Block)	None												
'U', 'T' (Variant)	Required												
'Z', 'X', 'Y' (X9.17)	Required												
'M', 'O' (CBC mode)	Required												
Notes: 	The ZMK key block must have the following field values: <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #d9eaf7;">"ZMK" Key Block Header</th><th style="background-color: #d9eaf7;">Value(s)</th></tr> </thead> <tbody> <tr> <td>Key Usage</td><td>'K0', 'K1', '52'</td></tr> <tr> <td>Algorithm</td><td>'D'*', 'T'</td></tr> <tr> <td>Mode of Use</td><td>'B', 'D', 'N'</td></tr> </tbody> </table> * Note: Importing from a key block format is not permitted with a single-length ZMK. This command cannot be used to import a ZMK.	"ZMK" Key Block Header	Value(s)	Key Usage	'K0', 'K1', '52'	Algorithm	'D'*', 'T'	Mode of Use	'B', 'D', 'N'				
"ZMK" Key Block Header	Value(s)												
Key Usage	'K0', 'K1', '52'												
Algorithm	'D'*', 'T'												
Mode of Use	'B', 'D', 'N'												

- When importing an AES ZKA Master Key:
- the key must be supplied in TR-31 format;
 - the key must be a 256-bit AES key;
 - the key must be in TR-31 format, with Key Usage = '11';
 - the optional block 'KS' will be ignored;
 - the output key (in Thales Key Block format) will have Key Usage = '53'.

If the option "Enforce Atalla variant match to Thales key type" is set to YES in the CS console command, the following matchings between Atalla variant and Thales variant key types will be enforced:

Key Type	Atalla Variant	Thales Variant (*)	Thales Variant (°)
TPK	1 or 01	002 LMK 14-15 001 LMK 06-07	70D LMK 36-37/7 001 LMK 06-07
ZPK			
ZEK	2 or 02	00B LMK 32-33 00A LMK 30-31	00B LMK 32-33 00A LMK 30-31
TAK	3 or 03	003 LMK 16-17	003 LMK 16-17
ZAK		008 LMK 26-27	008 LMK 26-27
CVK		402 LMK 14-15/4	402 LMK 14-15/4
TMK	4 or 04	002 LMK 14-15	80D LMK 36-37/8
TPK		002 LMK 14-15	70D LMK 36-37/7
PVK		002 LMK 14-15	002 LMK 14-15
TMK	5 or 05	002 LMK 14-15	80D LMK 36-37/8
BDK-1	8 or 08	009 LMK 28-29	009 LMK 28-29
MK-AC	9 or 09	109 LMK 28-29/1	109 LMK 28-29/1
MK-SMI	9 or 09	209 LMK 28-29/2	209 LMK 28-29/2
MK-SMC	9 or 09	309 LMK 28-29/3	309 LMK 28-29/3
TEK	26	30B LMK 32-33/3	30B LMK 32-33/3
BDK-2	30	609 LMK 28-29/6	609 LMK 28-29/6
BDK-3	8 or 08	809 LMK 28-29/8	809 LMK 28-29/8
BDK-4	9 or 09	909 LMK 28-29/9	909 LMK 28-29/9
BDK-5	N/A	N/A (Key Block only)	N/A (Key Block only)

* Applies if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N"

° Applies if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y"

Further Notes: In order to import a ZMK, the following security setting must be set:

Enable import of a ZMK: Yes

For security reasons, when using a Key Block LMK, this command will not support the import of a DEK (Key Usage = "D0" or "21") in variant or X9.17 format.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'A6'.						
Key Type	3 H	<p>For a Variant LMK:</p> <p>Indicates the key type of the key to be imported. For a list of possible values, see Key Type Codes in the <i>payShield 10K Host Programmer's manual</i>.</p>						
ZMK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>For a Key Block LMK:</p> <p>This field is ignored; should be set to 'FFF'.</p> <p>The ZMK encrypted under the LMK.</p> <p>For a Variant LMK, the 'ZMK' is encrypted under LMK pair 04-05.</p> <p>For a Key Block LMK, the 'ZMK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'K0', 'K1', '52'</td> <td>'D', 'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'K0', 'K1', '52'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'K0', 'K1', '52'	'D', 'T', 'A'	'B', 'D', 'N'						
Key (ZMK)	16 H or 'U' or 'X' or 'M' + 32 H or 'T' or 'Y' or 'O' + 48 H or 'R' + n A or 'S' + n A	<p>The Key to be imported, encrypted under the ZMK. The Key can be in X9.17 (ECB), CBC, Variant, TR-31 Key Block, or Thales Key Block format.</p> <p>If in Thales or TR-31 key block format, the 'Key (ZMK)' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>Any valid value</td> <td>'D', 'T', 'A'</td> <td>Any valid value</td> </tr> </tbody> </table> <p>For a list of valid Key Usage values, refer to <i>Available Key Types/Usages</i> (p. 37). Note that CBC mode (scheme 'M' or 'O') is only available when using a 3DES ZMK.</p>	Key Usage	Algorithm	Mode of Use	Any valid value	'D', 'T', 'A'	Any valid value
Key Usage	Algorithm	Mode of Use						
Any valid value	'D', 'T', 'A'	Any valid value						
Key Scheme (LMK)	1 A	Indicates the scheme for encrypting the key under the LMK. For a list of key schemes, see the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> .						
IV	16 H	<p>Optional. Only present when 'Key (ZMK)' uses key scheme 'M' or 'O'.</p> <p>The input IV, used in conjunction with the 'ZMK'.</p> <p>For a 3DES ZMK, the IV will be a 16 H field.</p>						
Atalla Variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
The following section applies when importing keys in TR-31 format when using a Key Block LMK.								
Delimiter	1 A	Value '#'. Optional; can only be present when the key to be imported is in TR-31 key block format; if present, the following fields must be present.						
Modified Key Usage	2 A	Key Usage field, to be included in the imported key block header; must be present if the above Delimiter is present..						
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '06'; must be present if the above Delimiter is present.						
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.								
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'KS', 'KV', 'PB'.						
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.						
Optional Block Data	n A	Optional block data.						
The following section applies when importing keys in a non-key block format (e.g. X9.17) when using a Key Block LMK.								
Delimiter	1 A	Value '#'. Optional; can only be present when the key to be imported is not in a key block format; if present, the following fields must be present.						
Key Usage	2 A	Key Usage field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Key Usage Table in the <i>payShield 10K Host Programmer's manual</i> .						
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. May be any permitted value for the key type; for a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .						

Field	Length & Type	Details
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; only permitted value is 'N' or 'S'; must be present if the above Delimiter is present.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'A7'.
Error Code	2 A	'00': No error '01': Key parity error, advice only '10': ZMK Parity error '11': Imported key is all zeros '68': Command disabled or a standard error code..
Key (under LMK)	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The imported key, encrypted under the LMK. For a Variant LMK, the 'Key (under LMK)' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'. For a Key Block LMK, the 'Key (under LMK)' will be encrypted under the LMK.
Key Check Value	6 H	The key check value.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Import a Key encrypted under a KTK

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Variant LMK	Authorization: Required Activities: command.hy.host
Key Block LMK	Authorization: Required Activity: command.hy.host

Function: To import a key encrypted under a KTK, and return it encrypted under the specified LMK.

Variant LMK	Key Block LMK
The HSM must either be in the Authorized State, or the activity command.hy.host must be authorized.	The HSM must either be in the Authorized State, or the activity command.hy.host must be authorized.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'HY'.
Key Type	3 H	Indicates the key type of the key to be imported. For a list of possible values, see <i>Key Type Codes</i> in the <i>payShield 10K Host Programmer's manual</i> .
KTK Identifier	2 N	Identifier of the KTK to be used to decrypt the key
Key (KTK)	'U' + 32 H or 'T' + 48 H	The Key to be imported, encrypted under the KTK.
Key Scheme (LMK)	1 A	Indicates the scheme for encrypting the key under the LMK. For a list of key schemes, see the <i>Key Scheme Table</i> in Appendix A of the <i>payShield 10K Host Programmer's manual</i> .
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
The following section applies when importing keys in a non-key block format (e.g. X9.17) when using a Key Block LMK.		
Delimiter	1 A	Value '#'. Optional; can only be present when the key to be imported is not in a key block format; if present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the <i>Key Usage Table</i> in the <i>payShield 10K Host Programmer's manual</i> .
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. May be any permitted value for the key type; for a list of possible values, see the <i>Mode of Use Table</i> in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; only permitted value is 'N' or 'S'; must be present if the above Delimiter is present.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'HZ'.
Error Code	2 A	'00': No error '01': Warning: Key parity check failure ignored '68': Command disabled or a standard error code..
Key (under LMK)	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The imported key, encrypted under the LMK. For a Variant LMK, the 'Key (under LMK)' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'. For a Key Block LMK, the 'Key (under LMK)' will be encrypted under the LMK.
Key Check Value	6 H	The key check value.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Export a Key

Variant LMK	Key Block LMK
Available in package(s): Classic & Premium	
Variant LMK	Authorization: Determined by KTT(E) Activity: export.{key}.host
Key Block LMK	Authorization: If export to non-KB Activity: export.{key}.host

Function: To encrypt a key under a ZMK or TMK for export.

Variant LMK	Key Block LMK														
<p>Authorization:</p> <p>This command examines the 'Export' flag of the given key type within the Key Type Table (see the <i>payShield 10K Host Programmer's manual</i>) to determine the authorization requirement. If the flag is 'A', the HSM must either be in the Authorized State, or the activity export.{key}.host must be authorized, where 'key' is the key type code of the key being exported.</p>	<p>The authorization requirement for this command depends on the type of export being requested:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">"Key Scheme (ZMK)"</th><th style="text-align: left;">Authorization</th></tr> </thead> <tbody> <tr> <td>'S' (Thales Key Block)</td><td>None</td></tr> <tr> <td>'R' (TR-31 Key Block)</td><td>None</td></tr> <tr> <td>'V' (Verifone/GISKE Key Block)</td><td>None</td></tr> <tr> <td>'U', 'T' (Variant)</td><td>Required</td></tr> <tr> <td>'Z', 'X', 'Y' (X9.17)</td><td>Required</td></tr> <tr> <td>'P', 'Q', 'W' (AES CBC)</td><td>Required</td></tr> </tbody> </table> <p>If authorization is required, the HSM must either be in the Authorized State, or the activity export.{key}.host must be authorized, where 'key' is the key usage code of the key being exported.</p>	"Key Scheme (ZMK)"	Authorization	'S' (Thales Key Block)	None	'R' (TR-31 Key Block)	None	'V' (Verifone/GISKE Key Block)	None	'U', 'T' (Variant)	Required	'Z', 'X', 'Y' (X9.17)	Required	'P', 'Q', 'W' (AES CBC)	Required
"Key Scheme (ZMK)"	Authorization														
'S' (Thales Key Block)	None														
'R' (TR-31 Key Block)	None														
'V' (Verifone/GISKE Key Block)	None														
'U', 'T' (Variant)	Required														
'Z', 'X', 'Y' (X9.17)	Required														
'P', 'Q', 'W' (AES CBC)	Required														

Notes:

A TMK can only export the following key types:
 If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N":
 002 (TPK)
 003 (TAK)
 30B (TEK)
 302 (IKEY)
 If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y":
 70D (TPK)
 003 (TAK)
 30B (TEK)
 302 (IKEY)

A TMK with Key Usage = '51' can only export keyblocks with the following Key Usage values:

'P0', '71' (TPK)
 'M1', 'M3', 'M5', 'M6' (TAK)
 '23' (TEK)
 'B1' (IKEY)

A key block that is exported to Verifone/GISKE key block format must have the following Key Usage values:

'P0', '71' (TPK)
 'M0', 'M3' (TAK)

The ZMK (or TMK) key block must have the following field values:

"ZMK" KB Header	Value(s)
Key Usage	'K0', 'K1', '51', or '52'
Algorithm	'D'*', 'T', or 'A'
Mode of Use	'B', 'E', or 'N'

* Note: Exporting to a key block format is not permitted with a single-length ZMK or TMK.

When exporting from Thales key block to TR-31 format, any Thales proprietary Key Usage value is converted to a standard TR-31 value.

When exporting an AES ZKA Master Key:

- the key must be a 256-bit AES key;
- the key (in Thales Key Block format) must use Key Usage = '53';
- the output key (in TR-31 format) will use 0020 Key Usage = '11'.

Further Notes:

Exporting to a key block format requires the use of a 3DES or AES ZMK or TMK.

Exporting to Verifone/GISKE key block format always requires a (3DES) TMK, and is further restricted to only permitting the export of a 3DES TPK or TAK.

In order to export a ZMK, the following security setting must be set:

Enable export of a ZMK: Yes

For security reasons, when using a Key Block LMK, this command will not support the export of a DEK (Key Usage = "D0" or "21") to variant or X9.17 format.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'A8'.
Key Type	3 H	<p>For a Variant LMK: Indicates the key type of the key to be exported. For a list of possible values, see <i>Available Key Types/Usages</i> (p.37).</p> <p>For a Key Block LMK: This field is ignored; should be set to 'FFF'.</p>

Field	Length & Type	Details												
Delimiter	1 A	Value ':'. Optional. If present, the following field must be present.												
ZMK/TMK Flag	1 N	Optional. Only present if the above delimiter is present. '0': ZMK (default value if these fields are not present) '1': TMK												
ZMK (or TMK)	16 H or 32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The Zone Master Key (or Terminal Master Key). For a Variant LMK, the 'ZMK' is encrypted under LMK pair 04-05 variant 0. The 'TMK' is encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 8 if the setting has the value "Y". For a Key Block LMK, the 'ZMK (or TMK)' must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'K0', 'K1', '51', '52'</td> <td>'D', 'T', 'A'</td> <td>'B', 'E', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'K0', 'K1', '51', '52'	'D', 'T', 'A'	'B', 'E', 'N'						
Key Usage	Algorithm	Mode of Use												
'K0', 'K1', '51', '52'	'D', 'T', 'A'	'B', 'E', 'N'												
Key	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	Key to be exported; encrypted under the LMK. For a Variant LMK, the 'Key' is encrypted under the LMK pair/variant indicated by the Key Type. For export to Verifone/GISKE key block format, the 'Key' must be a 3DES TPK or TAK. For a Key Block LMK, the 'Key' must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>Any valid value</td> <td>'D', 'T', 'A'</td> <td>Any valid value</td> </tr> </tbody> </table> For a list of valid Key Usage values, refer to <i>Available Key Types/Usages</i> (p. 37). For export to Verifone/GISKE key block format, the 'Key' must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'M0', 'M3', 'P0', '71'</td> <td>'T'</td> <td>Any valid value</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	Any valid value	'D', 'T', 'A'	Any valid value	Key Usage	Algorithm	Mode of Use	'M0', 'M3', 'P0', '71'	'T'	Any valid value
Key Usage	Algorithm	Mode of Use												
Any valid value	'D', 'T', 'A'	Any valid value												
Key Usage	Algorithm	Mode of Use												
'M0', 'M3', 'P0', '71'	'T'	Any valid value												
Key Scheme (ZMK or TMK)	1 A	Indicates the scheme for encrypting the key under the ZMK (or TMK). For a list of key schemes, see the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> .												
IV	32 H	Optional; only present if Key Scheme (ZMK or TMK) is 'P', 'Q' or 'W'. For details, see the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> . Specifies the IV to be used when exporting an AES key in CBC format.												
Atalla Variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.												
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.												
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.												
The following section applies when exporting to a key block format (e.g. TR-31 / Thales Key Block / GISKE) when using a Key Block LMK.														
Delimiter	1 A	Value '&'. Optional; can only be present when the exported key is in key block format; if present, the following fields must be present.												
Modified Exportability	1 A	Exportability field, to be included in the key block header; only permitted value is 'N'; must be present if the above Delimiter is present.												
Modified Key Usage	2 A	This field must be present when the above Delimiter is present and when exporting to GISKE format. Key Usage field, to be included in the key block header; permitted values are: 'P0', 'K0', '00', '10', '20', '30', '40', '50', or '60'.												
Modified Key Block Version ID	1 A	This field must be present when the above Delimiter is present and when exporting to GISKE format. Key Block Version ID field, to be included in the key block header; permitted values are: 'A', '2'.												

Field	Length & Type	Details
The following section specifies the optional blocks to be included in the exported TR-31 key block (only) when using a Key Block LMK.		
Delimiter	1 A	Value '\$'. Optional; only present if exporting in TR-31 format.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; must be present if the above Delimiter is present. Permitted values: '00' to '99'. Note this is reduced if Optional Blocks KS and/or KV are specified to be included as given above.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; to be included only in the exported TR-31 key block header. Valid values include: 'KS', 'KV', 'KC', 'KP', 'IK', 'TS' and '00' – '99'. Note: 'KS' and 'KV' can only be added if they are not already included in Thales Key Block - otherwise a "Repeated optional block ID" error is given.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present. A value of '00' indicates this block contains an Extended Numeric Optional Block.
The following 2 fields are relevant only if Optional Block Length = '00':		
Length of Optional Block Extended Length	2 H	Only present if the Optional Block Length field = '00'. Specifies the length (in bytes) of the following field. Value: '02'.
Optional Block Extended Length	4 H	Only present if the Optional Block Length field = '00'. Number of characters in the optional block (including the identifier and length); min permitted value X'0101; max permitted value X'2670.
Optional Block Data	n A	Optional block data.
Delimiter	1 A	Value '!'. Optional; can only be present when exporting the key to TR-31 key block format. If present, the following field must be present.
Key Block Version ID	1 A	Key Block Version ID 'A': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'B': Key block protected using the Key Derivation Binding Method (see Ref 8 §5.3.2.1) 'C': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'D': Key block protected using the AES Key Derivation Binding Method (see Ref 8 §5.3.2.3).

Field	Length & Type	Details
The following section applies when exporting to TR-31 format when using a Variant LMK.		
Delimiter	1 A	Value '&'. Optional; can only be present when the key is to be exported in TR-31 format; if present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the TR-31 key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Key Usage Table in the <i>payShield 10K Host Programmer's manual</i> .
Mode of Use	1 A	Mode of Use field, to be included in the TR-31 key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the TR-31 key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the TR-31 key block header; only permitted value is "N" or "S"; must be present if the above Delimiter is present.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below, to be included in the TR-31 key block header; permitted values '00' to '02'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; to be included only in the exported TR-31 key block header. Valid values include: 'KS', 'KV', 'KC', 'KP', 'IK', 'TS' and '00' – '99'. Note: 'KS' and 'KV' can only be added if they are not already included in Thales Key Block - otherwise a "Repeated optional block ID" error is given.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present. A value of '00' indicates this block contains an Extended Numeric Optional Block.
The following 2 fields are relevant only if Optional Block Length = '00':		
Length of Optional Block Extended Length	2 H	Only present if the Optional Block Length field = '00'. Specifies the length (in bytes) of the following field. Value: '02'.
Optional Block Extended Length	4 H	Only present if the Optional Block Length field = '00'. Number of characters in the optional block (including the identifier and length); min permitted value X'04.
Optional Block Data	n A	Optional block data; to be included in the TR-31 key block header.
Delimiter	1 A	Value '!'. Optional. If present, the following field must be present.
Key Block Version ID	1 A	Key Block Version ID: 'A': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'B': Key block protected using the Key Derivation Binding Method (see Ref 8 §5.3.2.1) 'C': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'D': Key block protected using the AES Key Derivation Binding Method (see Ref 8 §5.3.2.3).
The following section applies when exporting to GISKE format when using a Variant LMK.		
Delimiter	1 A	Value '&'. Optional; can only be present when the key is to be exported in GISKE format; if present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the GISKE key block header; permitted values: 'P0', 'K0', '00', '10', '20', '30', '40', '50', or '60'; must be present if the above Delimiter is present.
Key Version Number	2 N	Key Version Number field, to be included in the GISKE key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Key Block ID	1 A	Key Block Identifier, defines the first byte of the GISKE key block header; permitted values: 'A' or '2'; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'A9'.
Error Code	2 A	'00': No error '10': ZMK or TMK Parity error '11': Key parity error 'BC': Repeated optional block ID '68': Command disabled or a standard error code.
Key (under ZMK or TMK)	16 H or 'U' or 'X' or 'P' + 32 H or 'T' or 'Y' or 'Q' + 48 H or 'W' + 64 H or 'R' + n A or 'S' + n A or 'V' + n A	The key encrypted under ZMK or TMK.
Key Check Value	6 H	The key check value.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate Key Scheme

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Required	
Activity: misc.host	

Function: Translate an existing key to a new key scheme. Note that only translations between variant key schemes are possible.

This command only supports translation from 32H, X and Y formats.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'B0'.
Key Type	3 H	Indicates the key type of the key to be translated.
Key	32 H or 'X' + 32 H or 'Y' + 48 H	The key encrypted under appropriate LMK.
Key Scheme (LMK)	1 A	Indicates the scheme for encrypting the key under the LMK. For a list of key schemes, see the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> .
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'B1'.
Error Code	2 A	'00': No error '10': Key Parity error '68': Command disabled or a standard error code.
Key	'U' + 32 H or 'T' + 48 H	The key encrypted under LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate ZMK from ZMK to LMK encryption

Variant LMK	Key Block LMK
Available in package(s): Classic & Premium	
Variant LMK	Authorization: Required Activities: import.{key}.host
Key Block LMK	Authorization: Not required

Function: To translate a ZMK from encryption under a ZMK to encryption under the LMK

Variant LMK	Key Block LMK						
Authorization: The HSM must either be in the Authorized State, or the activity import.{key}.host must be authorized, where 'key' is the key type code of the key (in this case, a ZMK) being imported.	The authorization requirement for this command depends on the type of import being requested: <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #e0e0ff;">Scheme of "Key (ZMK)"</th> <th style="background-color: #f2e0e0;">Auth</th> </tr> </thead> <tbody> <tr> <td>'S' (Thales Key Block)</td> <td>None</td> </tr> <tr> <td>'R' (TR-31 Key Block)</td> <td>None</td> </tr> </tbody> </table> If authorization is required, the HSM must either be in the Authorized State, or the activity import.{key}.host must be authorized, where 'key' is the key usage code of the key being imported.	Scheme of "Key (ZMK)"	Auth	'S' (Thales Key Block)	None	'R' (TR-31 Key Block)	None
Scheme of "Key (ZMK)"	Auth						
'S' (Thales Key Block)	None						
'R' (TR-31 Key Block)	None						

Notes: This command is enabled and disabled using the CS (Configure Security) console command.

The command does not require the imported ZMK to have odd parity, but odd parity is forced on the encrypted output. Error 01 is returned and subsequent fields are not inhibited.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'BY'.						
ZMKi	16 / 32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The ZMKi encrypted under the LMK.</p> <p>For a Variant LMK, the 'ZMKi' is encrypted under LMK pair 04-05.</p> <p>For a Key Block LMK, the 'ZMKi' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'K0', 'K1', '52'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'K0', 'K1', '52'	'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'K0', 'K1', '52'	'T', 'A'	'B', 'D', 'N'						
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H or 'R' + n A or 'S' + n A	<p>The ZMK encrypted under ZMKi.</p> <p>For a Variant LMK, the 'ZMK' must be in Variant or TR-31 format.</p> <p>If in Thales or TR-31 key block format, the 'ZMK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'K0', 'K1', '52'</td><td>'D', 'T', 'A'</td><td>Any valid value</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'K0', 'K1', '52'	'D', 'T', 'A'	Any valid value
Key Usage	Algorithm	Mode of Use						
'K0', 'K1', '52'	'D', 'T', 'A'	Any valid value						
Atalla Variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.						
Delimiter	1 A	Optional. If present the following three fields must be present. Value ':'.						
Reserved	1 A	Optional. If present must be '0'.						
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> .						
Key Check Value Type	1 A	<p>Optional. Key Check Value calculation method:</p> <p>'0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV.</p> <p>Note: Thales Keyblocks will only generate 6-digit check values.</p>						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
The following section applies when importing from TR-31 format when using a Key Block LMK.								
Delimiter	1 A	Value '#'. Optional; can only be present when the ZMK to be imported is in TR-31 key block format; if present, the following fields must be present.						
Modified Key Usage	2 A	Key Usage field, to be included in the imported key block header; must be present if the above Delimiter is present.						
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '06'; must be present if the above Delimiter is present.						
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.								
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'KS', 'KV', 'PB'.						
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.						
Optional Block Data	n A	Optional block data.						
The following section applies when importing from a non-key block format (e.g. X9.17) when using a Key Block LMK.								
Delimiter	1 A	Value '#'. Optional; can only be present when the key to be imported is not in a key block format; if present, the following fields must be present.						
Key Usage	2 A	Key Usage field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Key Usage Table in the <i>payShield 10K Host Programmer's manual</i> .						

Field	Length & Type	Details
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. May be any permitted value for the key type; for a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; only permitted value is 'N' or 'S'; must be present if the above Delimiter is present.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'BZ'.
Error Code	2 A	'00': No error '01': ZMK parity error, advice only '10': ZMKi Parity error '68': Command disabled or a standard error code.
ZMK	16 / 32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The translated ZMK, encrypted under the LMK. For a Variant LMK, the 'ZMK' will be encrypted under LMK pair 04-05. For a Key Block LMK, the 'ZMK' will be encrypted under the LMK.
Key Check Value	6 H	Result of encrypting 64 binary zeroes with the ZMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

3.2 LMK Translation Commands

Much of the data held by the host is encrypted under the HSM's LMK. If the value of the LMK changes, the associated data cannot be used until it has been translated. To do this, a facility is provided for the simultaneous storage of the old and new LMK within the HSM. Two scenarios exist:

- If the current LMK is the 'new' LMK, then load the 'old' LMK into Key Change Storage (e.g. using the console LO command).
- If the current LMK is the 'old' LMK, then load the 'new' LMK into Key Change Storage (e.g. using the console LN command).

The HSM keeps track of whether an LMK held in Key Change Storage is a 'old' or 'new' LMK, and the commands that perform the LMK translation operations always translate from 'old' LMK to 'new' LMK.

When the appropriate LMK has been loaded into key change storage, all data held on the Host, encrypted under the 'old' LMK should be sent to the HSM for translation. Commands are provided for translating each type of key and PINs encrypted for Host storage.

The payShield 10K provides the following host commands to support LMK translation operations:

Function	Command	Page
<i>Translate a PIN and PIN Length</i>	BG (BH)	93
<i>Translate Keys from Old LMK to New LMK and Migrate to New Key Type</i>	BW (BX)	94
<i>Erase the Key Change Storage</i>	BS (BT)	98

Translate a PIN and PIN Length

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Translate a PIN and/or PIN length from encryption under an 'old' LMK to encryption under the 'new' LMK. The 'old' or 'new' LMK must have previously been loaded into Key Change Storage.

Notes: The command can be used to translate the PIN length only. In this case, load the same LMKs to "key change storage" that are loaded as the current LMK.
The PIN length is L₂N for PIN encryption algorithm A, and L₂H for PIN encryption algorithm B, as selected by the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'BG'.
Primary Account Number (PAN)	12 N or n N	If a 3DES Key Block or Variant LMK is used: The 12 right-most digits of the PAN, excluding the check digit. If an AES Key Block LMK is used: The full 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.
Delimiter	1 A	Value '.'. Only present if an AES Key Block LMK is used.
PIN	L ₁ N or L ₁ H or 'M' + 32 H	The PIN encrypted under the old LMK. When using an old 3DES Variant or Key Block LMK, the length of the encrypted PIN is L ₁ digits, where L ₁ is defined by the security setting "PIN Length" at the time the "old" LMK was loaded. When using an old AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'BH'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
PIN	L ₂ N or L ₂ H or 'M' + 32 H	The PIN encrypted under the current LMK, where L ₂ is the new encrypted PIN length, defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate Keys from Old LMK to New LMK and Migrate to New Key Type

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function:

This command can be used to perform one of the following functions:

- Translate keys from encryption under an 'old' LMK to encryption under a 'new' LMK. The 'old' or 'new' LMK must have previously been loaded into Key Change Storage.
- Migrate keys from key type 002 (LMK pair 14-15 variant 0) to new key type as required for key separation for PCI HSM compliance.

Notes:

Translation from an 'old' Key Block LMK to a 'new' Variant LMK is not supported.

If a valid 2-digit Key Type code is used, then the 3-digit Key Type field should not be present.

Refer to the *payShield 10K Host Programmer's manual* to see what key types should be used when migrating keys from key type 002 (i.e. when using Key Type Code E2 or F2 in the command).

The ability to migrate keys from key type 002 to their PCI HSM compliant key types (i.e. when using Key Type Code E2 or F2 in the command) is available only while the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N"

When Key Type Code E2 is being used (to migrate keys from key type 002 **without** changing the LMK), the "live" LMK is used and it is not required to load any LMK into Key Change Storage.

This command only supports returning a 6H KCV. If a 16H KCV is requested this command will return a 6H KCV with the leftmost 10 digits set to '0'.

Key Algorithm:	DES keys	AES keys	HMAC keys
Key Check Value Calculation Method	Encryption of a block of binary zeros	CMAC of a block of binary zeros	HMAC of a zero-length message

payShield 10K Core Host Commands

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'BW'.
2-digit Key Type Code	2 N	<p>For an old Variant LMK: One of the following values: '00' – '9E': LMK translation only; this field indicates a 2-digit Key Type Code (identical to the regular 3-digit Key Type Code but without the middle digit) 'E2': key migration only, from key type 002 to the key type specified after delimiter. This value may be used only if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" and there is no LMK in Key Change Storage. 'F2': LMK translation and key migration from key type 002 to the key type specified after delimiter. This value may be used only if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N". 'FF': LMK translation only; use 3-digit Key Type Code specified after delimiter.</p>
	or 2 H	<p>For an old Key Block LMK: This field is reserved, and should be set to 'FF'.</p>
Key Length Flag	1 N	<p>For an old Variant LMK: '0': for single-length key '1': for double-length key '2': for triple-length key.</p>
	or 1 H	<p>For an old Key Block LMK: This field is reserved, and should be set to 'F'.</p>
Key	16 / 32 H or 'U' + 32 H or 'T' + 48 H	<p>The Key to be translated from old LMK to new LMK and/or migrated to new key type.</p> <p>For an old Variant LMK, the 'Key' is encrypted under the old LMK (pair/variant as defined by 'Key Type Code' above).</p>
	or 'S' + n A	<p>For an old Key Block LMK, the 'Key' is encrypted under the old LMK.</p>
Delimiter	1 A	Optional. Only present if the following field is present. Value ':'.
3-digit Key Type Code	3 H	<p>For an old Variant LMK: Where 'FF' was entered for 2-digit Key Type Code, this is the 3-digit Key Type Code of the key being translated. For a list of Key Type Codes, see the appropriate table of Key Type Codes in the <i>payShield 10K Host Programmer's manual</i>. Where 'E2' or 'F2' was entered for Key Type Code, this field is the 3-digit key type code to which the key is to be migrated. The key type of the old key must be 002. Valid values are: 002 (PVK, PVVK: no migration is needed) 70D (TPK, PEK) 80D (TMK, KT, TK, KI, KCA, KMA) 90D (TKR)</p> <p>For an old Key Block LMK: This field is reserved, and should be set to 'FFF'.</p>
Delimiter	1 A	Optional. If present the following three fields must be present. Value ':'.
Reserved	1 A	Optional. If present must be '0'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0'). For a list of key schemes, see the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> .
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
The following section only applies when translating from a Variant LMK to a Key Block LMK.		
Delimiter	1 A	Value '#'. Optional; Must be present when translating a key from an old Variant LMK to a current Key Block LMK. If present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the key block header; any permitted value for the key type; must be compatible with the existing key type; must be present if the above Delimiter is present. For a list of possible values, see the Key Usage Table in the <i>payShield 10K Host Programmer's manual</i> .

payShield 10K Core Host Commands

Field	Length & Type	Details
COMMAND MESSAGE		
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. May be any permitted value for the key type; for a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; only permitted value is 'N' or 'S'; must be present if the above Delimiter is present.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
<p>For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.</p>		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
Delimiter	1 A	Optional. Only present if the Key Check Return Flag and Key Check Value Type fields are present. Value = '!'.
Key Check Return Flag	1 A	Optional. If present must be '1'
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV Length (6H KCV with the leftmost 10 digits will be set to '0') '1': 6 digit KCV. Note: Thales Keyblocks will only generate 6-digit check values. Only present if Key Check Return Flag is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'BX'.
Error Code	2 A	'00': No error '04': Invalid key type code '05': Invalid key length flag '10': Key parity error '44': Migration not allowed: key migration requested when the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y" '45': Invalid key migration destination key type '68': Command disabled or a standard error code.
Key	16 / 32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The translated Key, encrypted under the current LMK. For a new Variant LMK, the 'Key' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'. For a new Key Block LMK, the 'Key' will be encrypted under the LMK.
Key Check Value	16 or 6 H	Optional; The calculated check value of the supplied key. 16H with 6H KCV and the left most digits set to '0' / 6H depending on chosen Key Check Value option. Only present if the Key Check Return Flag and Key Check Value Flags are present.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Erase the Key Change Storage

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Erase the key change storage area of memory.

Notes: It is recommended that this command is used after keys stored by the Host have been translated from old to new LMKs.

Only the key change storage corresponding to the identified LMK will be erased.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'BS'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'BT'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

3.3 EMV Key Management Commands

The payShield 10K provides the following host commands to support generic key management operations:

Function	Command	Page
<i>Derive Card Unique DES Keys</i>	KI (KJ)	100
<i>Export a Key under a KEK</i>	K8 (K9)	106
<i>Import an RSA Private Key</i>	L6 (L7)	109
<i>Export an RSA Private Key</i>	L8 (L9)	113
<i>Generate Digitized Card Single Use Keys</i>	IY (IZ)	116
<i>Generate Remote Management Session ID and Session Keys</i>	IO (IP)	135

Derive Card Unique DES Keys

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Derive a Card Unique Key from a Master Key.

Notes: This function supports:

- Generation of Unique Derived keys for EMV cards
- Generation of Card Master Keys for personalization using EMV CPS
- Generation of the Account Unique Keys AUK DCVV for Discover
- Generation of the session keys for cloud based mobile payments (using HCE)

When using a Key Block LMK, the Key Derivation Method determines the choice of algorithms for the Master Key and the KEK, and additionally the key scheme(s) that can be used for encrypting the derived key under the KEK.

Key Derivation Method		Master Key		KEK
Name	Value	Key Usage	Alg	Alg
EMV 4.x Book 2 Option A or B method	'A', 'B'	'E0', 'E1', 'E2', 'E4', 'E6', 'E7', '32'	3DES / AES	3DES
EMV CPS method for Card Master Keys or Generic Personalisation Key Derivation Method	'C', 'D'	'E7'		
Visa Limited Use Key (LUK) QR Code	'H'	'E0'		
Visa Limited Use Key (LUK)	'E'	'E0'		
AMEX Limited Use Key (LUK)	'F'	'E0', 'E1', 'E2', 'E4', 'E6', 'E7', '32'		
Discover Network - Derive 16/24-byte AUKDCVV from DCVV	'2', '3'	'32'		AES
Discover One Time Personalisation Key (OTPK) (Key Gen = 0 or 1)	'G'	'E0'		
Discover One Time Personalisation Key (OTPK) (Key Gen = 2 or 3)		'E2', 'E6'		
Discover One Time Personalisation Key (OTPK) (Key Gen = 4 or 5)		'C0', '12', '13'		
EMV 4.x Option 'C' method (AES)	'I'	'E0', 'E1', 'E2', 'E4', 'E6', 'E7', '32'	AES	AES

The table below specifies the permitted Mode of Use values for the different Master Keys:

Master Key – Key Block Requirements	
Key Usage	Mode of Use
'32', 'E0', 'E1', 'E2', 'E4', 'E6', 'E7'	'X', 'N'
'C0', '12', '13'	'N'

The table below specifies the permitted Key Scheme values for different types of KEKs:

Key Encryption Key (KEK) – Key Scheme Requirements		
Key Derivation Method	KEK Algorithm	Permitted Key Schemes
'A', 'B', 'C', 'D', 'E', 'F', 'H', '2', '3'	3DES	'X' for a 112-bit 3DES key (ECB encrypted) 'Y' for a 168-bit 3DES key (ECB encrypted)
'A', 'B', 'C', 'D', 'H', 'I'	AES	'N' with AES-256 key (NIST SP800-38F Key Wrap)
'G'	AES	'X' for a 112-bit 3DES key (ECB encrypted)

Field	Length & Type	Details									
COMMAND MESSAGE											
Message Header	m A	Subsequently returned to the Host unchanged.									
Command Code	2 A	Value 'KI'.									
MK Type	3 H	For a Variant LMK, the field specifies the Master Key Type. The following Key Types are permitted: '109': MK-AC encrypted under LMK 28-29/1 '209': MK-SMI encrypted under LMK 28-29/2 '309': MK-SMC encrypted under LMK 28-29/3 '509': MK-DN encrypted under LMK 28-29/5 '709': MK-CVC3 or MK-DCVV encrypted under LMK 28-29/7 '207': KMC encrypted under LMK 24-25/2 '402': CVK encrypted under LMK 14-15/4. For a Key Block LMK, this field is ignored and should be set to 'FFF'.									
MK	32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	Master Key from which the unique key is derived, encrypted under LMK. For a Variant LMK, the 'MK' must be encrypted under the appropriate LMK pair/variant defined by the 'MK Type' field. For a Key Block LMK, the 'MK' must comply with one of the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'12', '13', 'C0',</td><td>'T'</td><td>'N'</td></tr> <tr> <td>'32', 'E0', 'E1', 'E2', 'E4', 'E6', 'E7'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'12', '13', 'C0',	'T'	'N'	'32', 'E0', 'E1', 'E2', 'E4', 'E6', 'E7'	'T', 'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use									
'12', '13', 'C0',	'T'	'N'									
'32', 'E0', 'E1', 'E2', 'E4', 'E6', 'E7'	'T', 'A'	'X', 'N'									
Key Derivation Method	1 A	Specifies the method to be used to derive a unique key from the Master Key: 'A': EMV 4.x Book 2 Option A method 'B': EMV 4.x Book 2 Option B method 'C': EMV CPS method for Card Master Keys Note: This derivation method will derive 3 keys (CK-ENC, CK-MAC and CK-DEK) from the Master key as defined in EMV CPS. 'D': Generic Personalisation Key Derivation Method 'E': Visa Limited Use Key (LUK) (only valid if MK Type = 109) 'F': AMEX Limited Use Key (LUK) 'G': Discover One Time Personalisation Key (OTPK) 'H': Visa Limited Use Key (LUK) QR Code (only valid if MK Type = 109) 'I': EMV 4.x Option 'C' method (AES) Discover Network specific methods for deriving unique key from Master Key (only valid if MK Type = 709): '2': 16-byte Account Unique Key for DCVV (AUK _{DCVV}) '3': 24-byte Account Unique Key for DCVV (AUK _{DCVV})									
Derivation Data	n N 6 B 16 B 20 N n N	If Key Derivation Method = 'A', 'B', 'E', 'F', 'H' or 'I': Concatenation of the Primary Account Number and 2 digit Sequence Number for the card. If the Sequence Number is not available it should be specified as '00'. If Key Derivation Method = 'C': Card Key derivation data (e.g. KEYDATA composed of Master Key ID and Chip Serial Number) If Key Derivation Method = 'D': The key derivation data. If Key Derivation Method = '2' or '3', or Key Derivation Method = 'G' and OTPK Key Generation Method = '2' or '3': Concatenation of the 16 digit Primary Account Number (PAN) and 4 digit Expiration Date for the card. If Key Derivation Method = 'G' and OTPK Key Generation Method = '0', '1', '4' or '5': Concatenation of the Primary Account Number and 2 digit PAN Sequence Number. If the Sequence Number is not available it should be specified as '00'.									
Delimiter	1 A	Delimiter. Value ':'.									
If Key Derivation Method = 'E' or 'H', the following field will be present:											

Field	Length & Type	Details						
YHHHHCC	7 N	Only present if Key Derivation Method = 'E'. The Year/Hour/Counter value used to derive the Limited Use Key (LUK) to produce the Limited Use Cryptogram (LUC). Y (0-9) : least significant digit of current year HHHH (0001-8784) : number of hours since Jan 1st CC (00-99) : counter						
If Key Derivation Method = 'F', the following 4 fields must be present:								
Output Key Flag	1 A	'0': Derive SK-AC session key '1': Derive SK-CVM session key						
UDK Key Derivation Method	1 A	'A': EMV 4.3 ii Option A 3DES ECB 'B': EMV 4.3 ii Option B 3DES ECB						
Session Key Method	2 N	'01': EMV Common Session Key Derivation						
ATC	2 B	Application Transaction Counter						
If Key Derivation Method = 'F' and Output Key Flag = '1', the following 3 fields must be present:								
Passcode Key Method	2 N	'01': PBKDF2 with HMAC SHA-1						
CVM Session Key Method	2 N	'01': 3DES CBC						
IV	8 B or 16 B	Initialisation Vector. 8 B: If CVM Session Key Method = '01' 16 B: If CVM Session Key Method = '02'						
If Key Derivation Method = 'F', Output Key Flag = '1' and Passcode Key Method = '01', the following 7 fields must be present:								
PIN Block Format Code	2 N	Valid PIN block format codes are: '02': Docutel ATM format '03': Diebold & IBM ATM format '05': ISO 9564-1 format 1 '34': Standard EMV 1996 format						
Passcode PIN Block ZPK	8 B	The Passcode PIN Block 3DES ECB encrypted under the ZPK. The Zone PIN Key, encrypted under the LMK.						
	32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	For a Variant LMK, the ZPK encrypted under LMK pair 06-07. For a LMK key block, the ZPK encrypted under LMK should comply with:						
		<table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode Of Use</th> </tr> </thead> <tbody> <tr> <td>'P0', '72'</td> <td>'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode Of Use	'P0', '72'	'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode Of Use						
'P0', '72'	'T', 'A'	'B', 'D', 'N'						
Salt Flag	1 N	'0': Random salt supplied in command '1': Random salt generated by command						
Salt Length	2 N	The length of the Salt supplied or the length of the Salt to generate.						
Salt	n B	If Salt Flag is '0', the random salt value.						
Iteration Count	6 N	The number of iterations performed by the PBKDF. Minimum value 1000.						
If Key Derivation Method = 'G', the following fields must be present:								
Number of OTPKs	2 N	The number of OTPKs to generate.						
OTPK Key Generation Method	1 A	The OTPK Key Generation Method: '0': Default EMV using MK AC '1': Server PIN based white box using MK AC '2': Enhanced DCVV OTPK using AUK DCVV '3': Server PIN based white box using AUK DCVV '4': Default EMV using CVK '5': Server PIN based white box using CVK						

Field	Length & Type	Details						
If OTPK Key Generation Method = '1', '3' or '5', the following 3 fields must be present:								
PIN Block Format Code	2 N	Valid PIN block format codes are: '02': Docutel ATM format '03': Diebold & IBM ATM format '05': ISO 9564-1 format 1 '34': Standard EMV 1996 format						
PIN Block ZPK	8 B	The PIN Block encrypted under the ZPK. The Zone PIN Key, encrypted under the LMK.						
	32 H or 'U' + 32 H or 'T' + 48 H	For variant LMK, the ZPK is encrypted under LMK pair 06-07.						
	or 'S' + n A	For Key Block LMK, the ZPK must comply with:						
		<table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode Of Use</th></tr> </thead> <tbody> <tr> <td>'P0', '72'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode Of Use	'P0', '72'	'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode Of Use						
'P0', '72'	'T', 'A'	'B', 'D', 'N'						
For all OTPK Key Generation Methods, the following 2 fields must be present:								
Start ATC	2 B	Application Transaction Counter, n.						
Key Transport Algorithm	2 N	'00': OTPKs encrypted using AES ECB mode						
For all Key Derivation Methods, the following fields must be present:								
KEK		<p>The transport Key Encryption Key, encrypted under the LMK.</p> <p>For a Variant LMK, the 'KEK' is encrypted under LMK pair 24-25 variant 1.</p>						
	32 H or 'U' + 32 H or 'T' + 48 H							
	or 'S' + n A	For a Key Block LMK, the 'KEK' must comply with:						
		<table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode Of Use</th></tr> </thead> <tbody> <tr> <td>'54'</td><td>'T', 'A'</td><td>'B', 'E', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode Of Use	'54'	'T', 'A'	'B', 'E', 'N'
Key Usage	Algorithm	Mode Of Use						
'54'	'T', 'A'	'B', 'E', 'N'						
Key Scheme (KEK)	1 A	Key scheme for encrypting derived key under KEK. Refer to the Permitted Key Schemes table above for details.						
Key Check Value Type	1 A	'0': KCV for entire key, 6 bytes long '1': KCV for entire key, 3 bytes long						
Atalla Variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'KJ'.
Error Code	2 N	<p>'00': No error '04': Unrecognized key derivation method '05': Invalid MK type '06': Invalid MK type or Derivation Data for Derivation Method or YHHHHCC value '10': MK parity error '11': KEK parity error '20': Invalid PIN Block '23': Invalid PIN Block Format value '27': Key Scheme (KEK) and derived key mismatch 'DA': KEK – key block error 'DB': ZPK – key block error 'E2': ZPK parity error 'EA': MK – key block error 'F1': Invalid UDK Method 'F2': Invalid Session Key Method 'F3': Invalid CVM Session key Method 'F4': Invalid Passcode Key Method 'F5': Invalid Salt Flag value 'F6': Invalid Output Key Flag 'F7': Invalid Iteration Count 'F8': Invalid OTPK Key Generation Method value 'F9': Invalid Key transport Algorithm 'FA': Invalid KEK Key Type or Algorithm 'FB': Invalid OTPK Count 'FC': Invalid Derivation Data length 'FD': Invalid OTPK Option 'FE': Not supported with variant LMK 'FF': Key Derivation Method not allowed or a standard error code.</p>
If Error Code = 'DA', 'DB' or 'EA', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
If Key Derivation Method = 'A' or 'B' the following 2 fields will be present:		
DK (KEK)	'X' + 16 B or 'Y' + 24 B or 'N' + n B	The derived unique key encrypted under KEK.
Key check value	6 B or 3 B	The key check value for the DK.
If Key Derivation Method = 'C', the following 6 fields will be present:		
CK-ENC	'X' + 16 B or 'N' + n B	Card Key for cryptograms encrypted under KEK.
CK-ENC KCV	6 B or 3 B	The key check value for K-ENC.
CK-MAC	'X' + 16 B or 'N' + n B	Card Key for authentication encrypted under KEK.
CK-MAC KCV	6 B or 3 B	The key check value for K-MAC.
CK-DEK	'X' + 16 B or 'N' + n B	Card Key for encryption encrypted under KEK.
CK-DEK KCV	6 B or 3 B	The key check value for K-DEK.
If Key Derivation Method = 'D', the following 2 fields will be present:		
PSK	'X' + 16 B or 'N' + n B	The Personalisation System Key encrypted under the KEK.
PSK KCV	6 B or 3 B	The PSK key check value
If Key Derivation Method = 'E', '2' or '3' the following 2 fields will be present:		
DK (KEK)	'X' + 16 B or 'Y' + 24 B	The derived unique key encrypted under KEK.
Key check value	6 B or 3 B	The key check value for the DK.

Field	Length & Type	Details
If Key Derivation Method = 'F' and Output Key Flag = '0', the following 2 fields will be present:		
SK-AC	'X' + 16 B	The AC session key encrypted under the KEK.
SK-AC KCV	6 B or 3 B	The AC session key check value.
If Key Derivation Method = 'F' and Output Key Flag = '1', the following 3 fields will be present:		
SK-CVM	'X' + 16 B	The Passcode protected CVM session key encrypted under the KEK.
SK-CVM KCV	6 B or 3 B	The CVM session key check value.
Salt Value	n B	If Salt Flag is '1', the generated random salt value.
If Key Derivation Method = 'G', the following fields will be present:		
Final ATC	2 B	The updated ATC value, n + Number Of OTPKs.
Key Blob Length	4 N	The length in bytes of the following key blob field. For the number of OTPKs requested, the key blob will consist of the concatenation of:
SK	'X' + 16 B	The OTPK session key encrypted under the KEK.
SK KCV	6 B or 3 B	The key check value for the OTPK session key.
If Key Derivation Method = 'H', the following 2 fields will be present:		
DK (KEK)	'X' + 16 B or 'Y' + 24 B or 'N' + n B	Derived Key, DK, encrypted under the KEK.
Key Check Value	6 B or 3 B	The key check value for DK.
If Key Derivation Method = 'I', the following 2 fields will be present:		
DK (KEK)	'N' + n B	Derived Key, DK, encrypted under the KEK.
Key Check Value	6 B or 3 B	The key check value for DK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Export a Key under a KEK

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Encrypt a Key under a KEK for transport to EMV data personalization system

Notes: See the Key Scheme Table in the *payShield 10K Host Programmer's manual* for schemes available to encrypt keys.

Field	Length & Type	Details												
COMMAND MESSAGE														
Message Header	m A	Subsequently returned to the Host unchanged.												
Command Code	2 A	Value 'K8'.												
Key Type	3 H	For a Variant LMK, this is the type of the key to be exported. Only the following Key Types are permitted: '001': ZPK encrypted under LMK 06-07 '008': ZAK encrypted under LMK 26-27 '00A': ZEK encrypted under LMK 30-31 <i>This field can be expanded in the future to accommodate other key types.</i>												
Key	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	For a Key Block LMK, this field is ignored and should be set to 'FFF'. The key to be exported, encrypted under the LMK. For a Variant LMK, the Key is encrypted under the LMK pair/variant defined by Key Type. For a Key Block LMK, the Key in key block format; must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode Of Use</th> </tr> <tr> <td>'P0', '72'</td> <td>'T'</td> <td>'B', 'D', 'E', 'N'</td> </tr> <tr> <td>'M1', 'M2', 'M3'</td> <td>'T'</td> <td>'C', 'G', 'N', 'V'</td> </tr> <tr> <td>'22'</td> <td>'T'</td> <td>'B', 'D', 'E', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode Of Use	'P0', '72'	'T'	'B', 'D', 'E', 'N'	'M1', 'M2', 'M3'	'T'	'C', 'G', 'N', 'V'	'22'	'T'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode Of Use												
'P0', '72'	'T'	'B', 'D', 'E', 'N'												
'M1', 'M2', 'M3'	'T'	'C', 'G', 'N', 'V'												
'22'	'T'	'B', 'D', 'E', 'N'												
KEK	32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The Key Encryption Key, to be used to protect the exported key. For a Variant LMK, the Key is encrypted under LMK 24-25/1. For a Key Block LMK, the Key in key block format; must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode Of Use</th> </tr> <tr> <td>'54'</td> <td>'T'</td> <td>'N'</td> </tr> </table>	Key Usage	Algorithm	Mode Of Use	'54'	'T'	'N'						
Key Usage	Algorithm	Mode Of Use												
'54'	'T'	'N'												
Key Scheme (KEK)	1 A	Key scheme for encrypting key under KEK. Valid values are 'X', 'Y', 'R', 'Z', 'U' and 'T'. See the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> .												
Atalla Variant	1 / 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.												
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.												
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.												

Field	Length & Type	Details
If Variant LMK and Key Scheme (KEK) = 'R', the following fields must be present:		
Delimiter	1 A	Mandatory. Must be '&'
Key Usage	2 A	Key Usage field, to be included in the TR-31 key block header; any permitted value for the key type. For a list of possible values, see the Key Usage Table in the <i>payShield 10K Host Programmer's manual</i> .
Mode Of Use	1 A	Mode of Use field, to be included in the TR-31 key block header; any permitted value for the key type. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the TR-31 key block header; permitted values: '00' to '99'.
Exportability	1 A	Exportability field, to be included in the TR-31 key block header. The only permitted values are 'N' or 'S';
Number of Optional Blocks	2 N	Number of Optional Blocks specified below, to be included in the TR-31 key block header; permitted values '00' to '02'.
If Number of Optional Blocks > '00', the following 3 fields are repeated for each optional block.		
Optional Block Identifier	2 A	Optional Block Identifier; to be included in the TR-31 key block header; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); to be included in the TR-31 key block header; permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data; to be included in the TR-31 key block header.
Delimiter	1 A	Value '!'. Optional. If present, the following field must be present.
Key Block Version ID	1 A	Key Block Version ID: 'A': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'B': Key block protected using the Key Derivation Binding Method (see Ref 8 §5.3.2.1) 'C': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'D': Key block protected using the AES Key Derivation Binding Method (see Ref 8 §5.3.2.3).
If Key Block LMK and Key Scheme = 'R', then the following fields must be present:		
Delimiter	1 A	Mandatory. Must be '&'.
Modified Exportability	1 A	Exportability field, to be included in the key block header. The only permitted value = 'N'.
The following section specifies the optional blocks to be included in the exported TR-31 key block (only) when using a Key Block LMK.		
Delimiter	1 A	Value '\$'. Optional; only present if exporting in TR-31 format.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; must be present if the above Delimiter is present. Permitted values: '00' to '99'. Note this is reduced if Optional Blocks KS and/or KV are specified to be included as given above.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; to be included only in the exported TR-31 key block header. Valid values include: 'KS', 'KV', 'KC', 'KP', 'IK', 'TS' and '00' - '99'. Note: 'KS' and 'KV' can only be added if they are not already included in Thales Key Block - otherwise a "Repeated optional block ID" error is given.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
Delimiter	1 A	Value '!'. Optional; can only be present when exporting the key to TR-31 keyblock format. If present, the following field must be present.
Key Block Version ID	1 A	'A': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'B': Key block protected using the Key Derivation Binding Method (see Ref 8 §5.3.2.1) 'C': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'D': Key block protected using the AES Key Derivation Binding Method (see Ref 8 §5.3.2.3).
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'K9'.
Error Code	2 N	'00': No error '05': Invalid key type '10': Key parity error '11': KEK parity error 'BC': Repeated optional block ID 'DA': KEK – key block error 'DB': Key – key block error or a standard error code.
If Error Code = 'DA' or 'DB', the following field will be present		
Additional Error Code	2 A	The key block specific error code.
Key (KEK)	8 B or 'X' + 16 B or 'U' + 16 B or 'Y' + 24 B or 'T' + 24 B or 'R' + n A	The exported key, encrypted under the KEK.
Key check value	3 B	The key check value.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Import an RSA Private Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Variant LMK	Authorization: Required Activity: import.00C.host
Key Block LMK	Authorization: Required Activity: import.03.host

Function: This function supports the import of an RSA Private Key from encryption under a Zone Master Key to encryption under the LMK.

The comparable algorithm key strengths defined in NIST SP800-57 part 1 are applied when importing or exporting a key under a ZMK.

The following security settings must be configured to allow use of this command:

- **Enable import and export of RSA Private Keys:** Yes
- **Key export and import in trusted format only:** No

Notes: See: *payShield 10K Host Programmer's manual* for more information.

The RSA private key for import must be in CRT format (p , q , dp , dq , u) where $dp = d \bmod (p-1)$, $dq = d \bmod (q-1)$, $u = (q-1) \bmod p$.

Each CRT component is decrypted using an AES or 3DES ZMK, and block cipher mode ECB or CBC.

The following table indicates the size of 3DES or AES key required to protect the different size RSA private keys:

Key Length (bits)	3DES ZMK	AES ZMK
320..1024	112/168-bit	128/192/256-bit
1025..2048	168-bit only	128/192/256-bit
2049..3072	Not allowed	128/192/256-bit
3073..4096	Not allowed	192/256-bit only

The following table indicates the possible values for the output key block, containing the RSA private key:

Key Usage	Valid Mode of Use values
'03' (for signing/key mgt)	'D', 'N', 'S'
'04' (for ICCs)	'N', 'S'
'05' (for PIN translation)	'D', 'N'

'06' (for data decryption) 'D', 'N'

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'L6'.						
ZMK	32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n B	The Zone Master Key, used to protect the exported RSA private key. For a Variant LMK, the ZMK is encrypted under LMK 04-05 variant 0. For a Key Block LMK, the ZMK must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'K0', 'K1', '52'</td> <td>'T', 'A'</td> <td>'B', 'D', 'E', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'K0', 'K1', '52'	'T', 'A'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'K0', 'K1', '52'	'T', 'A'	'B', 'D', 'E', 'N'						
Key Format	1 N	The format of the private key to import. '0': CRT components (P, Q, DP, DQ, U in order)						
Block Cipher Mode	1 N	The Block Cipher Mode to use when decrypting the RSA private key under the ZMK: '0': ECB '1': CBC. Each component (plus any pad) individually encrypted using an IV of 0.						
Pad Mode	1 N	The ISO 9797-1 padding mode: '1': Optional 0x00 pad bytes to block length appended '2': Mandatory 0x80 and optional 0x00 to block length appended '3': Prepended length byte(s) (containing the unpadded CRT component byte length value) and optional 0x00 pad appended						
If Pad Mode = '3', the following field must be present:								
Length Byte	1 N	'0': non BER encoded length (one byte) '1': BER encoded length.						
Private Key Length	4 H	The length of the Private Key in bytes						
Private Key	n B	Private Key encrypted under the ZMK						
Validate imported private key flag	1 N	'0': No validation of the private key is performed. '1': Validate the imported private key						
If Validate Imported Private key flag = '1', the following 4 fields must be present								
Public Key length	4 H	The length of the Public Key modulus in bytes						
Public key	n B	The public key modulus (n)						
Public Exponent Length	4 H	The length of the Public Exponent in bytes						
Public Exponent	n B	The exponent (e)						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by licence; must be present if the above Delimiter is present.						

Field	Length & Type	Details
If Key Block LMK, the following fields must be present:		
Delimiter	1 A	Value '#'.
Delimiter	1 A	Value '~'. Optional; if present, the following 2 fields must be present.
Key Usage	2 H	Only present if the '~' delimiter (above) is present. Key Usage field, to be included in the key block header; permitted values: '03', '04', '05', '06'. If not present, the imported key will have a Key Usage field of '03'.
Mode of Use	1 A	Only present if the '~' delimiter (above) is present. Mode of Use field, to be included in the key block header; permitted values 'D', 'N', 'S'. If not present, the imported key will have a Mode of Use field of 'N'.
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99';
Exportability	1 A	Exportability field, to be included in the key block header; only permitted values are 'N', 'E' or 'S';
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08';
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present
Optional Block Data	n A	Optional block data
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details						
RESPONSE MESSAGE								
Message Header	m A	Returned to the Host unchanged.						
Response Code	2 A	Value 'L7'.						
Error Code	2 A	<p>'00': No error '03': Command disabled by security configuration '10': ZMK key parity error '80': Private Key Length error 'D1': ZMK – key block error 'D3': Invalid Key Format 'D4': Invalid format for private key 'D5': ZMK key strength error (key length security check failed) 'D6': Key export not allowed (Export field in key block set to 'N') 'D7': Private Key – key block error 'D8': Invalid Block Cipher Mode 'D9': Invalid pad mode 'DA': Invalid length byte value 'DB': Public key length error 'DC': Public Exponent length error 'DD': Imported CRT length error 'DE': Invalid Validate Imported Secret Key Flag or a standard error code.</p>						
If Error Code = 'D1' or 'D7', the following field will be present:								
Additional Error Code	2 A	The key block specific error code.						
Private Key Length	4 H	<p>Only present if using a Variant LMK. If present, this field indicates the length of the following field.</p>						
Private Key	n B or 'S' + n B	<p>The RSA private key, encrypted under the LMK. For a Variant LMK, the Private Key is encrypted under LMK 34-35 variant 0. For a Key Block LMK, the Private Key will conform to:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'03' or Key Usage specified after '~' delimiter</td> <td>'R'</td> <td>'S' or Mode of Use specified after '-' delimiter</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'03' or Key Usage specified after '~' delimiter	'R'	'S' or Mode of Use specified after '-' delimiter
Key Usage	Algorithm	Mode of Use						
'03' or Key Usage specified after '~' delimiter	'R'	'S' or Mode of Use specified after '-' delimiter						
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.						
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.						

Export an RSA Private Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Variant LMK	Authorization: Required Activity: export.00C.host
Key Block LMK	Authorization: Required Activity: export.03.host

Function: This function supports the export of an RSA Private Key from encryption under the LMK to encryption under a Zone Master Key.

The comparable algorithm key strengths defined in NIST SP800-57 part 1 are applied when importing or exporting a key under a ZMK.

The following security settings must be configured to allow use of this command:

- 'Enable import / export of RSA Private Keys?' MUST be set to 'YES' (defaults to NO)
- 'Key export and import in trusted format only?' MUST be set to 'NO' (defaults to YES)

Notes: See: *payShield 10K Host Programmer's manual* for more information.

The exported RSA private key will be in CRT format (p , q , dp , dq , u) where $dp = d \bmod (p-1)$, $dq = d \bmod (q-1)$, $u = (q-1) \bmod p$.

Each CRT component is encrypted using an AES or 3DES ZMK, and block cipher mode ECB or CBC.

The following table indicates the size of 3DES or AES key required to protect the different size RSA private keys:

Key Length (bits)	3DES ZMK	AES ZMK
320..1024	112/168-bit	128/192/256-bit
1025..2048	168-bit only	128/192/256-bit
2049..3072	Not allowed	128/192/256-bit
3073..4096	Not allowed	192/256-bit only

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code ZMK	2 A 32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n B	Value 'L8'. The Zone Master Key, used to protect the exported RSA private key. For a Variant LMK, the ZMK is encrypted under LMK 04-05. For a Key Block LMK, the ZMK must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'K0', 'K1', '52'</td> <td>'T', 'A'</td> <td>'B', 'D', 'E', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'K0', 'K1', '52'	'T', 'A'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'K0', 'K1', '52'	'T', 'A'	'B', 'D', 'E', 'N'						
Key Format	1 N	The format of the private key to export. '0': CRT components (P, Q, DP, DQ, U in order)						
Block Cipher Mode	1 N	The Block Cipher Mode to be used to encrypt the RSA private key under the ZMK: '0': ECB '1': CBC. Each component (plus any pad) individually encrypted using an IV of 0.						
Pad Mode	1 N	The ISO 9797-1 padding mode: '1': Optional 0x00 pad bytes to block length appended '2': Mandatory 0x80 and optional 0x00 to block length appended '3': Prepended length byte(s) (containing the unpadded CRT component byte length value) and optional 0x00 pad appended						
If Pad Mode = '3', the following field must be present:								
Length Byte	1 N	'0': non BER encoded length (one byte) '1': BER encoded length.						
Private Key Length	4 H	The length of the Private Key in bytes For a Variant LMK, the length of the Private Key, in bytes.						
Private Key	n B or 'S' + n B	For a Key Block LMK, this field is ignored and should be set to 'FFFF'. The Private Key, encrypted under the LMK. For a Variant LMK, the Private Key is encrypted under LMK pair 34-35 variant 0. For a Key Block LMK, the Private Key must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'03'</td> <td>'R'</td> <td>'S', 'D', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'03'	'R'	'S', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'03'	'R'	'S', 'D', 'N'						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'L9'.
Error Code	2 A	<p>'00': No error '03': Command disabled by security configuration '10': ZMK key parity error '75': Public/Private key mismatch '80': Private Key Length error 'D1': ZMK – key block error 'D3': Invalid Key Format 'D4': Invalid format for private key 'D5': ZMK key strength error (key length security check failed) 'D6': Key export not allowed (Export field in key block set to 'N') 'D7': Private Key – key block error 'D8': Invalid Block Cipher Mode 'D9': Invalid pad mode 'DA': Invalid length byte value 'DB': Public key length error 'DC': Public Exponent length error 'DD': Imported CRT length error 'DE': Invalid Validate Imported Secret Key Flag or a standard error code.</p>
If Error Code = 'D1' or 'D7', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
If Error Code = '00', the following 2 fields will be present:		
Private Key Length	4 H	The length of the Private Key.
Private Key	n B	The exported Private Key, encrypted under the ZMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Digitized Card Single Use Keys

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Derive Single Use Keys (SUKs) for Host Card Emulation (HCE) mobile payment applications.

Notes:

Command	Page
Generate Digitized Card Single Use Keys (Mode Flag '0': MCBP SUK Derivation; include PIN; output in legacy JSON format.)	117
<i>Generate Digitized Card Single Use Keys (Mode Flag '1': MCBP SUK Derivation; include PIN; output in MC SDK JSON format)</i>	121
<i>Generate Digitized Card Single Use Keys (Mode Flag '2': VCP LUK from Card Key)</i>	125
<i>Generate Digitized Card Single Use Keys (Mode Flag '3': MCBP SK from MDES; add PIN; output encrypted SUK under KEK.)</i>	127
<i>Generate Digitized Card Single Use Keys (Mode Flag '4': MCBP SUK Derivation; output encrypted under KEK)</i>	129
<i>Generate Digitized Card Single Use Keys (Mode Flag '5': LUK from Card Key with PIN)</i>	133

Generate Digitized Card Single Use Keys (Mode Flag '0': MCBP SUK Derivation; include PIN; output in legacy JSON format.)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Derive Single Use Keys (SUKs) for Mastercard Cloud Based Payments (MCBP). The user and mobile PINs will be used during the production of the SUKs. The keys will be output in legacy JSON format.

Notes: This command generates one or more DC_SUK blocks that contain the single use keys for user and mobile device authentication for contactless and remote payments, the ATC and the Dynamic Number for use in CDA.

For details of the JSON format used in the DC_SUK block, refer to *Card Issuing Appendix O – DC_SUK block template*.

The DC_SUK blocks are concatenated together and encrypted using the Remote Management Session key for confidentiality MS_KEY_CONF and MAC protected using the Remote Management Session key for integrity MS_KEY_MAC. The output is in the format suitable to loading directly to the Mobile Payment Application.

The ATC value is updated by this command according to the number of DC_SUK blocks generated.

The following input data elements will have been generated by the data preparation system using the 'KI' Generate Card Unique Keys function encrypted under a transport key:

- CMK_CL_UMD
- CMK_RP_UMD
- CMK_CL_MD
- CMK_RP_MD
- CMK_IDN

The transport keys will have been imported and encrypted under the Local Master Key.

The Mobile PIN block will be created using the PIN Translation commands and transported encrypted under a ZPK.

payShield 10K Core Host Commands

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IY'.						
Mode Flag	1 N	'0': MCBP SUK Derivation; include PIN; output in legacy JSON format						
Key Generation Option Delimiter	1 A	Value '\$'. Optional; if present, the following field must also be present.						
Key Generation Option	1 N	'0': Generate SUKs for Contactless Transactions (with PIN) '1': Generate SUKs for Remote Payment Transactions (with PIN) '2': Generate SUKs for Contactless Transactions (no PIN) '3': Generate SUKs for Remote Payment Transactions (no PIN) '4': Generate SUKs for Contactless & Remote Payment Transactions (no PIN)						
Message Counter	5 N	The message counter is maintained by the CMS and is incremented for each message sent from the CMS to MPA. Maximum value is 65535 or 0xFFFF.						
MS_KEY_CONF	'S' + n A	The Remote Management Session Key for message confidentiality, encrypted under AES Key Block LMK and which must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'35'</td><td>'A'</td><td>'B', 'D', 'E', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'35'	'A'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'35'	'A'	'B', 'D', 'E', 'N'						
MS_KEY_MAC	'S' + n A	The Remote Management Session Key for message integrity, encrypted under AES Key Block LMK and which must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'36'</td><td>'A'</td><td>'C', 'G', 'V', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'36'	'A'	'C', 'G', 'V', 'N'
Key Usage	Algorithm	Mode of Use						
'36'	'A'	'C', 'G', 'V', 'N'						
Start ATC	2 B	The start value for the Application Transaction Counter						
Number of DC_SUK	2 N	The number of DC_SUK blocks to generate. Value: '01'...'50'.						
CMK_CL_UMD	'X' + 16 B	This field is NOT present when Key Generation Option = '1' or '3'. User and Mobile Device Authentication Key for contactless transactions. 3DES ECB Encrypted under the transport KEK.						
CMK_RP_UMD	'X' + 16 B	This field is NOT present when Key Generation Option = '0' or '2'. User and Mobile Device Authentication Key for remote payments. 3DES ECB Encrypted under the transport KEK.						
CMK_CL_MD	'X' + 16 B	This field is NOT present when Key Generation Option = '1' or '3'. Mobile Device Authentication Key for contactless transactions. 3DES ECB Encrypted under the transport KEK.						
CMK_RP_MD	'X' + 16 B	This field is NOT present when Key Generation Option = '0' or '2'. User and Mobile Device Authentication Key for remote payments. 3DES ECB Encrypted under the transport KEK.						
CMK_IDN	'X' + 16 B	CDA Dynamic Number generation key encrypted 3DES ECB Encrypted under the transport KEK.						
Atalla Variant	2 N	Atalla variant; for use in systems with Atalla equipment. Must be set to '00' if not used.						
Transport KEK	'S' + n A	The transport KEK key encrypted under LMK key block and should comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'54'</td><td>'T', 'A'</td><td>'B', 'D', 'E', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'54'	'T', 'A'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'54'	'T', 'A'	'B', 'D', 'E', 'N'						
If Key Generation Option = '2', '3' or '4', the following 6 fields are omitted:								
Mobile PIN Block Length	2 N	The length of the Mobile PIN Block. Valid values: '08' or '16'.						
Mobile PIN Block	n B	The mobile PIN encrypted under the ZPK transport key						
ZPK	'S' + n A	Zone PIN key encrypted under LMK key block and should comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'P0', '72'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '72'	'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'T', 'A'	'B', 'D', 'N'						
Mobile PIN Block Format Code	2 N	The PIN Block format of the supplied Mobile PIN. Valid values are: '34': Standard EMV 1996 format '47': ISO 9564-1 PIN Block Format 3 (3DES) '48': ISO 9564-1 PIN Block Format 4 (AES)						

payShield 10K Core Host Commands

Field	Length & Type	Details
Primary Account Number (PAN) Length	2 N	Only present if Mobile PIN Block Format Code is '47' or '48'. The number of digits in the following Primary Account Number (PAN) field.
Primary Account Number (PAN)	n N	Only present if Mobile PIN Block Format Code is '47' or '48'. If Mobile PIN Block Format Code = '47', this is the 12-19 digits of the Primary Account Number (PAN), excluding the check digit. If Mobile PIN Block Format Code = '48', this is the 12-19 digits of the Primary Account Number (PAN), including the check digit.
Session Key Method	1 N	Value '1': EMV CSK
Single Use Key Method	1 N	Value '1': XOR
SUK_Info	1 B	For example, 0x38 to denote release 1.0 for Mastercard Cloud Based payments
DC_CP Hash Code	32 B	SHA 256 hash code over the Digitised Card Profile data DC_CP. The DC_CP will have been created using the 'IU' Generate Secure Message function which returns the hash code over the plain text DC-CP data.
RFU Byte	1 B	Set to 0x00 as reserved for future use.
Template Length	4 N	The length of the DC_SUK Template.
DC_SUK Template	n A	The DC_SUK template in JSON format into which the generated keys and input data will be inserted.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by licence; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IZ'.
Error Code	2 A	<p>'00': No error '06': Invalid YHHHHCC value '07': Invalid KCV type '20': Invalid PIN Block '23': Invalid PIN Block Format code '26': Invalid key scheme '27': Key Scheme (KEK) mismatch 'A1': Invalid LMK scheme 'D4': MS_KEY_CONF or Output KEK – key block error 'D5': MS_KEY_MAC – key block error 'DA': KEK – key block error 'DB': ZPK – key block error 'DC': KEK parity error 'DD': DK parity error 'E0': Invalid Mode Flag 'E1': CMK_CL_UMD key parity error 'E2': CMK_RP_UMD key parity error 'E3': CMK_CL_MD key parity error 'E4': CMK_RP_MD key parity error 'E5': CMK_IDN parity error 'E6': Invalid Session Key Method 'E7': Invalid Single Use Key method 'E8': ATC will exceed maximum value 'E9': Invalid DC_SUK block count specified 'EA': Invalid JSON Template 'EB': Missing entry in template 'EC': Invalid RFU byte 'ED': Invalid DC_SUK_ID length 'EF': Invalid Key Generation Option value 'F1': Invalid session key length 'F2': Mobile data Encryption key block error 'F3': Invalid PIN Block Decryption Key Type 'F4': Invalid Block Cipher 'F5': Invalid Block Cipher Mode 'F6': Mobile data decryption key error Or a standard error code.</p>
If Error Code = 'D4', 'D5', 'DA' or 'DB', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
Final ATC	2 B	The updated ATC value
DC_SUK Block Length	6 N	The length of the Encrypted DC_SUK Block to follow
Encrypted DC_SUK Block	n B	The DC_SUK Block will consist of 1 or more 116 byte DC_SUK containers AES encrypted using Counter Mode under the Remote Management MS_KEY_CONF session key.
Encrypted DC_SUK Block MAC	8 B	The MAC over the Encrypted DC_SUK Block using the MS_KEY_MAC session key and AES with MAC Algorithm 1 in ISO/IEC 9797-1 with padding method 2.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Digitized Card Single Use Keys (Mode Flag '1': MCBP SUK Derivation; include PIN; output in MC SDK JSON format)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Derive Single Use Keys (SUKs) for Mastercard Cloud Based Payments (MCBP). The user and mobile PINs will be used during the production of the SUKs. The keys will be output in Mastercard's SDK JSON format.

Notes: This command generates one or more DC_SUK blocks that contain the single use keys for user and mobile device authentication for contactless and remote payments, the ATC and the Dynamic Number for use in CDA.

For details of the JSON format used in the DC_SUK block, refer to *Card Issuing Appendix O – DC_SUK block template*.

The DC_SUK blocks are concatenated together and encrypted using the Remote Management Session key for confidentiality MS_KEY_CONF and MAC protected using the Remote Management Session key for integrity MS_KEY_MAC. The output is in the format suitable to loading directly to the Mobile Payment Application.

The ATC value is updated by this command according to the number of DC_SUK blocks generated.

The following input data elements will have been generated by the data preparation system using the 'KI' Generate Card Unique Keys function encrypted under a transport key:

- CMK_CL_UMD
- CMK_RP_UMD
- CMK_CL_MD
- CMK_RP_MD
- CMK_IDN

The transport keys will have been imported and encrypted under the Local Master Key.

The Mobile PIN block will be created using the PIN Translation commands and transported encrypted under a ZPK.

payShield 10K Core Host Commands

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IY'.						
Mode Flag	1 N	'1': MCBP SUK Derivation; include PIN; output in MC SDK JSON format						
Key Generation Option Delimiter	1 A	Value '\$'. Optional; if present, the following field must also be present.						
Key Generation Option	1 N	'0': Generate SUKs for Contactless Transactions (with PIN) '1': Generate SUKs for Remote Payment Transactions (with PIN) '2': Generate SUKs for Contactless Transactions (no PIN) '3': Generate SUKs for Remote Payment Transactions (no PIN) '4': Generate SUKs for Contactless & Remote Payment Transactions (no PIN)						
Message Counter	5 N	The message counter is maintained by the CMS and is incremented for each message sent from the CMS to MPA. Maximum value is 65535 or 0xFFFF.						
MS_KEY_CONF	'S' + n A	The Remote Management Session Key for message confidentiality, encrypted under AES Key Block LMK and which must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'35'</td><td>'A'</td><td>'B', 'D', 'E', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'35'	'A'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'35'	'A'	'B', 'D', 'E', 'N'						
MS_KEY_MAC	'S' + n A	The Remote Management Session Key for message integrity, encrypted under AES Key Block LMK and which must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'36'</td><td>'A'</td><td>'C', 'G', 'V', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'36'	'A'	'C', 'G', 'V', 'N'
Key Usage	Algorithm	Mode of Use						
'36'	'A'	'C', 'G', 'V', 'N'						
Start ATC	2 B	The start value for the Application Transaction Counter						
Number of DC_SUK	2 N	The number of DC_SUK blocks to generate. Value: '01'...'50'.						
CMK_CL_UMD	'X' + 16 B	This field is NOT present when Key Generation Option = '1' or '3'. User and Mobile Device Authentication Key for contactless transactions. 3DES ECB Encrypted under the transport KEK.						
CMK_RP_UMD	'X' + 16 B	This field is NOT present when Key Generation Option = '0' or '2'. User and Mobile Device Authentication Key for remote payments. 3DES ECB Encrypted under the transport KEK.						
CMK_CL_MD	'X' + 16 B	This field is NOT present when Key Generation Option = '1' or '3'. Mobile Device Authentication Key for contactless transactions. 3DES ECB Encrypted under the transport KEK.						
CMK_RP_MD	'X' + 16 B	This field is NOT present when Key Generation Option = '0' or '2'. User and Mobile Device Authentication Key for remote payments. 3DES ECB Encrypted under the transport KEK.						
CMK_IDN	'X' + 16 B	CDA Dynamic Number generation key encrypted 3DES ECB Encrypted under the transport KEK.						
Atalla Variant	2 N	Atalla variant; for use in systems with Atalla equipment. Must be set to '00' if not used.						
Transport KEK	'S' + n A	The transport KEK key encrypted under LMK key block and should comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'54'</td><td>'T', 'A'</td><td>'B', 'D', 'E', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'54'	'T', 'A'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'54'	'T', 'A'	'B', 'D', 'E', 'N'						
If Key Generation Option = '2', '3' or '4', the following 6 fields are omitted:								
Mobile PIN Block Length	2 N	The length of the Mobile PIN Block. Valid values: '08' or '16'.						
Mobile PIN Block	n B	The mobile PIN encrypted under the ZPK transport key						
ZPK	'S' + n A	Zone PIN key encrypted under LMK key block and should comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'P0', '72'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '72'	'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'T', 'A'	'B', 'D', 'N'						
Mobile PIN Block Format Code	2 N	The PIN Block format of the supplied Mobile PIN. Valid values are: '34': Standard EMV 1996 format '47': ISO 9564-1 PIN Block Format 3 (3DES) '48': ISO 9564-1 PIN Block Format 4 (AES)						
Primary Account Number (PAN) Length	2 N	Only present if Mobile PIN Block Format Code is '47' or '48'. The number of digits in the following Primary Account Number (PAN) field.						

Field	Length & Type	Details
Primary Account Number (PAN)	n N	Only present if Mobile PIN Block Format Code is '47' or '48'. If Mobile PIN Block Format Code = '47', this is the 12-19 digits of the PAN, excluding the check digit. If Mobile PIN Block Format Code = '48', this is the 12-19 digits of the PAN, including the check digit.
Session Key Method	1 N	'1': EMV CSK
Single Use Key Method	1 N	'1': XOR
SUK_Info	1 B	For example, 0x38 to denote release 1.0 for Mastercard Cloud Based payments
DC_CP Hash Code	32 B	SHA 256 hash code over the Digitised Card Profile data DC_CP. The DC_CP will have been created using the 'IU' Generate Secure Message function which returns the hash code over the plain text DC-CP data.
RFU Byte	1 B	Set to 0x00 as reserved for future use.
Template Length	4 N	The length of the DC_SUK Template.
DC_SUK Template	n A	The DC_SUK template in JSON format into which the generated keys and input data will be inserted.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by licence; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IZ'.
Error Code	2 A	<p>'00': No error '06': Invalid YHHHHCC value '07': Invalid KCV type '20': Invalid PIN Block '23': Invalid PIN Block Format code '26': Invalid key scheme '27': Key Scheme (KEK) mismatch 'A1': Invalid LMK scheme 'D4': MS_KEY_CONF or Output KEK – key block error 'D5': MS_KEY_MAC – key block error 'DA': KEK – key block error 'DB': ZPK – key block error 'DC': KEK parity error 'DD': DK parity error 'E0': Invalid Mode Flag 'E1': CMK_CL_UMD key parity error 'E2': CMK_RP_UMD key parity error 'E3': CMK_CL_MD key parity error 'E4': CMK_RP_MD key parity error 'E5': CMK_IDN parity error 'E6': Invalid Session Key Method 'E7': Invalid Single Use Key method 'E8': ATC will exceed maximum value 'E9': Invalid DC_SUK block count specified 'EA': Invalid JSON Template 'EB': Missing entry in template 'EC': Invalid RFU byte 'ED': Invalid DC_SUK_ID length 'EF': Invalid Key Generation Option value 'F1': Invalid session key length 'F2': Mobile data Encryption key block error 'F3': Invalid PIN Block Decryption Key Type 'F4': Invalid Block Cipher 'F5': Invalid Block Cipher Mode 'F6': Mobile data decryption key error Or a standard error code.</p>
If Error Code = 'D4', 'D5', 'DA' or 'DB', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
Final ATC	2 B	The updated ATC value
DC_SUK Block Length	6 N	The length of the Encrypted DC_SUK Block to follow
Encrypted DC_SUK Block	n B	The DC_SUK Block will consist of 1 or more 116 byte DC_SUK containers AES encrypted using Counter Mode under the Remote Management MS_KEY_CONF session key.
Encrypted DC_SUK Block MAC	8 B	The MAC over the Encrypted DC_SUK Block using the MS_KEY_MAC session key and AES with MAC Algorithm 1 in ISO/IEC 9797-1 with padding method 2.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Digitized Card Single Use Keys (Mode Flag '2': VCP LUK from Card Key)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Derive Limited Use Keys (LUKs) for Visa Cloud-based Payments.

Notes: Allows a Visa LUK to be generated from a unique card key generated with a previous call to 'KI' with Key Derivation Method 'A' or 'B'. 'IY' should be used instead of 'KI' by systems that do not store the PAN.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IY'.						
Mode Flag	1 N	'2': VCP LUK from Card Key						
DK (KEK)	1 A + 16 B	The derived unique key encrypted under the KEK.						
YHHHHCC	7 N	The Year/Hour/Counter value used to derive the Limited Use Key (LUK) to produce the Limited Use Cryptogram (LUC) where: Y (0-9) : least significant digit of current year HHHH (0001-8784) : number of hours since Jan 1st of the current year CC (00-99) : counter that starts at 00 at the beginning of each hour and is incremented by 1 each time a Limited Use Key is generated.						
Transport KEK	'S' + n A	The transport KEK key encrypted under LMK key block and should comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'54'</td> <td>'T'</td> <td>'B', 'D', 'E', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'54'	'T'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'54'	'T'	'B', 'D', 'E', 'N'						
Key Scheme	1 A	The Key scheme for encrypting the LUK key under KEK. Valid values are 'U' and 'X'. See the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> .						
Key Check Value Type	1 A	'0': KCV for entire key, 6 bytes long '1': KCV for entire key, 3 bytes long						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by licence; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IZ'.
Error Code	2 A	<p>'00': No error '06': Invalid YHHHHCC value '07': Invalid KCV type '20': Invalid PIN Block '23': Invalid PIN Block Format code '26': Invalid key scheme '27': Key Scheme (KEK) mismatch 'A1': Invalid LMK scheme 'D4': MS_KEY_CONF or Output KEK – key block error 'D5': MS_KEY_MAC – key block error 'DA': KEK – key block error 'DB': ZPK – key block error 'DC': KEK parity error 'DD': DK parity error 'E0': Invalid Mode Flag 'E1': CMK_CL_UMD key parity error 'E2': CMK_RP_UMD key parity error 'E3': CMK_CL_MD key parity error 'E4': CMK_RP_MD key parity error 'E5': CMK_IDN parity error 'E6': Invalid Session Key Method 'E7': Invalid Single Use Key method 'E8': ATC will exceed maximum value 'E9': Invalid DC_SUK block count specified 'EA': Invalid JSON Template 'EB': Missing entry in template 'EC': Invalid RFU byte 'ED': Invalid DC_SUK_ID length 'EF': Invalid Key Generation Option value 'F1': Invalid session key length 'F2': Mobile data Encryption key block error 'F3': Invalid PIN Block Decryption Key Type 'F4': Invalid Block Cipher 'F5': Invalid Block Cipher Mode 'F6': Mobile data decryption key error Or a standard error code.</p>
If Error Code = 'D4', 'D5', 'DA' or 'DB', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
LUK (KEK)	1 A + 16 B	The Limited Use Key, encrypted under the KEK according to the Key Scheme.
Key Check Value	6 B or 3 B	The key check value of the Limited Use Key.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Digitized Card Single Use Keys (Mode Flag '3': MCBP SK from MDES; add PIN; output encrypted SUK under KEK.)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Derive a Single Use Key (SUK) for Mastercard Cloud Based Payments (MCBP). The user and mobile PINs are used in the production of the SUK. The SUK is output encrypted under a supplied KEK.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IY'.						
Mode Flag	1 N	'3': MCBP SK from MDES; add PIN; output encrypted SUK under KEK						
Session Key Length	2 N	The length of the Session Key in bytes.						
Session Key	n B	The session key, encrypted under the transport key 'Mobile Data Decryption Key' using AES ECB						
Delimiter	1 A	Value ';'.						
Mobile Data Decryption Key	'S' + n A	The transport decryption key, encrypted under the LMK, and should comply with:						
		<table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'21'</td> <td>'A'</td> <td>'B', 'D', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'21'	'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'21'	'A'	'B', 'D', 'N'						
Mobile Data Encryption Key	'S' + n A	The transport encryption key, encrypted under the LMK, and should comply with:						
		<table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'21'</td> <td>'A'</td> <td>'B', 'E', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'21'	'A'	'B', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'21'	'A'	'B', 'E', 'N'						
Mobile PIN Block Decryption Key Type	1 N	Valid values are: '0': Mobile PIN Block encrypted under the LMK '1': Mobile PIN Block encrypted under ZPK						
Mobile PIN Block Length	2 N	Only present if Mobile PIN Block Decryption Key Type='1'. The length of the Mobile PIN Block. Value: '08' or '16'.						
Mobile PIN Block	n B or 'J' + 32 H	The encrypted Mobile PIN Block. The Mobile PIN Block, encrypted under the supplied ZPK. The Mobile PIN Block, encrypted under the (AES) LMK.						
ZPK		Only present if Mobile PIN Block Decryption Key Type is '1'. The Zone PIN Key, encrypted under the LMK.						
		<table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'P0', '72'</td> <td>'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'P0', '72'	'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'T', 'A'	'B', 'D', 'N'						
Mobile PIN Block Format Code	2 N	Only present if Mobile PIN Block Decryption Key Type is '1'. The PIN Block format of the supplied Mobile PIN. Valid values are: '34': Standard EMV 1996 format '47': ISO 9564-1 PIN Block Format 3 (3DES) '48': ISO 9564-1 PIN Block Format 4 (AES)						
Primary Account Number (PAN) Length	2 N	Only present if Mobile PIN Block Format Code is '47' or '48'. The number of digits in the following Primary Account Number (PAN) field.						
Primary Account Number (PAN)	n N	Only present if Mobile PIN Block Format Code is '47' or '48'. If Mobile PIN Block Format Code = '47', this is the 12-19 digits of the PAN, excluding the check digit. If Mobile PIN Block Format Code = '48', this is the 12-19 digits of the PAN, including the check digit.						

Field	Length & Type	Details
Single Use Key Method	1 N	The single use key generation method. Valid values are: Value: '1': XOR
Key Check Value Type	1 A	Valid values are: '0': KCV for entire key, 6 bytes long. '1': KCV for entire key, 3 bytes long.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by licence; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IZ'.
Error Code	2 A	<p>'00': No error '06': Invalid YHHHHCC value '07': Invalid KCV type '20': Invalid PIN Block '23': Invalid PIN Block Format code '26': Invalid key scheme '27': Key Scheme (KEK) mismatch 'A1': Invalid LMK scheme 'D4': MS_KEY_CONF or Output KEK – key block error 'D5': MS_KEY_MAC – key block error 'DA': KEK – key block error 'DB': ZPK – key block error 'DC': KEK parity error 'DD': DK parity error 'E0': Invalid Mode Flag 'E1': CMK_CL_UMD key parity error 'E2': CMK_RP_UMD key parity error 'E3': CMK_CL_MD key parity error 'E4': CMK_RP_MD key parity error 'E5': CMK_IDN parity error 'E6': Invalid Session Key Method 'E7': Invalid Single Use Key method 'E8': ATC will exceed maximum value 'E9': Invalid DC_SUK block count specified 'EA': Invalid JSON Template 'EB': Missing entry in template 'EC': Invalid RFU byte 'ED': Invalid DC_SUK_ID length 'EF': Invalid Key Generation Option value 'F1': Invalid session key length 'F2': Mobile data Encryption key block error 'F3': Invalid PIN Block Decryption Key Type 'F4': Invalid Block Cipher 'F5': Invalid Block Cipher Mode 'F6': Mobile data decryption key error Or a standard error code.</p>
If Error Code = 'D4', 'D5', 'DA' or 'DB', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
Single Use Key Length	2 N	The length of the Single Use Key.
Single Use Key	n B	The single use key, encrypted under the Mobile Data Encryption Key transport key, using AES ECB.
Key Check Value	6 B or 3 B	The key check value of the Limited Use Key.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Digitized Card Single Use Keys (Mode Flag '4': MCBP SUK Derivation; output encrypted under KEK)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Derive Single Use Keys (SUKs) for Mastercard Cloud-Based Payments (MCBP). No PIN is used in the production of the SUKs. The SUKs are output encrypted under a supplied KEK.

Notes: The following input data elements will have been generated by the data preparation system using the 'KI' Generate Card Unique Keys function encrypted under a transport key:

- CMK_CL_UMD
- CMK_RP_UMD
- CMK_CL_MD
- CMK_RP_MD
- CMK_IDN

The transport keys will have been imported and encrypted under the Local Master Key.

The Mobile PIN block will be created using the PIN Translation commands and transported encrypted under a ZPK.

The following keys are output, with their associated check value:

- SUK_CL_UMD
- SK_CL_MD
- SUK_RP_UMD
- SK_RP_MD

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IY'.						
Mode Flag	1 N	'4': MCBP SUK Derivation; output encrypted under KEK						
Key Generation Option Delimiter	1 A	Value '\$'. Optional; if present, the following field must also be present.						
Key Generation Option	1 N	'0': Generate SUKs for Contactless Transactions (with PIN) '1': Generate SUKs for Remote Payment Transactions (with PIN) '2': Generate SUKs for Contactless Transactions (no PIN) '3': Generate SUKs for Remote Payment Transactions (no PIN) '4': Generate SUKs for Contactless & Remote Payment Transactions (no PIN)						
Output KEK	'S' + n A	The Remote Management Session Key for message integrity, encrypted under AES Key Block LMK and which must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'54','21'</td><td>'T', 'A'</td><td>'B', 'D', 'E', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'54','21'	'T', 'A'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'54','21'	'T', 'A'	'B', 'D', 'E', 'N'						
Start ATC	2 B	The start value for the Application Transaction Counter						
Number of DC_SUK	2 N	The number of DC_SUK blocks to generate. Value: '01' ... '50'.						
CMK_CL_UMD	'X' + 16 B	This field is NOT present when Key Generation Option is specified as '1' or '3'. User and Mobile Device Authentication Key for contactless transactions. 3DES ECB Encrypted under the transport KEK.						
CMK_RP_UMD	'X' + 16 B	This field is NOT present when Key Generation Option is specified as '0' or '2'. User and Mobile Device Authentication Key for remote payments. 3DES ECB Encrypted under the transport KEK.						
CMK_CL_MD	'X' + 16 B	This field is NOT present when Key Generation Option is specified as '1' or '3'. Mobile Device Authentication Key for contactless transactions. 3DES ECB Encrypted under the transport KEK.						
CMK_RP_MD	'X' + 16 B	This field is NOT present when Key Generation Option is specified as '0' or '2'. User and Mobile Device Authentication Key for remote payments. 3DES ECB Encrypted under the transport KEK.						
CMK_IDN	'X' + 16 B	CDA Dynamic Number generation key encrypted 3DES ECB Encrypted under the transport KEK.						
Atalla Variant	2 N	Atalla variant; for use in systems with Atalla equipment. Must be set to '00' if not used.						
KEK	'S' + n A	The transport KEK key encrypted under LMK key block and should comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'54'</td><td>'T', 'A'</td><td>'B', 'D', 'E', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'54'	'T', 'A'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'54'	'T', 'A'	'B', 'D', 'E', 'N'						
If Key Generation Option is '2', '3' or '4', the following 6 fields are omitted:								
Mobile PIN Block Length	2 N	The length of the Mobile PIN Block. Valid values: '08' or '16'.						
Mobile PIN Block	n B	The mobile PIN encrypted under the ZPK transport key						
ZPK	'S' + n A	Zone PIN key encrypted under LMK key block and should comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'P0', '72'</td><td>'T', 'A'</td><td>'B', 'D', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '72'	'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'T', 'A'	'B', 'D', 'N'						
Mobile PIN Block Format Code	2 N	The PIN Block format of the supplied Mobile PIN. Valid values are: '34': Standard EMV 1996 format '47': ISO 9564-1 PIN Block Format 3 (3DES) '48': ISO 9564-1 PIN Block Format 4 (AES)						
Primary Account Number (PAN) Length	2 N	Only present if Mobile PIN Block Format Code is '47' or '48'. The number of digits in the following PAN field.						
Primary Account Number (PAN)	n N	Only present if Mobile PIN Block Format Code is '47' or '48'. If Mobile PIN Block Format Code = '47', this is the 12-19 digits of the PAN, excluding the check digit. If Mobile PIN Block Format Code = '48', this is the 12-19 digits of the PAN, including the check digit.						
Session Key Method	1 N	Value: '1': EMV CSK						
Single Use Key Method	1 N	Value: '1': XOR						
Block Cipher	1 N	The block cipher for encrypting the output single use keys. Valid values are:						

Field	Length & Type	Details
Block Cipher Mode	1 N	'0': AES (Output KEK Algorithm must be 'A') '1': 3DES (Output KEK Algorithm must be 'T') The block cipher mode used for encrypting the output single use keys. Valid values are: '0': CBC '1': ECB
IV	16 H or 32 H	The initialisation vector. Only present if Block Cipher Mode is '0'.
Key Check Value Type	1 A	Valid values are: '0': KCV for entire key, 6 bytes long '1': KCV for entire key, 3 bytes long
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by licence; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IZ'.
Error Code	2 A	<p>'00': No error '06': Invalid YHHHHCC value '07': Invalid KCV type '20': Invalid PIN Block '23': Invalid PIN Block Format code '26': Invalid key scheme '27': Key Scheme (KEK) mismatch 'A1': Invalid LMK scheme 'D4': MS_KEY_CONF or Output KEK – key block error 'D5': MS_KEY_MAC – key block error 'DA': KEK – key block error 'DB': ZPK – key block error 'DC': KEK parity error 'DD': DK parity error 'E0': Invalid Mode Flag 'E1': CMK_CL_UMD key parity error 'E2': CMK_RP_UMD key parity error 'E3': CMK_CL_MD key parity error 'E4': CMK_RP_MD key parity error 'E5': CMK_IDN parity error 'E6': Invalid Session Key Method 'E7': Invalid Single Use Key method 'E8': ATC will exceed maximum value 'E9': Invalid DC_SUK block count specified 'EA': Invalid JSON Template 'EB': Missing entry in template 'EC': Invalid RFU byte 'ED': Invalid DC_SUK_ID length 'EF': Invalid Key Generation Option value 'F1': Invalid session key length 'F2': Mobile data Encryption key block error 'F3': Invalid PIN Block Decryption Key Type 'F4': Invalid Block Cipher 'F5': Invalid Block Cipher Mode 'F6': Mobile data decryption key error Or a standard error code.</p>
If Error Code = 'D4', 'D5', 'DA' or 'DB', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
Each key will be encrypted under the 'Output KEK' using the 'Block Cipher'. If the optional 'Key Generation Option' delimiter was specified and the 'Key Generation Option' set to '0' or '2', the SUK_RP_UMD and SK_RP_MD keys with their KCVS will not be output. If the optional 'Key Generation Option' delimiter was specified and the 'Key Generation Option' set to '1' or '3', the SUK_CL_UMD and SK_CL_MD keys with their KCVS will not be output.		
ATC	4 H	Application Transaction Counter
Single Use Key Length	2 N	The length of the Single Use Keys
SUK_CL_UMD	n B	The Contactless Single Use Key for User and Mobile Device Authentication
SUK_CL_UMD KCV	6B or 3B	The key check value
SK_CL_MD	n B	The Contactless Single Use Key for Mobile Device Authentication
SK_CL_MD KCV	6B or 3B	The key check value
SUK_RP_UMD	n B	The Remote Payments Single Use Key for User and Mobile Device Authentication
SUK_RP_UMD KCV	6B or 3B	The key check value
SK_RP_MD	n B	The Remote Payment Single Use Key for Mobile Device Authentication
SK_RP_MD KCV	6B or 3B	The key check value
IDN	32 H	Dynamic Number in ASCII hexadecimal
Delimiter	1 A	'; Delimiter to denote end of keys generated using the ATC
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Digitized Card Single Use Keys (Mode Flag '5': LUK from Card Key with PIN)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Derive a Limited Use Key (LUK) using a proprietary derivation method. The mobile PIN is used in the production of the LUK.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IY'.						
Mode Flag	1 N	'5': Proprietary unique session key with PIN						
DK (KEK)	1 A + 16 B	The derived unique key encrypted under the KEK.						
YHHHHCC	7 N	The Year/Hour/Counter value used to derive the Limited Use Key (LUK) to produce the Limited Use Cryptogram (LUC) where: Y (0-9) : least significant digit of current year HHHH (0001-8784) : number of hours since Jan 1st of the current year CC (00-99) : counter that starts at 00 at the beginning of each hour and is incremented by 1 each time a Limited Use Key is generated.						
KEK	'S' + n A	The transport KEK key encrypted under LMK key block and should comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'54'</td> <td>'T'</td> <td>'B', 'D', 'E', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'54'	'T'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'54'	'T'	'B', 'D', 'E', 'N'						
Key Scheme	1 A	The Key scheme for encrypting the LUK key under KEK. Valid values are 'U' and 'X'. See the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> .						
Key Check Value Type	1 A	'0': KCV for entire key, 6 bytes long '1': KCV for entire key, 3 bytes long						
Single Use Key Method	1 N	Method by which the PIN is combined with the LUK '1': XOR						
Mobile PIN Block Length	2 N	The length of the Mobile PIN Block.						
Mobile PIN Block	n B	The mobile PIN encrypted under the ZPK.						
ZPK	'S' + n A	The Zone PIN Key, encrypted under the LMK and should comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '72'</td> <td>'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '72'	'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'T', 'A'	'B', 'D', 'N'						
Mobile PIN Block Format Code	2 N	The PIN Block format of the supplied Mobile PIN. Valid values are: '34': Standard EMV 1996 format '47': ISO 9564-1 PIN Block Format 3 (3DES) '48': ISO 9564-1 PIN Block Format 4 (AES)						
Primary Account Number (PAN) Length	2 N	Only present if Mobile PIN Block Format Code is '47' or '48'. The number of digits in the following PAN field.						
Primary Account Number (PAN)	n N	Only present if Mobile PIN Block Format Code is '47' or '48'. If Mobile PIN Block Format Code = '47', this is the 12-19 digits of the PAN, excluding the check digit. If Mobile PIN Block Format Code = '48', this is the 12-19 digits of the PAN, including the check digit.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by licence; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IZ'.
Error Code	2 A	<p>'00': No error '06': Invalid YHHHHCC value '07': Invalid KCV type '20': Invalid PIN Block '23': Invalid PIN Block Format code '26': Invalid key scheme '27': Key Scheme (KEK) mismatch 'A1': Invalid LMK scheme 'D4': MS_KEY_CONF or Output KEK – key block error 'D5': MS_KEY_MAC – key block error 'DA': KEK – key block error 'DB': ZPK – key block error 'DC': KEK parity error 'DD': DK parity error 'E0': Invalid Mode Flag 'E1': CMK_CL_UMD key parity error 'E2': CMK_RP_UMD key parity error 'E3': CMK_CL_MD key parity error 'E4': CMK_RP_MD key parity error 'E5': CMK_IDN parity error 'E6': Invalid Session Key Method 'E7': Invalid Single Use Key method 'E8': ATC will exceed maximum value 'E9': Invalid DC_SUK block count specified 'EA': Invalid JSON Template 'EB': Missing entry in template 'EC': Invalid RFU byte 'ED': Invalid DC_SUK_ID length 'EF': Invalid Key Generation Option value 'F1': Invalid session key length 'F2': Mobile data Encryption key block error 'F3': Invalid PIN Block Decryption Key Type 'F4': Invalid Block Cipher 'F5': Invalid Block Cipher Mode 'F6': Mobile data decryption key error Or a standard error code.</p>
If Error Code = 'D4', 'D5', 'DA' or 'DB', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
LUK (KEK)	1 A + 16 B	The Limited Use Key, encrypted under the KEK according to the Key Scheme.
Key Check Value	6 B or 3 B	The key check value of the Limited Use Key.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Remote Management Session ID and Session Keys

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Generate Remote Management Session ID and Session Keys

Notes: The random Session ID is generated by the host Credentials Management System (CMS) to uniquely identify a remote management session between the Mobile Payment Application (MPA) and the host CMS.

The Remote Management Session keys are derived from the M_KEY_CONF and M_KEY_MAC keys and Session ID.

The M_KEY_CONF and M_KEY_MAC are generated using the 'A0' Generate Key command.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IO'.						
Control Bits	1 B	Mastercard defined version control and options. For example, set to 0x80 for Release 1.0 for Mastercard Cloud-Based Payments.						
Expiry Date	6 N	Expiry date for the session, in the format 'YYMMDD', where: YY (00-99): least significant 2 digits of the year of the expiry date; MM (01-12): month of expiry date; DD (01-31): day of expiry date; Note this value is not validated by this command.						
Remote Management Info	6 H	Defined by Mastercard. For example: '810000': when provisioning card profile DC_CP '820000': when provisioning key profile DC_SUK						
M_KEY_CONF	'S' + n A	The Remote Management Master Key for message confidentiality, encrypted under AES Key Block LMK and which must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'33'</td> <td>'A'</td> <td>'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'33'	'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'33'	'A'	'X', 'N'						
M_KEY_MAC	'S' + n A	The Remote Management Master Key for message integrity, encrypted under AES Key Block LMK and which must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'34'</td> <td>'A'</td> <td>'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'34'	'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'34'	'A'	'X', 'N'						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by licence; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details						
RESPONSE MESSAGE								
Message Header	m A	Returned to the Host unchanged.						
Response Code	2 A	Value 'IP'.						
Error Code	2 A	'00': No error '15': Expiry Date not numeric 'A1': Invalid LMK scheme 'D1': M_KEY_CONF – key block error 'D2': M_KEY_MAC – key block error Or a standard error code						
If Error Code = 'D1' or 'D2', the following field will be present:								
Additional Error Code	2 A	The key block specific error code.						
If Error Code = '00', the following 5 fields will be present:								
Encrypted Session ID under LMK	32 B	The Session ID encrypted under the LMK for local use.						
Encrypted Session ID under M_KEY_CONF	32 B	The Session ID encrypted under M_KEY_CONF using AES and ECB mode for transfer to MPA.						
Session ID MAC	8 B	MAC over Session ID using M_KEY_MAC and AES with MAC Algorithm 1 in ISO/IEC 9797-1, padding method 2.						
MS_KEY_CONF	'S' + n A	The Remote Management Session Key for message confidentiality, encrypted under the AES Key Block LMK. <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'35'</td> <td>'A'</td> <td>'B'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'35'	'A'	'B'
Key Usage	Algorithm	Mode of Use						
'35'	'A'	'B'						
MS_KEY_MAC	'S' + n A	The Remote Management Session Key for message integrity, encrypted under the AES Key Block LMK. <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'36'</td> <td>'A'</td> <td>'C'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'36'	'A'	'C'
Key Usage	Algorithm	Mode of Use						
'36'	'A'	'C'						
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.						
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.						

3.4 Mastercard Key Management (OBKM) Commands

The commands in this section allow the Card Issuer to set up the appropriate RSA keys required for the MasterCard OBKM Three-level key management hierarchy process. The following step by step description shows how the commands are intended to be used.

i) The Issuer creates his own RSA keyset by using the *Generate Issuer RSA Key Set* command. The key length will have to be defined (typically 512, 640, 768, 896 or 1024 bits) and the public exponent chosen. The Private Key part of the keyset is returned to the host system encrypted under the HSM's Local Master Key. This must be stored on the host database. The Public Key (PK) part of the keyset is also returned to the host system in two formats; a self-signed certificate and the Public Key protected with a MAC. The self-signed certificate is in the format required for transportation to the scheme Certification Authority (CA). It is normally transferred directly to suitable transport media for transport to the Certification Authority. The exact format details of how the self-signed PK certificate is written to the media is to be determined by the scheme provider (MasterCard).

If the PK is to be stored on the local database it is recommended that it is protected from alteration by storing the MAC as well. In this way, the authenticity of the PK can be later verified using the *Validate a Public Key* command.

ii) The MasterCard KMC will read the self-signed PK certificate from the transport media. The Certification Authority PK(s) (in the form of self-signed certificate(s)) will be written to a transport media for transportation back to the Issuer.

iii) The Issuer reads the transport media and places the CA PK(s) on the host database. The certificates are then verified. First it is necessary to verify the CA self-signed certificate(s) using the *Validate Certification Authority Self-Signed Certificate* command. This command returns the CA Public Key and a MAC which should be stored for later use.

iv) During the key transport process it is necessary to have available the appropriate Issuer Private Key (SK) within the HSM. It may be held (in encrypted form) on the host database and sent to the HSM every time it is used. Alternatively, to save on communication time, it may be pre-loaded into each HSM requiring it using the *Load a Private Key* command. It is the responsibility of the host application to keep track of the SK loaded at any time. Different HSM configurations can store a different number of SK(s) simultaneously. In this case the stored SK is referenced by a Key Index number.

v) At infrequent intervals it is normal to change the Local Master Keys (LMKs) of the HSMs. When this happens it is necessary to translate all keys encrypted under the old LMKs to encryption under the new LMKs. The Private Key(s) can be translated using the *Translate a Private Key* host command. The MACs protecting the Public Key(s) can be translated using the *Translate a Public Key* command.

The payShield 10K provides the following host commands to Mastercard key management (OBKM):

Function	Command	Page
<i>Generate an Issuer RSA Key Set</i>	J0 (J1)	138
<i>Validate a CA Self-Signed Certificate</i>	JO (JP)	140
<i>Import Transport Key Set</i>	R8 (R9)	141
<i>Export Magnetic Stripe Card Key Set</i>	R6 (R7)	143
<i>Export Chip Card Key Set (2002 & 2003 Version)</i>	R4 (R5)	145
<i>Export Chip Card Key Set (2007 Version)</i>	R4 (R5)	149

Generate an Issuer RSA Key Set

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Required	
Activity: generate.rsa-sk.host	

Function: To generate an Issuer RSA Key Set and return the Public Key in the form of a MasterCard-format Self-Signed Issuer Public Key Certificate.

Notes: Depending on key size, this function may take up to a minute or more to execute. This command may be used with either an odd Public Exponent or a Public Exponent = 2. This command uses the "MasterCard" method of generating key pairs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'J0' (J-zero).
Hash Identifier	2 N	Identifier of algorithm used to hash data.
Signature Identifier	2 N	Identifier of signature algorithm.
Key Length	4 N	Modulus length in bits (must be a multiple of 8) Range: '0400' – '2040'.
Data Block	10 B	Data block to be included in the Self-Signed Certificate (comprises Certificate Subject ID (5 bytes), Expiry Date (2 bytes) and Certificate Serial Number (3 bytes)).
Issuer Public Key Index	3 B	Issuer Public Key Index.
Authentication Data	n A	Optional; additional data to be included in the MAC calculation (must not include ';').
Delimiter	1 A	Delimiter to indicate end of Authentication Data field: Value ':'.
Public Exponent Length	4 N	Optional; length in bits of the Public Exponent; must be supplied if Public Exponent present in command message.
Public Exponent	n B	Optional; if supplied then it must be odd or equal to 2; if not supplied then a default exponent of 65537 is assumed.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'J1'.
Error Code	2 N	'00': No error '04': Key length error '05': Invalid hash identifier '06': Invalid signature identifier '07': Public exponent length error '08': Invalid public exponent or a standard error code.
MAC	4 B	MAC on Public Key and Authentication Data calculated using LMK 36-37.
Public Key	n B	Public Key, DER encoded in ASN.1 format (sequence of modulus and exponent).
Certificate Length	4 N	Length in bytes of Self-Signed Certificate.
Self-Signed Issuer Public Key Certificate	n B	Self-Signed Issuer Public Key Certificate (the concatenation of the Clear Data and the Self-Signed Certificate).
Hash Length	2 N	Length in hex characters of hash result in next field. This length will depend on the hash algorithm specified in the command message. For SHA-1, this length will be 40.
Hash Value	n H	Hash value of self signed Issuer Public Key data.
Private Key Length	4 N	Length (in bytes) of the Private Key field.
Private Key	n B	Private Key, encrypted using LMK pair 34-35.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Validate a CA Self-Signed Certificate

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Required	
Activity: import.rsa-sk.host	

Function: To validate a MasterCard-style Self-Signed Certification Authority (CA) Certificate.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'JO' (J-Oh).
Certificate Length	4 N	Length (in bytes) of CA Self-Signed Certificate.
CA Self-Signed Certificate	n B	CA Self-Signed Certificate (concatenation of the Clear Data and the Self-Signed Certificate).
Delimiter	1 A	Delimiter, value ':'.
Authentication Data	n A	Optional; additional data to be included in the MAC calculation (must not include ';').
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'JP'.
Error Code	2 N	'00': No error '02': Hash validation failure '05': Invalid hash algorithm '06': Invalid public key algorithm indicator '08': Invalid public key '80': Certificate length error '81': Invalid certificate header '82': Invalid trailer '83': Invalid certificate format '84': Invalid subject ID '85': Invalid public key data or a standard error code.
MAC	4 B	MAC on Public Key and Authentication Data, calculated using LMK 36-37.
Public Key	n B	Public key, DER encoded in ASN.1 format (sequence of modulus, exponent).
Hash Length	2 N	Length in hex characters of hash result in next field. This length will depend on the hash algorithm specified in the command message. For SHA-1, this length will be 40.
Hash Value	n H	Hash value of self signed CA Public Key data.
Expiry Date	2 D	The Certificate Expiry Date (MMYY) recovered from the certificate.
Certificate Serial Number	3 B	The Certificate Serial Number recovered from the certificate.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Import Transport Key Set

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not Required	

Function: To import the transport keys generated by the KMC.

Notes: The output from this function is a double length key used to encrypt keys sent from the MasterCard KMC (BKEM) and a double length key used to MAC keys sent from the MasterCard KMC (BKAM).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'R8'.
KMC Sequence Number	8 B	Sequence number generated by KMC.
Member ID	10 N	The ID of the member this key set is intended for.
Transport Key Set ID	4 N	Identifier of the set BKEM, BKAM, as given by the KMC.
MAC on Public Key	4 B	MAC on the MasterCard Public key.
Public Key	n B	MasterCard Public Key, DER encoded in ASN.1 format (sequence of modulus and exponent).
Delimiter	1 A	Value ';'.
Signature Length	4 N	Length of signature block (T). This is a two byte signed integer with Most Significant Byte first.
Signature Block	T B	Signature generated using the MasterCard private key.
Delimiter	1 A	Value ';'.
Private Key Length	4 N	Length (in bytes) of the following Private Key field.
Private Key	n B	Member's Private Key, encrypted using LMK pair 34-35.
Delimiter	1 A	Value ';'.
Encrypted Key Length	4 N	Length of encrypted key (S). This is a two byte signed integer with Most Significant Byte first.
Encrypted BKEM	S B	BKEM encrypted with the member's public key.
Encrypted BKAM	S B	BKAM encrypted with the member's public key.
Delimiter	1 A	Value ';'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

payShield 10K Core Host Commands

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'R9'.
Error Code	2 N	'00': No error '51': Invalid message header '52': Invalid MAC algorithm number '53': Invalid Signature '54': Invalid BKAM data format '55': Invalid BKEM data format '56': BKAM parity error '57': BKEM parity error '58': Invalid MAC on Public Key or a standard error code.
BKAM	1 A + 32 H	BKAM encrypted under LMK pair 22-23 variant 6.
BKEM	1 A + 32 H	BKEM encrypted under LMK pair 22-23 variant 5.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Export Magnetic Stripe Card Key Set

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To export a member's magnetic stripe key set for transport to the KMC.

Notes: The output from this function is a set of double length keys encrypted under the BKEM, together with a MAC over the key set, calculated using the BKAM.
Some of the keys in the key set may be set to 'all zeroes' to indicate they are not used.
The ESP sequence number is created from the date/time in BCD = YYYYMMDDhhmmss00.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'R6'.
Delimiter	1 A	Optional. If present the following field must be present. Value ':'.
OBKM Version	1 A	'0': September 2002 Specification '1': April 2003 Specification (Version = 01 02). Only present if above Delimiter is present.
Member ID	10 N	Identifier for the member, as defined by the KMC.
Key Set Reference	4 N	Reference of the Magnetic Stripe Card Keys provided in this key set, as defined by the member.
Floor Expiry Date for key set	4 N	Expiry Date in format MMYY.
PAN Range for Key Set	38 N	Concatenation of 19 digits formed of PAN-low left padded by 0s and 19 digits formed of PAN-high left padded by 0s.
PVKI	1 N	Index of PVV, '0' to '9'.
PVV Key	1 A + 32 H	Double length PVV key, encrypted under LMK pair 14-15 using Key Encryption Scheme U.
Extra PVV Key Information	12 N	Extra data linked to the key.
CVC1	1 A + 32 H	Double length CVC1 key, encrypted under LMK 14-15 variant 4 using Key Encryption Scheme U.
Extra CVC1 Key Information	11 N	Extra data linked to the key.
CVC2	1 A + 32 H	Double length CVC2 key, encrypted under LMK 14-15 variant 4 using Key Encryption Scheme U.
Extra CVC2 Key Information	7 N	Extra data linked to the key.
Transport Key ID	4 N	Key ID of the BKAM BKEM pair used.
MAC algorithm	1 N	MAC algorithm parameters to be used with BKAM: '2', '3', '4' or '6': as defined in ISO/IEC 9797-1.
BKAM	1 A + 32 H	BKAM encrypted under LMK pair 22-23 variant 6.
BKEM	1 A + 32 H	BKEM encrypted under LMK pair 22-23 variant 5.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19'.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'R7'.
Error Code	2 N	'00': No error '08': BKAM parity error '09': BKEM parity error '10': PVV key parity error '11': CVC Key1 parity error '50': CVC Key2 parity error '51': Invalid message header or a standard error code.
ESP Sequence Number	16 H	Sequence Number from the ESP.
Encrypted PVV Key	32 H	BKEM Encrypted PVV Key.
PVV Key CV	3 B	Check Value on PVV.
Encrypted CVC1 Key	32 H	BKEM Encrypted CVC1 Key.
CVC1 Key CV	3 B	Check Value on CVC1.
Encrypted CVC2 Key	32 H	BKEM Encrypted CVC2 Key.
CVC2 Key CV	3 B	Check Value on CVC2.
MAC	16 H	MAC calculated over key set data using BKAM.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Export Chip Card Key Set (2002 & 2003 Version)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To export a member's chip card key set for transport to the KMC.

Notes: The output from this function is a set of double length keys encrypted under the BKEM, together with a MAC over the key set, calculated using the BKAM.

Some of the keys in the key set may be set to 'all zeroes' to indicate they are not used.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'R4'.
Delimiter	1 A	Optional. If present the following field must be present. Value ';'.
OBKM Version	1 A	'0': September 2002 Specification '1': April 2003 Specification (Version = 02 02) Only present if above Delimiter is present.
Member ID	10 N	Identifier for the member, as defined by the KMC.
Key Set Reference	4 N	Reference of the Magnetic Stripe Card Keys provided in this key set, as defined by the member.
Floor Expiry Date for key set	4 N	Expiry Date in format MMYY.
PAN Range for Key Set	38 N	Concatenation of 19 digits formed of PAN-low left padded by 0s and 19 digits formed of PAN-high left padded by 0s.
Key Derivation Index	3 N	Index for the Key Set.
Cryptogram Version Number	1 B	
IMKac	1 A + 32 H	Double length IMKac, encrypted under LMK pair 28-29 Variant 1, using Key Encryption Scheme U.

Field	Length & Type	Details
Extra IMKac Key Data (8 fields)		
Decision Matrix in case of Invalid Cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
ICC Master Key Derivation Algorithm ID	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme.
Session Key Derivation Algorithm ID (SKD)	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme.
ARQC/ARPC Algorithm ID	1 N	'1': reserved for future use.
Issuer Application Data Layout	1 N	'1': M/Chip Lite 2.1 and M/Chip 4 schemes '2': M/Chip Select 2.0.5 scheme.
H	2 N	Height of the tree. Only present if SKD = '4'.
B	2 N	Branch of the tree. Only present if SKD = '4'.
IMKsmi	1 A + 32 H	Double length IMKsmi, encrypted under LMK pair 28-29 Variant 2, using Key Encryption Scheme U.
Extra IMKsmi Key Data (5 fields)		
ICC Master Key Derivation Algorithm ID	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme.
Session Key Derivation Algorithm ID (SKD)	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme.
MAC Algorithm ID	1 N	'1': reserved for future use.
H	2 N	Height of the tree. Only present if SKD = '4'.
B	2 N	Branch of the tree. Only present if SKD = '4'.
IMKsmc	1 A + 32 H	Double length IMKsmc encrypted under LMK pair 28-29 Variant 3, using Key Encryption Scheme U.
Extra IMKsmc Key Data (5 fields)		
ICC Master Key Derivation Algorithm ID	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme.
Session Key Derivation Algorithm ID (SKD)	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme.
Encryption Algorithm ID	1 N	'1': reserved for future use.
H	2 N	Height of the tree. Only present if SKD = '4'.
B	2 N	Branch of the tree. Only present if SKD = '4'.
IMKidn	1 A + 32 H	Double length IMKidn, encrypted under LMK pair 28-29 Variant 5, using Key Encryption Scheme U.

Field	Length & Type	Details
Extra IMKldn Key Data (4 fields)		
Decision Matrix in case of invalid cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
ICC Master Key Derivation Algorithm ID	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme.
IDN Algorithm ID	1 N	'1': reserved for future use.
IMKdac	1 A + 32 H	Double length IMKdac, encrypted under LMK pair 28-29 Variant 4, using Key Encryption Scheme U.
Extra IMKdac Key Data (3 fields)		
Decision Matrix in case of invalid cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
DAC Algorithm ID	1 N	'1': reserved for future use.
Transport Key ID	4 N	Key ID of the BKAM, BKEM used.
MAC algorithm	1 N	MAC algorithm to be used with BKAM, '2', '3', '4' or '6': as defined in ISO/IEC 9797-1.
BKAM	1 A + 32 H	BKAM encrypted under LMK pair 22-23, variant 6.
BKEM	1 A + 32 H	BKEM encrypted under LMK pair 22-23, variant 5.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'R5'.
Error Code	2 N	'00': No error '08': BKAM parity error '09': BKEM parity error '10': IMKac parity error '11': IMKsmi parity error '50': IMKsmc parity error '51': Invalid message header '52': IMKidn parity error '53': IMKdac parity error or a standard error code.
ESP Sequence Number	16 H	Sequence Number from the ESP.
Encrypted IMKac	32 H	BKEM Encrypted Key.
IMKac Key Check Value	3 B	
Encrypted IMKsmi	32 H	BKEM Encrypted Key.
IMKsmi Key Check Value	3 B	
Encrypted IMKsmc	32 H	BKEM Encrypted Key.
IMKsmc Key Check Value	3 B	
Encrypted IMKidn	32 H	BKEM Encrypted Key.
IMKidn Key Check Value	3 B	
Encrypted IMKdac	32 H	BKEM Encrypted Key
IMKdac Key Check Value	3 B	
MAC	16 H	MAC calculated over key set data using BKAM.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Export Chip Card Key Set (2007 Version)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To export a member's chip card key set for transport to the KMC.

Notes: The output from this function is a set of double length keys encrypted under the BKEM, together with a MAC over the key set, calculated using the BKAM.

Some of the keys in the key set may be set to 'all zeroes' to indicate they are not used.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'R4'.
Delimiter	1 A	Value ';'.
OBKM Version	1 A	'2': September 2007 Specification (Version = 02 05)
Member ID	10 N	Identifier for the member, as defined by the KMC.
Key Set Reference	4 N	Reference of the Magnetic Stripe Card Keys provided in this key set, as defined by the member.
Floor Expiry Date for key set	4 N	Expiry Date in format MMYY.
PAN Range for Key Set	38 N	Concatenation of 19 digits formed of PAN-low left padded by 0s and 19 digits formed of PAN-high left padded by 0s.
Key Derivation Index	3 N	Index for the Key Set.
Cryptogram Version Number	1 B	
IMKac	1 A + 32 H	Double length IMKac, encrypted under LMK pair 28-29 Variant 1, using Key Encryption Scheme U.

Field	Length & Type	Details
Extra IMKac Key Data (14 fields)		
Decision Matrix in case of Invalid Cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '055': Invalid PIN '057': Transaction not permitted to Cardholder '075': Allowable number of PIN tries exceeded '086': PIN Validation not possible.
Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '055': Invalid PIN '057': Transaction not permitted to Cardholder '075': Allowable number of PIN tries exceeded '086': PIN Validation not possible.
Decision Matrix in case of invalid TVR/CVR	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '055': Invalid PIN '057': Transaction not permitted to Cardholder '075': Allowable number of PIN tries exceeded '086': PIN Validation not possible.
Decision Matrix in case cryptogram is not an ARQC	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '055': Invalid PIN '057': Transaction not permitted to Cardholder '075': Allowable number of PIN tries exceeded '086': PIN Validation not possible. <i>Supported on Banknet only.</i>
ICC Master Key Derivation Algorithm ID	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme '5': CCD scheme
Card Application Identifier (CAI)	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme '5': CCD scheme
ARQC/ARPC Algorithm ID	1 N	'1': M/Chip schemes '2': CCD scheme
CVN Position Indicator	1 N	Indicates the position of CVN (Cryptogram Version Number) sub-element with tag 9F10 (Issuer Application Data): '1': 2 nd byte of tag 9F10 – for M/Chip scheme (M/Chip 2.1 Lite and M/Chip 4.0 and CCD) '2': 3 rd byte of 9F10 – for VSDC scheme (M/Chip 2.0.5 Select).
H	2 N	If CAI = '1', this field should be set to '00'. If CAI = '4' or '5': Height factor of the EMV 2000 session key derivation algorithm. Acceptable values: If CAI = '4': '8' or '16' If CAI = '5': '8'.
b	2 M	If CAI = '1', this field should be set to '00'. If CAI = '4' or '5': Branch factory of the EMV 2000 session key derivation algorithm. Acceptable values: If CAI = '4': '2' (if H='16') or '4' (if H='8') If CAI = '5': '4'.

Field	Length & Type	Details
ARC if transaction accepted	8 H	If CAI = '1', this field should be set to '00000000'. If CAI = '4' or '5', this field specifies the ARPC Response Code for an approved transaction.
ARC if transaction rejected	8 H	If CAI = '1', this field should be set to '00000000'. If CAI = '4' or '5', this field specifies the ARPC Response Code for a declined transaction.
TVR/CVR bitmask and expected value	44 H	TVR/CVR bitmask and expected value needed by Mastercard Chip On-behalf Services to check transaction TVR and CVR data elements on behalf of the issuer. Filled with 44 digits '0' if not used.
POS Terminal PAN Entry Mode	2 N	This parameter gives the issuers the flexibility to use, for the same PAN range, floor expiry date and Key Derivation Index, a different chip cryptography type, specified through field 6 (Card Application Identifier) above, depending on the value of DE22 SF1. Allowed values: '05': M/Chip contact '07': M/Chip contactless. <i>Supported on Banknet only.</i>
Transport Key ID	4 N	Key ID of the BKAM, BKEM used.
MAC algorithm	1 N	MAC algorithm to be used with BKAM, '2', '3', '4' or '6': as defined in ISO/IEC 9797-1.
BKAM	1 A + 32 H	BKAM encrypted under LMK pair 22-23, variant 6.
BKEM	1 A + 32 H	BKEM encrypted under LMK pair 22-23, variant 5.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'R5'.
Error Code	2 N	'00': No error '08': BKAM parity error '09': BKEM parity error '10': IMKac parity error '51': Invalid message header or a standard error code.
ESP Sequence Number	16 H	Sequence Number from the ESP.
Encrypted IMKac	32 H	IMKac encrypted under BKEM.
IMKac Key Check Value	3 B	The check value of the IMKac.
MAC	16 H	MAC calculated over key set data using BKAM.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

3.5 AS2805 Key Management Commands

The payShield 10K provides the following host commands to AS2805 key management:

Function	Command	Page
<i>Generate a Set of Zone Keys</i>	OI (OJ)	154
<i>Translate a Set of Zone Keys to Encryption under the</i>	OK (OL)	156
<i>Generate Initial Terminal Master Keys (AS2805 – 2001)</i>	C0 (C1)	159
<i>Update Terminal Master Key 1</i>	OU (OV)	161
<i>Update Terminal Master Keys</i>	OW (OX)	163
<i>Generate a Set of Terminal Keys</i>	PI (PJ)	165
<i>Generate an Acquirer Master Key Encrypting Key</i>	C8 (C9)	168
<i>Translate an Acquirer Master Key Encrypting Key</i>	D6 (D7)	170
<i>KEKGEN – 6.3</i>	F6 (F7)	172
<i>KEKREC – 6.3</i>	F8 (F9)	174
<i>Generate a KCA and KMACH</i>	E8 (E9)	176
<i>Generate a KEKs for use in Node to Node interchange using RSA</i>	H4 (H5)	178
<i>Receive a KEKr for use in Node to Node interchange using RSA</i>	H6 (H7)	180
<i>Decrypt a PIN Pad Public Key</i>	H0 (H1)	182
<i>Encrypt a Cross Acquirer Key Encrypting Key under an Initial Transport Key</i>	H8 (H9)	184
<i>Encrypt a Terminal Key under the LMK</i>	I0 (I1)	186

Generate a Set of Zone Keys

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate a Zone PIN Key (ZPK), Zone Authentication Key (ZAK) and Zone Encryption Key (ZEK) and return each key encrypted under their appropriate variants of a Key Encrypting Key Send (KEKs) / Zone Master Key (ZMK) and the appropriate LMK pair.

Notes: Each of the zone keys will be adjusted for odd parity on each byte. A check value for each key will be generated (as defined in *AS2805 Appendix C – Key Check Value*). The definition of each of the KEKs / ZMK variants is given in *AS2805 Appendix D – Key Encrypting Key Variants*.

If the Key type flag is used, the key scheme must also be used.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value '01'
KEKs / Zone Master Key	32 H or 1 A + 32 H or 1 A + 48 H	KEKs, encrypted under LMK pair 04-05 variant 4 or ZMK, encrypted under LMK pair 04-05
Delimiter	1 A	Optional: If present the following three fields must be present. Value ':'
Key Scheme KEKs / ZMK	1 A	Optional. Key Scheme for encrypting keys under KEKs / ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Delimiter	1 A	Optional: If present the following field must be present. Value ':'
Key type Flag	1 N	Optional flag to indicate if KEKs or ZMK is used. 1 = KEKs; 2 = ZMK ONLY AVAILABLE IF PRECEDING KEY SCHEME IS USED
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'OJ'
Error Code	2 N	'00': No errors '10': ZMK parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '26': Invalid Key Scheme '27': Incompatible key length '28': Invalid key type
PIN Key (LMK)	16 H or 1 A + 32 H or 1 A + 48 H	ZPK, encrypted under LMK pair 06-07
PIN Key (ZMK)	16 H or 1 A + 16 H or 1 A + 32 H or 1 A + 48 H	ZPK, encrypted under appropriate variant of ZMK
ZPK Check Value	6 H	Check value (KCV) for ZPK
Authentication Key (LMK)	16 H or 1 A + 32 H or 1 A + 48 H	ZAK, encrypted under LMK pair 26-27 variant 1
Authentication Key (ZMK)	16 H or 1 A + 16 H or 1 A + 32 H or 1 A + 48 H	ZAK, encrypted under appropriate variant of ZMK
ZAK Check Value	6 H	Check value (KCV) for ZAK
Encryption Key (LMK)	16 H or 1 A + 32 H or 1 A + 48 H	ZEK, encrypted under LMK pair 30-31 variant 1
Encryption Key (ZMK)	16 H or 1 A + 16 H or 1 A + 32 H or 1 A + 48 H	ZEK, encrypted under appropriate variant of ZMK
ZEK Check Value	6 H	Check value (KCV) for ZEK
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate a Set of Zone Keys to Encryption under the LMK

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To translate a Zone PIN Key (ZPK) and/or a Zone Authentication Key (ZAK) and/or a Zone Encryption Key (ZEK) from encryption under a Key Encrypting Key Receive (KEKr) / Zone Master Key (ZMK) to encryption under the appropriate LMK pair.

Notes: The command will translate one, two or all three key types depending on the state of the key flags. If a flag is set ('1') the key is to be translated. If the flag is clear ('0') the input key (ZPK, ZAK or ZEK) will not be translated but the HSM will generate a random value and return it in clear as the key (ZPK, ZAK or ZEK).

All translated key types (ZPK, ZAK & ZEK) MUST be the same length.

The plaintext keys will be adjusted for odd parity on each byte before they are encrypted under the LMK. Each of the three zone keys will be received encrypted under a different variant of the KEKr / ZMK (see AS2805 Appendix D – Key Encrypting Key Variants for definition of these variants).

If no key schemes are specified the KEKr/ZMK will be treated as ZMK; e.g. for a ZPK, the single-length version of variant H is used, regardless of the length of the ZPK. Likewise, variant A is used for the ZAK and variant E for the ZEK, regardless of length.

If the Key type flag is used, the key scheme must also be used.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'OK'
KEKr / Zone Master Key	32 H or 1 A + 32 H or 1 A + 48 H	KEKr, encrypted under LMK pair 04-05 variant 3 or ZMK, encrypted under LMK pair 04-05
KCV Processing Flag	1 N	Flag to denote how KCV's are processed: 0 = KCV on input & output 1 = KCV on input only 2 = KCV on output only
ZPK flag	1 N	ZPK flag. If set ('1') ZPK is to be translated. If clear ('0') a clear random value will be returned (appropriate dummy values should be entered in the following 2 fields if flag set to '0')
Zone PIN Key	16 H or 1 A + 16 H or 1 A + 32 H or 1 A + 48 H	ZPK, encrypted under appropriate variant of KEKr / ZMK
ZPK Check Value	6 H	Check value (KCV) for ZPK Only present if KCV processing is set to 0 or 1
ZAK flag	1 N	ZAK flag. If set ('1') ZAK is to be translated. If clear ('0') a clear random value will be returned (appropriate dummy values should be entered in the following 2 fields if flag set to '0')
Zone Authentication Key	16 H or 1 A + 16 H or	ZAK, encrypted under appropriate variant of KEKr / ZMK

Field	Length & Type	Details
ZAK Check Value	1 A + 32 H or 1 A + 48 H	
ZEK flag	6 H	Check value (KCV) for ZAK Only present if KCV processing is set to 0 or 1
	1 N	ZEK flag. If set ('1') ZEK is to be translated. If clear ('0') a clear random value will be returned (appropriate dummy values should be entered in the following 2 fields if flag set to '0')
Zone Encryption Key	16 H or 1 A + 16 H or 1 A + 32 H or 1 A + 48 H	ZEK, encrypted under appropriate variant of KEKr / ZMK (A dummy value should be entered if ZEK flag set to '0')
ZEK Check Value	6 H	Check value (KCV) for ZEK Only present if KCV processing is set to 0 or 1
Delimiter	1 A	Optional: If present the following three fields must be present. Value ';'
Key Scheme ZMK	1 A	Optional. Key Scheme for encrypting keys under ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Delimiter	1 A	Optional: If present the following field must be present. Value ';'
Flag	1 N	Optional flag to indicate if KEKs or ZMK is used. 1 = KEKr; 2 = ZMK ONLY AVAILABLE IF PRECEDING KEY SCHEME IS USED
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'OL'
Error Code	2 N	'00': No errors '01': ZPK KCV validation failure '02': ZAK KCV validation failure '03': ZEK KCV validation failure '10': ZMK parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '26': Invalid Key Scheme '27': Incompatible key length '28': Invalid key type
KCV Processing Flag	1 N	Flag to denote how KCV's are processed: 0 = KCV on input & output 1 = KCV on input only 2 = KCV on output only
Zone PIN Key	16 H or 1 A + 32 H or 1 A + 48 H	ZPK, encrypted under LMK pair 06-07 or a random value if the ZPK flag was clear ('0')
ZPK Check Value	6 H	Check value (KCV) for ZPK Only present if KCV processing is set to 0 or 2
Zone Authentication Key	16 H or 1 A + 32 H or 1 A + 48 H	ZAK, encrypted under LMK pair 26-27 variant 2 or a random value if the ZAK flag was clear ('0')
ZAK Check Value	6 H	Check value (KCV) for ZAK Only present if KCV processing is set to 0 or 2
Zone Encryption Key	16 H or 1 A + 32 H or 1 A + 48 H	ZEK, encrypted under LMK pair 30-31 variant 2 or a random value if the ZEK flag was clear ('0')
ZEK Check Value	6 H	Check value (KCV) for ZEK Only present if KCV processing is set to 0 or 2
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Initial Terminal Master Keys (AS2805 – 2001)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate two random initial Terminal Master Keys (TMK1 and TMK2) and encrypt them under an Acquirer Initialization Key (KIA) and the appropriate LMK pair.

Notes: The plaintext keys will be adjusted for odd parity on each byte before they are encrypted under the LMK. A check value for each key is generated (see *AS2805 Appendix C – Key Check Value*).

If the TMK's are required to be output under KIA without any variants applied, for backward compatibility, then Key Scheme X is used. This must be enabled under the 'CS' command before usage.

PPASN use is only permitted when key scheme option is used.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'C0'
KIA	1 A + 32 H or 1 A + 48 H	Acquirer Initialization Key (KIA) encrypted under LMK pair 14-15 variant 6
Delimiter	1 A	Optional: If present the following three fields must be present. Value ';'
Key Scheme KIA	1 A	Optional. Key Scheme for encrypting keys under KIA
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Delimiter	1 A	Optional: If present the following field must be present. Value ';' Only available if preceding key scheme fields are present,
PPASN Flag	1 N	Optional, value 1. if present PPASN will be present in response message
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'C1'
Error Code	2 N	'00': No errors '10': KIA parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '26': Invalid Key Scheme '27': Incompatible key length '28': Invalid key type
Terminal Master Key 1	1 A + 32 H or 1 A + 48 H	TMK1, encrypted under Variant 1 of LMK pair 14-15
Terminal Master Key 1	1 A + 32 H or 1 A + 48 H	TMK1, encrypted under KIA
TMK1 Check Value	6 H	Check value (KCV) for TMK1
Terminal Master Key 2	1 A + 32 H or 1 A + 48 H	TMK2, encrypted under Variant 2 of LMK pair 14-15
Terminal Master Key 2	1 A + 32 H or 1 A + 48 H	TMK2, encrypted under KIA
TMK2 Check Value	6 H	Check value (KCV) for TMK2
PPASN (LMK)	16 H	PPASN, encrypted under Variant 8 of LMK pair 14-15
PPASN (KIA)	16 H	PPASN, encrypted under the KIA. Variant 88 applied when 1 A + 32 H key used in input.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Update Terminal Master Key 1

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate a new Terminal Master Key (TMK1) and encrypt it under Variant 1 of LMK pair 14-15.

Notes: The plaintext key will be adjusted for odd parity on each byte before it is encrypted under the LMK. A check value for the key is generated (see *AS2805 Appendix C – Key Check Value*). The method of updating the Terminal Master Key is defined in *AS2805 Appendix I – Terminal Master Key Update*.
The PIN Pad Acquirer Security Number (PPASN) is not checked for parity.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'OU'
Terminal Master Key 1	32 H or 1 A + 32 H	Old TMK1, encrypted under Variant 1 of LMK pair 14-15
PPASN	16 H	PPASN, encrypted under Variant 8 of LMK pair 14-15
Delimiter	1 A	Optional: If present the following field must be present. Value ';'
Key update process	1 N	Optional: If present '0': AS2805 – 1988 method '1': AS2805 – 2001 method
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'OV'
Error Code	2 N	'00': No errors '10': Old TMK1 parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '26': Invalid Key Scheme '27': Incompatible key length '28': Invalid key type
Terminal Master Key 1	32 H or 1 A + 32 H	New TMK1, encrypted under Variant 1 of LMK pair 14-15
TMK1 Check Value	6 H	Check value (KCV) for New TMK1
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Update Terminal Master Keys

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate two new Terminal Master Keys (TMK1 and TMK2) and encrypt them under the appropriate LMK pairs.

Notes: The plaintext keys will be adjusted for odd parity on each byte before they are encrypted under the LMK. A check value for each key is generated (see *AS2805 Appendix C – Key Check Value*). The method of updating the Terminal Master Keys is defined in *AS2805 Appendix I – Terminal Master Key Update*.
The PIN Pad Acquirer Security Number (PPASN) is not checked for parity.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'OW'
Terminal Master Key 2	32 H or 1 A + 32 H	Old TMK2, encrypted under Variant 2 of LMK pair 14-15
PPASN	16 H	PPASN, encrypted under Variant 8 of LMK pair 14-15
Delimiter	1 A	Optional: If present the following field must be present. Value ';'
Key update process	1 N	Optional: If present 0 = AS2805 – 1988 method 1 = AS2805 – 2001 method
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'OX'
Error Code	2 N	'00': No errors '10': Old TMK2 parity error '12': No keys loaded in user storage~ '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '26': Invalid Key Scheme '27': Incompatible key length '28': Invalid key type
Terminal Master Key 1	32 H or 1 A + 32 H	New TMK1, encrypted under Variant 1 of LMK pair 14-15
TMK1 Check Value	6 H	Check value (KCV) for New TMK1
Terminal Master Key 2	32 H or 1 A + 32 H	New TMK2, encrypted under Variant 2 of LMK pair 14-15
TMK2 Check Value	6 H	Check value (KCV) for New TMK2
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a Set of Terminal Keys

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate a Terminal PIN Key (TPK), Terminal Authentication Key Receive (TAKr), Terminal Authentication Key Send (TAKs), Terminal Encryption Key Receive (TEKr) and Terminal Encryption Key Send (TEKs) and return each key encrypted under a variant of a Terminal Master Key (TMK) or KMA and the appropriate LMK pair.

Notes:

- A flag will indicate whether TMK1, TMK2 or KMA will be used.
- Each of the terminal keys will be adjusted for odd parity on each byte.
- A check value for each key will be generated (as defined in *AS2805 Appendix C – Key Check Value*).
- The definition of each of the TMK and KMA variants is given in *AS2805 Appendix D – Key Encrypting Key Variants*.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'PI'
Flag	1 N	Flag to indicate which TMK is used: '0': KMA is to be used (Variant H) '1': TMK1 is to be used (Variant H) '2': TMK2 is to be used (Variant H) '3': KMA is to be used (Variant Hb) '4': TMK1 is to be used (Variant Hb) '5': TMK2 is to be used (Variant Hb)
Terminal Master Key	32 H or 1 A + 32 H or 1 A + 48 H	TMK or KMA, encrypted under the appropriate variant* of LMK pair 14-15 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N". If the setting has the value "Y" then for Flag=1 or Flag=2 the encryption is as above, but for Flag=0 the key is encrypted under LMK pair 36-37 variant 8. * Variant 0 if flag = 0; Variant 1 if Flag = 1; Variant 2 if Flag = 2
Delimiter	1 A	Optional: If present the following three fields must be present. Value ';'
Key Scheme TMK	1 A	Optional. Key Scheme for encrypting keys under TMK or KMA
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'PJ'
Error Code	2 N	'00': No errors '10': TMK parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '26': Invalid Key Scheme '27': Incompatible key length '28': Invalid key type
If Key Delimiter Not used		
PIN Key (LMK)	16 H	TPK, encrypted under: LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N". LMK pair 36-37 variant 7 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y".
PIN Key (TMK)	16 H	TPK, encrypted under appropriate variant of TMK or KMA
TPK Check Value	6 H	Check value (KCV) for TPK
Authentication Key(LMK)	16 H	TAK, encrypted under LMK pair 16-17
Authentication Key (TMK)	16 H	TAK, encrypted under appropriate variant of TMK or KMA
TAK Check Value	6 H	Check value (KCV) for TAK
Encryption Key (LMK)	16 H	TEK, encrypted under LMK pair 32-33
Encryption Key (TMK)	16 H	TEK, encrypted under appropriate variant of TMK or KMA
TEK Check Value	6 H	Check value (KCV) for TEK
If Key Delimiter used		
PIN Key (LMK)	16 H or 1 A + 32 H or 1 A + 48 H	TPK, encrypted under: LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N". LMK pair 36-37 variant 7 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y".
PIN Key (TMK)	16 H or 1 A + 32 H or 1 A + 48 H	TPK, encrypted under appropriate variant of TMK or KMA
TPK Check Value	6 H	Check value (KCV) for TPK
Authentication Key(LMK) Send	16 H or 1 A + 32 H or 1 A + 48 H	TAKs, encrypted under LMK pair 16-17 Variant 1
Authentication Key(LMK) Receive	16 H or 1 A + 32 H or 1 A + 48 H	TAKr, encrypted under LMK pair 16-17 Variant 2
Authentication Key (TMK) Send	16 H or 1 A + 32 H or 1 A + 48 H	TAKs, encrypted under appropriate variant of TMK or KMA
Authentication Key (TMK) Receive	16 H or 1 A + 32 H or 1 A + 48 H	TAKr, encrypted under appropriate variant of TMK or KMA
TAKs Check Value	6 H	Check value (KCV) for TAKs
TAKr Check Value	6 H	Check value (KCV) for TAKr
Encryption Key (LMK) Send	16 H or 1 A + 32 H	TEKs, encrypted under LMK pair 32-33 Variant 1

payShield 10K Core Host Commands

Field	Length & Type	Details
Encryption Key (LMK) Receive	or 1 A + 48 H 16 H or 1 A + 32 H or 1 A + 48 H	TEKr, encrypted under LMK pair 32-33 Variant 2
Encryption Key (TMK) Send	16 H or 1 A + 32 H or 1 A + 48 H	TEKs, encrypted under appropriate variant of TMK or KMA
Encryption Key (TMK) Receive	16 H or 1 A + 32 H or 1 A + 48 H	TEKr, encrypted under appropriate variant of TMK or KMA
TEKs Check Value	6 H	Check value (KCV) for TEKs
TEKr Check Value	6 H	Check value (KCV) for TEKr
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate an Acquirer Master Key Encrypting Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate an Acquirer Master Key Encrypting Key (KIA) and return the result encrypted under LMK pair 14-15.

Notes: The KIA is generated from a Cross Acquirer Key Encrypting Key (KCA) and an Acquiring Institution Identification Code (AIIC) using the one-way function defined in *AS2805 Appendix A – One-Way Functions*.
The key scheme flags are ignored in processing.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'C8'
KCA	16 H or 1 A + 32 H or 1 A + 48 H	KCA, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
Flag	1 N	Flag to denote format of AIIC following: '1': 11 N '2': 16 H '3': 32 H
AIIC	11 N or 16 H or 32H	Acquiring Institution Identification Code
Delimiter	1 A	Optional: If present the following three fields must be present. Value ';'
Key Scheme ZMK	1 A	Optional. Key Scheme for encrypting keys under ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'C9'
Error Code	2 N	'00': No errors '10': KCA parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '26': Invalid Key Scheme '27': Incompatible key length '28': Invalid key type
KIA	16 H or 1 A + 32 H	KIA, encrypted under LMK pair 14-15 variant 6
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate an Acquirer Master Key Encrypting Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To translate an Acquirer Master Key Encrypting Key (TMK 1) to encryption under LMK pair 14-15 variant 1.

Notes: The TMK 1 is received encrypted under a Privacy Key (KP) which in turn is received encrypted under a Communications Key (KC). The KC will be received encrypted under LMK pair 04-05.
The key scheme flags are ignored in processing.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'D6'
KC	16 H or 1 A + 32 H or 1 A + 48 H	KC, encrypted under LMK pair 04-05
KP	16 H or 1 A + 32 H or 1 A + 48 H	KP, encrypted under KC
TMK 1	16 H or 1 A + 32 H or 1 A + 48 H	TMK 1, encrypted under KP
Delimiter	1 A	Optional: If present the following three fields must be present. Value ':'
Key Scheme ZMK	1 A	Optional. Key Scheme for encrypting keys under ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'D7'
Error Code	2 N	'00': No errors '10': KC parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '26': Invalid Key Scheme '27': Incompatible key length '28': Invalid key type
TMK 1	16 H or 1 A + 32 H or 1 A + 48 H	TMK 1, encrypted under LMK pair 14-15 variant 1
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

KEKGEN – 6.3

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate a KEK send key and KEK receive key, return the keys enciphered under a KTK (ZMK) with appropriate variants and under the LMK.

Notes: If no key scheme flags are supplied, the HSM will use the single length KTK (ZMK) variant on the output KEKs & KEKr. If key scheme flags are supplied the HSM uses the appropriate variant of ZMK, depending on length for the output KEKs & KEKr.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'F6'
ZMK	16 H or 32 H or 1 A + 32 H or 1 A + 48 H	The ZMK encrypted under LMK pair 4-5
Delimiter	1 A	Optional: If present the following three fields must be present. Value ';'
Key Scheme ZMK	1 A	Optional. Key Scheme for encrypting keys under ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'F7'
Error Code	2 N	'00': No errors. '10': ZMK parity error. '12': No keys or table loaded in user storage. '13': LMK error; report to supervisor. '15': Error in input data. '21': Invalid user storage index. '26': Invalid Key Scheme '27': Incompatible key length '28': Invalid key type
eZMK(KEKs)	16 H or 1 A + 32 H	The KEKs encrypted under supplied ZMK with variant 7
eZMK(KEKr)	16 H or 1 A + 32 H	The KEKr encrypted under supplied ZMK with variant 8
eLMK(KEKs)	16 H or 1 A + 32 H	The KEKs encrypted under LMK 04-05 variant 4
eLMK(KEKr)	16 H or 1 A + 32 H	The KEKr encrypted under LMK 04-05 variant 3
KCV(KEKs)	6 H	Only present if KCV type = 1 in input message
KCV(KEKr)	6 H	Only present if KCV type = 1 in input message
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

KEKREC – 6.3

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To receive a Interchange partner's KEK send key and KEK receive key encrypted under a KTK (ZMK) and return the keys enciphered under the LMK.

Notes: The partner's KEKs becomes the host KEKr, and conversely the partner's received KEKr becomes the host KEKs

If no key scheme flags are supplied, the HSM will use the single length KTK (ZMK) variant on the input KEKs & KEKr. If key scheme flags are supplied the HSM uses the appropriate variant of ZMK, depending on length for the input KEKs & KEKr

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'F8'
ZMK	16 H or 32 H or 1 A + 32 H or 1 A + 48 H	The ZMK encrypted under LMK pair 4-5
eZMK(KEKs) [Partner]	16 H or 1 A + 32 H	The KEKs encrypted under supplied ZMK with variant 7
eZMK(KEKr) [Partner]	16 H or 1 A + 32 H	The KEKr encrypted under supplied ZMK with variant 8
Delimiter	1 A	Optional: If present the following three fields must be present. Value ';'
Key Scheme ZMK	1 A	Optional. Key Scheme for encrypting keys under ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'F9'
Error Code	2 N	'00': No errors. '10': ZMK parity error. '12': No keys or table loaded in user storage. '13': LMK error; report to supervisor. '15': Error in input data. '21': Invalid user storage index. '26': Invalid Key Scheme '27': Incompatible key length '28': Invalid key type
eLMK(KEKs) [Host]	16 H or 1 A + 32 H	The KEKs encrypted under LMK 04-05 variant 4
eLMK(KEKr) [Host]	16 H or 1 A + 32 H	The KEKr encrypted under LMK 04-05 variant 3
KCV(KEKs)	6 H	Only present if KCV type = 1 in input message
KCV(KEKr)	6 H	Only present if KCV type = 1 in input message
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a KCA and KMACH

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate a Sponsor Cross Acquirer Key (KCA) and Sponsor MAC key. Return the keys under appropriate LMK key pairs, and PIN Pad Initial Transport key (KI).

Notes: Valid key schemes for KI are H, K & L, and valid key schemes for LMK are U & T. If these values are not entered, error code 04 will be returned.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'E8'.
Flag	1 N	Flag to indicate which LMK pair input is stored under 0 = LMK 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y". 1 = LMK 14-15 variant 6
KI	16 H or 1 A + 32 H or 1 A + 48 H	Initial Transport Key, encrypted under: If Flag=0: LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y". If Flag=1: LMK 14-15 variant 6
Delimiter	1 A	Optional: If present the following three fields must be present. Value ';'
Key Scheme KI	1 A	Optional. Key Scheme for encrypting keys under KI. Valid values: 'H', 'K' and 'L'.
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK. Valid values: 'U' and 'T'.
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'E9'
Error Code	2 N	'00': No errors '04': Invalid key scheme '10': KI parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index
KCA (LMK)	16 H or 1 A + 32 H or 1 A + 48 H	Sponsor Cross Acquirer Key encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
KCA (KI)	16 H or 1 A + 32 H or 1 A + 48 H	Sponsor Cross Acquirer Key encrypted under KI with appropriate variant
KMACH (LMK)	16 H or 1 A + 32 H or 1 A + 48 H	Sponsor MAC key encrypted under LMK pair 16-17 variant 1
KMACH (KI)	16 H or 1 A + 32 H or 1 A + 48 H	Sponsor MAC key encrypted under KI with appropriate variant
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a KEKs for use in Node to Node interchange using RSA

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate a new Random Key Encrypting Key (Send) KEKs for use with interchange partners, encrypt the key under the supplied Public Key, and encrypt it under LMK pair 04-05 variant 4.

Notes:

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'H4'
Public Key Encoding	2 N	Encoding rules for the supplied Public Key Rcv
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37
Public Key Rcv	n B	PKr Public Key of Interchange partner
Authentication Data	n A	Optional. Additional data to be included in the MAC calculation (must not include ;).
Delimiter	1 A	Value ','
Secret key flag	2 N	The number is the index of the stored secret key, except 99 which means use the key supplied in the command
Secret key length	4 N	Length (in bytes) of the next field (present only if the secret key flag is 99).
Secret Key	n B	SKs Secret Key encrypted under LMK pair 34-35. (Present only if the secret key flag is 99.)
Delimiter	1 A	Optional: If present the following three fields must be present. Value ','
Key Scheme ZMK	1 A	Optional. Key Scheme for encrypting keys under ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'H5'
Error Code	2 N	<p>'00': No Errors '01': PK MAC failure '03': Invalid PK encoding value (only '01' defined). '04': Invalid SK flag '05': SK modulus length < 512. '06': Corrupt PK '07': Invalid SK type '08': PK modulus length < 512. '13': LMK parity error '15': Input data error '47': DSP failure '49': Corrupt SK '78': SK length error </p>
KEKs	1 A + 32 H	KEKs, encrypted under LMK pair 04-05 variant 4
ePKr (KEKs)	n B	Key Block encrypted by Public Key of recipient
sSKs(H(KEKs))	n B	Signed SHA-1 hash of Key Block
KVC	6 H	Key Check Value of KEKs
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Receive a KEKr for use in Node to Node interchange using RSA

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To decrypt a Key Encrypting Key from under a RSA key pair and to encrypt it under LMK pair 04-05 variant 3.

Notes:

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'H6'
Public Key Encoding	2 N	Encoding rules for the supplied Public Key Send
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37
Public Key Send	n B	PKs Public Key of Interchange partner ASN.1 encoded
Authentication Data	n A	Optional. Additional data to be included in the MAC calculation (must not include ;).
Delimiter	1 A	Value ','
Secret key flag	2 N	The number is the index of the stored secret key, except 99 which means use the key supplied in the command
Secret key length	4 N	Length (in bytes) of the next field (present only if the secret key flag is 99).
Secret Key	n B	SKs Secret Key encrypted under LMK pair 34-35. (present only if the secret key flag is 99).
Delimiter	1 A	Value ';' (present only if the secret key flag is 99)
Data Length	4 N	Length (in bytes) of the following data block
sSKs(H(KEKr))	n B	Signed SHA-1 hash of Key Block
Delimiter	1 A	Value ','
Data Length	4 N	Length (in bytes) of the following data block
ePKr (KEKr)	n B	Key Block encrypted by Public Key
Delimiter	1 A	Value ','
KVC	6 H	Key Check Value of KEKr
Delimiter	1 A	Optional: If present the following three fields must be present. Value ','
Key Scheme ZMK	1 A	Optional. Key Scheme for encrypting keys under ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'H7'
Error Code	2 N	<p>'00': No errors '01': PK MAC failure '02': Signature failure '03': Invalid PK encoding value (only '01' defined). '04': Invalid SK flag '05': SK modulus length < 512. '06': Corrupt PK '07': Invalid SK type '08': PK modulus length < 512. '09': KCV failure '13': LMK parity error '15': Input data error '47': DSP failure '49': Corrupt SK '76': Signature/KEK length <> modulus length '77': Decrypted Signature/KEK blocks corrupt '78': SK length error </p>
KEKr	1 A + 32 H	KEKr encrypted under LMK 04-05 variant 3
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Decrypt a PIN Pad Public Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To decrypt a PIN Pad Public Key (PPPK) from encryption under a Manufacturer Secret Key (MSK), using the Manufacturer Public Key (MPK).

Notes: All RSA data blocks will conform to the format defined in "APCA2000 SPECIFICATION FOR A SECURITY CONTROL MODULE FUNCTION SET", version 3.3, §5.4.4.1 DEA 2 Text Block - DFormat 1 (see AS2805 Appendix U1 – DEA 2 Text Block - DFormat 1).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'H0'
Public Key Encoding	2 N	Encoding rules for the supplied public key (must allow the public key to be inferred)
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37
Manufacturer Public Key	n B	MPK Public Key of Manufacturer ASN.1 encoded
Authentication Data	n A	Optional. Additional data to be included in the MAC calculation (must not include ';').
Delimiter	1 A	Value ','
Data Length	4 N	Length (in bytes) of the following data block
sMSK(PPPK)	n B	PIN PAD Public Key signed by Manufacturer Secret Key
Delimiter	1 A	Optional; if present, the following two fields must be present. Value ':'
Exponent Length	4 N	Optional; indicates the length (in bits) of the PPPK exponent.
PPPK Exponent	n B	Optional; PPPK exponent. If supplied, this field must be an odd value.
Delimiter	1 A	Optional, if present following field must be present Value ','
PPPK Authentication Data	n A	Optional; additional data to be included in the MAC calculation (must not include ';').
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

payShield 10K Core Host Commands

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'H1'
Error Code	2 N	'00': No errors '01': MPK MAC failure '02': Signature failure '03': Invalid PK encoding value '06': Corrupt PK '13': LMK parity error '15': Input data error '47': DSP failure '76': Data Length not equal to MPK modulus length '77': RSA block checksum failure '80': sMSK(PPPK) length error
PPPK	n B	PIN PAD Public Key ASN.1 encoded
MAC	4 B	MAC on the PIN PAD Public Key and authentication data, calculated using LMK pair 36-37
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Encrypt a Cross Acquirer Key Encrypting Key under an Initial Transport Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To decrypt an Initial Transport Key (KTI) from encryption under a Host RSA Public Key (KHPK) and a PIN Pad Secret Key (PPSK) and to encrypt a newly generated Cross Acquirer Key Encrypting Key (KCA) under a variant of the KTI and also under the appropriate LMK pair.

Notes: IT IS THE RESPONSIBILITY OF THE PROGRAMMER TO ENSURE THE KEY SIZES ARE CONSISTENT WITH THE RELEVANT AS2805 STANDARD.

e.g. AS2805.6.5.3 currently recommends these to be 1024 bits for the Manufacturer PK/SK. 960 bits for the PIN Pad PK/SK and 896 bits for the Acquirer (HSM) PK/SK

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'H8'
Public Key Encoding	2 N	Encoding rules for the supplied PIN PAD Public Key
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37
PIN PAD Public Key	n B	PPPK Public Key of PIN PAD ASN.1 encoded
Authentication Data	n A	Optional. Additional data to be included in the MAC calculation (must not include ;)
Delimiter	1 A	Value ';'
Secret key flag (SKsp)	2 N	The number is the index of the stored secret key, except 99 which means use the key supplied in the command
Secret key length	4 N	Length (in bytes) of the next field (present only if the secret key flag is 99).
Secret Key	n B	SK Secret Key (SKsp) encrypted under LMK pair 34-35. (Present only if the secret key flag is 99.)
Delimiter	1 A	Value ';' Only present if the secret key flag is 99.
Data Block Format Code	1 A	Optional. Required when supplying the Data Block Format Code (in the following field). Note: If using Data Block Format Code = '04', this field is mandatory. Value '#'. If present, the following field must be present.
Data Block Format Code	2 N	The format code of the following Data Block: '01': Format 01 '02': Format 02 '03': Format 03 '04': Format 04 See <i>AS2805 Appendix V – Plaintext Data Block Formats</i> for details. Must be present if the above delimiter is present.
Data Length	4 N	Length (in bytes) of the following data block
Data Block	n B	Data block encrypted by the Host Public Key, and the PIN PAD Secret Key
Delimiter	1 A	Optional, If present following field must be present Value ';'
Random Number	16 H	Random number
Delimiter	1 A	Optional: If present the following three fields must be present. Value
Key Scheme KTI	1 A	Optional. Key Scheme for encrypting keys under KTI. Valid values include 'K'.
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK.
Key Check Value type	1 A	Optional. Key check value calculation method.

Field	Length & Type	Details
		1 = KCV 6H
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'H9'
Error Code	2 N	'00': No errors '01': PPPK MAC failure '03': Invalid Secret Key index '04': Public Key does not match encoding rules '05': Data block format error '10': KTI parity error; advice only '13': LMK parity error '15': Error in input data '47': DSP error; report to supervisor '49': SKsp corrupt; report to supervisor '50': Random number error '76': Key length/data block length mismatch '77': Clear data block does not conform to encoding rules '78': SKsp length error '80': PPPK length error
KCA (KTI)	1 A + 32 H	KCA, encrypted under Variant G of KTI
KCA (LMK)	1 A + 32 H	KCA, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
DTS	10 N	Date/Time Stamp
PPSN	16 N	PIN Pad Serial Number
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Encrypt a Terminal Key under the LMK

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To decrypt a Terminal Key (KT) from encryption under a Host RSA Public Key (KHPK) and a PIN Pad Secret Key (PPSK) and to encrypt it under the appropriate LMK pair.

Notes:

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'I0'
Public Key Encoding	2 N	Encoding rules for the supplied PIN PAD Public Key
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37
PIN PAD Public Key	n B	PPPK Public Key of PIN PAD ASN.1 encoded
Authentication Data	n A	Optional. Additional data to be included in the MAC calculation (must not include ;)
Delimiter	1 A	Value ';'
Secret key flag (SKsp)	2 N	The number is the index of the stored secret key, except 99 which means use the key supplied in the command
Secret key length	4 N	Length (in bytes) of the next field (present only if the secret key flag is 99).
Secret Key	n B	SK Secret Key (SKsp) encrypted under LMK pair 34-35. (Present only if the secret key flag is 99.)
Delimiter	1 A	Value ';' Only present if the secret key flag is 99
Data Block Format Code	1 A	Optional. Required when supplying the Data Block Format Code (in the following field). Note: If using Data Block Format Code = '04', this field is mandatory. Value '#'. If present, the following field must be present.
Data Block Format Code	2 N	The format code of the following Data Block: '01': Format 01 '02': Format 02 '03': Format 03 '04': Format 04 See <i>AS2805 Appendix V – Plaintext Data Block Formats</i> for details. Must be present if the above delimiter is present.
Data Length	4 N	Length (in bytes) of the following data block
Data Block	n B	Data block, encrypted with the KHPK and the PPSK, right justified and padded with 0 if necessary
Delimiter	1 A	Value ';'
Random Number	16 H	Random Number
Delimiter	1 A	Optional, if present following field must be present Value ;'
Key Scheme ZMK	1 A	Optional. Key Scheme for encrypting keys under ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'I1'
Error Code	2 N	<p>'00': No errors '01': PPPK MAC failure '03': Invalid Secret Key index '04': Public Key does not match encoding rules '05': Data block format error '10': KTI parity error; advice only '13': LMK parity error '15': Error in input data '47': DSP error; report to supervisor '49': SKsp corrupt; report to supervisor '50': Random number error '76': Key length/data block length mismatch '77': Clear data block does not conform to encoding rules '78': SKsp length error '80': PPPK length error </p>
KT	1 A + 32 H	KT, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
DTS	10 N	Date/Time Stamp
PPID	16 N	PIN Pad Identification Number
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

3.6 Asymmetric Key Management Commands

The payShield 10K provides the following host commands to support RSA & ECC operations:

Function	Command	Page
<i>Generate an RSA Public/Private Key Pair</i>	EI (EJ)	188
<i>Generate an ECC Public/Private Key Pair</i>	FY (FZ)	193
<i>Load a Private Key</i>	EK (EL)	195
<i>Translate a Private Key</i>	EM (EN)	196
<i>Import a Public Key</i>	EO (EP)	197
<i>Validate a Public Key</i>	EQ (ER)	201
<i>Validate a Certificate and Import the Public Key</i>	ES (ET)	202
<i>Translate a Public Key</i>	EU (EV)	205
<i>Import Key or data under an RSA Public Key</i>	GI (GJ)	207
<i>Export Key under an RSA Public Key</i>	GK (GL)	213
<i>Generate a Certificate Request</i>	QE (QF)	219
<i>Key Derivation using Elliptic Curve Key Agreement</i>	IG (IH)	222
<i>TR-34 Key Export</i>	B8 (B9)	244

Generate an RSA Public/Private Key Pair

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Variant LMK	Authorization: Required* Activity: generate.rsa.host
Key Block LMK	Authorization: Required* Activity: generate.{key}.host

Function: Generate an RSA public/private key pair.

Notes: Depending on key size, the function may take some time to execute.

If a Public Exponent is supplied in the command message, it must be an odd value (i.e. the least-significant bit must be 1). If an even Public Exponent is supplied, an error code is returned.

The type of RSA key pair to be generated is indicated by the Key Type Indicator. All requests except where Key Type Indicator = '3' (ICC key pairs) require that the HSM is in the authorized state (or the appropriate activity is authorized).

When using a Variant LMK, the following activity applies: **generate.rsa.host**.

When using a Key Block LMK, the following activity applies: **generate.{key}.host**, where 'key' indicates the Key Usage field of the RSA private key to be generated.

Example: In order to generate an RSA key pair with Key Type Indicator = '2', the activity **generate.03.host** must be authorized.

Example: In order to generate an RSA key pair with Key Type Indicator = '4', the activity **generate.06.host** must be authorized.

RSA keys larger than 2048 bits require an AES Key Block LMK to be used.

WARNING: Public keys generated by this command should not be imported using the same LMK.

For information about support for the RSA algorithm, see the *payShield 10K Host Programmer's manual*.

For Key Block LMKs, the RSA Private Key is created in a key block format, with the following attributes:

Field	Value
Key Usage	'03' (for Key Type Indicator = '0', '1', '2', & '4') '04' (for Key Type Indicator = '3') '05' (for Key Type Indicator = '5') '06' (for Key Type Indicator = '4')
Algorithm	'R'
Mode Of Use	'S' (for Key Type Indicator = '0' & '3') 'D' (for Key Type Indicator = '1' & '5') 'N' (for Key Type Indicator = '2' & '4')
Exportability	'N' (unless Exportability = 'S' is specified)
Key Length	Defined by 'Key Length' parameter

The generated RSA public key is returned in the same format as per a Variant LMK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'EI'.
Key Type Indicator	1 N	Defines the intended usage of the key pair: '0': Signature only '1': Key management only '2': Both signature and key management '3': Integrated Chip Card (ICC) Key '4': Data encryption/decryption (e.g. TLS/SSL premaster secret) '5': PIN encryption/decryption
Key Length	4 N	The length of the RSA modulus, in bits: '0320' ... '2048': if not using an AES Key Block LMK '0320' ... '4096': when used with an AES Key Block LMK
Public Key Encoding	2 N	Encoding rules for the Public Key: '01': DER encoded ASN.1 RSA Public Key (INTEGER uses unsigned representation). '02': DER encoded ASN.1 RSA Public Key (INTEGER uses 2's complement representation).
Public Exponent Length	4 N	Optional. Must be present if a public exponent is supplied. Indicates the length (in bits) of the public exponent.
Public Exponent	n B	Optional. Must be an odd value. If not supplied, a default exponent of 65537 is assumed.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
The following section applies when generating a Key Block RSA private key.		
Delimiter	1 A	Value '#'. Optional; must be present if using a Key Block LMK; if present, the following fields must be present.
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
Delimiter	1 A	Value '&'. Optional; if present, the following field must also be present.
Exportability	1 A	Only present if the preceding delimiter is present. The Exportability field (byte 11) of the exported private key; only permitted values are 'N' or 'S'.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details						
RESPONSE MESSAGE								
Message Header	m A	Returned to the Host unchanged.						
Response Code	2 A	Value 'EJ'.						
Error Code	2 A	'00': No error '03': Invalid public key encoding type '04': Key Length error '05': Invalid key type '06': Public exponent length error '08': Supplied public exponent is even '47': Algorithm not licensed '48': Stronger LMK required to protect this size RSA key '68': Command disabled or a standard error code.						
Public key	n B	RSA Public key, encoded appropriately.						
RSA Private Key length	4 N	For a Variant LMK: Length (in bytes) of the next field.						
	or 4 H	For a Key Block LMK: This field is reserved, and set to 'FFFF'.						
RSA Private Key	n B	The RSA Private Key, encrypted under the LMK. For a Variant LMK, the private key is encrypted under LMK pair 34-35.						
	or 'S' + n B	For a Key Block LMK, the private key is encrypted under the LMK: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'03', '04', '05', '06'</td> <td>'R'</td> <td>'S', 'D', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'03', '04', '05', '06'	'R'	'S', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'03', '04', '05', '06'	'R'	'S', 'D', 'N'						
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.						
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.						

Generate an ECC Public/Private Key Pair

Variant LMK <input checked="" type="checkbox"/>	AES Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Required	Activity: generate.ecc.host

Function: Generate an ECC public/private key pair using the Elliptic Curve algorithm.

Notes: This command is only available for use with an AES Key Block LMK.

The following set of elliptic curves are supported:

- FIPS 186-3 – NIST P-256
- FIPS 186-3 – NIST P-384
- FIPS 186-3 – NIST P-521

The output ECC private key is encoded with the curve identifier in ASN.1 format and encrypted under the LMK.

The public key is output as a SubjectPublicKeyInfo block in ASN.1 format as defined by ANSI X9.62.

The Key Generation Method field provides support for generating EMV compliant ECC key pairs. Note that when generating ECC keys for EMV, this command may timeout, resulting in error code 'E2' being returned.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FY'.
Command Version	2 N	Value '01'.
Curve Reference	2 H	Prime Curves defined in FIPS 186-3: '00': FIPS 186-3 – NIST P-256 '01': FIPS 186-3 – NIST P-384 '02': FIPS 186-3 – NIST P-521
Delimiter	1 A	Value ' '. Optional; if present, the following field must also be present.
Key Generation Method	1 N	Method for generating the ECC key pair: '0': ISO 159460-1 (this is the default method if the Key Generation Method is not specified) '1': EMV v4.4 B2.2.4 Key Generation
Public Key Encoding	2 N	'03': DER encoded ASN.1 ECC X9.62 format uncompressed key
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by licence; must be present if the above Delimiter is present.
Delimiter	1 A	Value '#'. Always required.
Mode of use	1 A	Mode of Use to be included in the key block header. Permitted values: 'S', 'X', 'N'.
Key Version Number	2 A	Key Version Number field to be included in the key block header. Permitted values: '00' to '99'.
Exportability	1 A	Exportability field to be included in the key block header. Permitted values: 'N', 'E' or 'S'.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below. Permitted values '00' to '08'.

Field	Length & Type	Details
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details						
RESPONSE MESSAGE								
Message Header	m A	Returned to the Host unchanged.						
Response Code	2 A	Value 'FZ'.						
Error Code	2 A	'00': No error 'A1': Function requires AES key block 'D2': Invalid curve reference 'D3': Invalid Key Encoding 'E0': Invalid command version number 'E1': Invalid Key Generation Method 'E2': Timeout (only valid if Key Generation Method = '1') - please retry or a standard error code.						
ECC Public Key Length	4 N	The length (in bytes) of the following field.						
ECC Public Key	n B	The ECC Public key, encoded appropriately.						
ECC Private Key	'S' + n B	The ECC Private Key, encrypted under the LMK: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'03'</td> <td>'E'</td> <td>'S', 'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'03'	'E'	'S', 'X', 'N'
Key Usage	Algorithm	Mode of Use						
'03'	'E'	'S', 'X', 'N'						
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.						
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.						

Load a Private Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Load an RSA or ECC private key (encrypted under the LMK) into the HSM's internal memory.

Notes: It is the responsibility of the Host application to ensure that a previously-loaded private key is not accidentally overwritten by this command.

For information about support for the RSA and ECC algorithms, see the *payShield 10K Host Programmer's manual*.

Field	Length & Type	Details									
COMMAND MESSAGE											
Message Header	m A	Subsequently returned to the Host unchanged.									
Command Code	2 A	Value 'EK'.									
Key index	2 N	'00 ... '20': Index number for the Private Key to be stored (used if multiple storage of keys is required).									
Private Key length	4 N or 4 H	For a Variant LMK: Length (in bytes) of the next field. For a Key Block LMK: This field is ignored; should be set to 'FFFF'.									
Private Key	n B or 'S' + n B	The RSA Private Key to be loaded and stored inside the HSM. For a Variant LMK, the 'Private Key' must be encrypted under LMK pair 34-35. For a Key Block LMK, the 'Private Key' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'03', '04', '05', '06'</td> <td>'R'</td> <td>'S', 'D', 'N'</td> </tr> <tr> <td>'03'</td> <td>'E'</td> <td>'S', 'X', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'03', '04', '05', '06'	'R'	'S', 'D', 'N'	'03'	'E'	'S', 'X', 'N'
Key Usage	Algorithm	Mode of Use									
'03', '04', '05', '06'	'R'	'S', 'D', 'N'									
'03'	'E'	'S', 'X', 'N'									
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.									
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.									
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.									
Message Trailer	n A	Optional. Maximum length 32 characters.									

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'EL'.
Error Code	2 A	'00': No error '03': Invalid key index '04': Insufficient memory for private key storage '47': Algorithm not licensed '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate a Private Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Translate an RSA or ECC private key from encryption under an 'old' LMK to encryption under the 'new' LMK. The 'old' or 'new' LMK must have previously been loaded into Key Change Storage.

Note: For information about support for the RSA and ECC algorithms, see the *payShield 10K Host Programmer's manual*.

When translating an RSA Private Key from encryption under a Variant LMK to a Key Block LMK, the RSA Private Key is re-created in Thales Key Block format with the following attributes:

Field	Value
Key Usage	If Key Type Indicator is '0', '1', '2', a Key Usage value of '03' will be used. If Key Type Indicator is '3', a Key Usage value of '04' will be used. If Key Type Indicator is '4', a Key Usage value of '03' or '06' will be used (depending on the presence of the '\$' delimiter in the command). If Key Type Indicator is '5', a Key Usage value of '05' will be used.
Algorithm	'R'
Mode Of Use	Inferred from the input key's type
Exportability	'N' or 'S'
Key Length	Defined by the input key's length

Field	Length & Type	Details									
COMMAND MESSAGE											
Message Header	m A	Subsequently returned to the Host unchanged.									
Command Code	2 A	Value 'EM'.									
Private key length	4 N	For a Variant LMK: Length (in bytes) of the next field.									
	or 4 H	For a Key Block LMK: This field is ignored, and should be set to 'FFFF'.									
Private key	n B or 'S' + n B	The Private Key to be translated. For a Variant LMK, the 'Private Key' must be encrypted under LMK pair 34-35. For a Key Block LMK, the 'Private Key' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'03', '04', '05', '06'</td> <td>'R'</td> <td>'S', 'D', 'N'</td> </tr> <tr> <td>'03'</td> <td>'E'</td> <td>'S', 'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'03', '04', '05', '06'	'R'	'S', 'D', 'N'	'03'	'E'	'S', 'X', 'N'
Key Usage	Algorithm	Mode of Use									
'03', '04', '05', '06'	'R'	'S', 'D', 'N'									
'03'	'E'	'S', 'X', 'N'									
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.									
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.									

The following section applies when translating from a Variant LMK to Key Block LMK		
Delimiter	1 A	Value '#'. Optional; must be present if translating the Private Key from encrypted under a Variant LMK to a Key Block LMK; if present, the following fields must be present.
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
Delimiter	1 A	Value '\$'. Optional; can only be present if the Key Type Indicator of the key encrypted under the Variant LMK is '4'. Must be present if the following field is present.
Key Usage	2 A	Only present if the preceding delimiter is present. Key Usage to be included in the key block header. Only value permitted is '06'.
Delimiter	1 A	Value '&'. Optional; if present, the following field must also be present.
Exportability	1 A	Only present if the preceding delimiter is present.
End Message Delimiter	1 C	The Exportability field (byte 11) of the translated private key; only permitted values are 'N' or 'S'.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'EN'.
Error Code	2 A	'00': No error '47': Algorithm not licensed '68': Command disabled or a standard error code.
Private key length	4 N	For a Variant LMK: Length (in bytes) of the next field.
	or 4 H	For a Key Block LMK: This field is reserved, and set to 'FFFF'.
Private key	n B	The translated Private Key.
	or 'S' + n B	For a Variant LMK, the 'Private Key' is encrypted under current LMK pair 34-35. For a Key Block LMK, the 'Private Key' is encrypted under the current LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Import a Public Key

Variant LMK	Key Block LMK
Available in package(s): Classic & Premium	
Variant LMK	Authorization: Required Activity: import.rsa.host
Key Block LMK	Authorization: Required Activity: import.02.host

Function: Import an RSA or ECC Public Key by generating a MAC on it. When used with a Key Block LMK, the imported Public Key will be in the form of a Thales Key Block.

Note: The function can be used, for example, to protect a certification authority public key.

WARNING: This command should not be used to import an RSA public key for which the corresponding RSA private key exists encrypted under the LMK.

For information about support for the RSA and ECC algorithms, see the *payShield 10K Host Programmer's manual*.

When importing an RSA Public Key using a Key Block LMK, the RSA Public Key is returned in a key block format with the following attributes:

Field	Value
Key Usage	'02'
Algorithm	'R', 'E'
Mode Of Use	Specified after the '#' delimiter
Exportability	Specified after the '#' delimiter
Key Length	Determined by the input key parameter

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'EO'.
Public Key Encoding	2 N	Encoding rules for Public Key: '01': DER encoded ASN.1 RSA Public Key (INTEGER using unsigned representation). '02': DER encoded ASN.1 RSA Public Key (INTEGER using 2's complement representation). '03': DER encoded ASN.1 ECC X9.62 format uncompressed key
Public Key	n B	Public key, DER encoded in the above specified ASN.1 format.
The following field applies only when using a Variant LMK.		
Authentication data	n B	Optional. Additional data to be included in the MAC calculation (must not include ';' or '~').
Delimiter	1 A	Value '~'. Optional; must be present if the '%' or '#' delimiter is present below. This field is used to terminate the previous one/two variable length fields.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
The following section applies only when using a Key Block LMK.		
Delimiter	1 A	Value '#'. Required when using a Key Block LMK. If present, the following fields must be present.
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in the <i>payShield 10K Host Programmer's manual</i> .
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details												
RESPONSE MESSAGE														
Message Header	m A	Returned to the Host unchanged.												
Response Code	2 A	Value 'EP'.												
Error Code	2 A	'00': No error '03': Invalid public key encoding type '04': Public key does not conform to encoding rules '47': Algorithm not licensed '68': Command disabled 'D4': Invalid ECC public key or a standard error code.												
MAC	4 B	For use with a Variant LMK only: MAC on the Public Key and Authentication Data, calculated using LMK pair 36-37.												
Public Key	n B or 'S' + n B	The imported Public Key. For a Variant LMK, the RSA 'Public Key' is DER encoded in ASN.1 format (sequence of modulus, exponent). For a Key Block LMK, the 'Public Key' is stored (without encryption) in key block format (which includes the MAC). Imported RSA Public Key: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'02'</td> <td>'R'</td> <td>'V', 'E', 'N'</td> </tr> </tbody> </table> Imported ECC Public Key: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'02'</td> <td>'E'</td> <td>'V', 'X', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'02'	'R'	'V', 'E', 'N'	Key Usage	Algorithm	Mode of Use	'02'	'E'	'V', 'X', 'N'
Key Usage	Algorithm	Mode of Use												
'02'	'R'	'V', 'E', 'N'												
Key Usage	Algorithm	Mode of Use												
'02'	'E'	'V', 'X', 'N'												
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.												
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.												

Validate a Public Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Validate an RSA Public Key.

Note: This command does not support the use of ECC Public Keys.

For information about support for the RSA algorithm, see the *payShield 10K Host Programmer's manual*.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'EQ'.						
The following section applies only when using a Variant LMK.								
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.						
Public key	n B	The Public key; DER encoded in ASN.1 format (sequence of modulus, exponent).						
Authentication data	n B	Optional. Additional data included in the MAC calculation (must not include ';' or '~').						
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present. Used to terminate all previous fields.						
The following section applies only when using a Key Block LMK.								
Public Key	'S' + n B	The 'Public Key', in key block format; must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'02'</td> <td>'R'</td> <td>'S', 'B', 'E', 'N', 'V'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'02'	'R'	'S', 'B', 'E', 'N', 'V'
Key Usage	Algorithm	Mode of Use						
'02'	'R'	'S', 'B', 'E', 'N', 'V'						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ER'.
Error Code	2 A	'00': No error '01': MAC verification failure '04': Public key does not conform to encoding rules '47': Algorithm not licensed '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Validate a Certificate and Import the Public Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Validate a certificate and import an RSA Public Key contained within the certificate.

Notes: This command does not support the use of ECC Public/Private Keys.

The command can (optionally) check whether the public key in the certificate corresponds to a private key encrypted under the LMK.

For information about support for the RSA algorithm, see the *payShield 10K Host Programmer's manual*.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'ES'.						
The following section applies only when using a Variant LMK.								
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.						
Public Key	n B	The Public Key used to validate the certificate; DER encoded in ASN.1 format (sequence of modulus, exponent).						
Authentication data	n B	Optional. Additional data included in the MAC calculation (must not include ';' or '~').						
Delimiter	1 A	Value ';'. Used to indicate the end of the authentication data field.						
The following section applies only when using a Key Block LMK.								
Public Key	'S' + n B	<p>The Public Key used to validate the certificate; must be in key block format, and comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'02'</td> <td>'R'</td> <td>'S', 'B', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'02'	'R'	'S', 'B', 'N'
Key Usage	Algorithm	Mode of Use						
'02'	'R'	'S', 'B', 'N'						
Certificate length	4 N	Certificate length (in bytes).						
Hash offset	4 N	Offset to the first byte in the certificate data to be included in the hash calculation.						
Hash length	4 N	Length (in bytes) of the data within the certificate which is included in the hash calculation.						
Signature offset	4 N	Offset to the first byte of the signature contained in the certificate data.						
Signature length	4 N	Length (in bytes) of the signature contained in the certificate data.						
Certificate	n B	Certificate data to be validated.						
Delimiter	1 A	Value ';'. Used to indicate the end of the certificate field.						
Hash identifier	2 N	Identifier of the hash algorithm used to hash the certificate data.						
Signature algorithm	2 N	Identifier of the signature algorithm used to sign the certificate data.						
Pad mode identifier	2 N	Identifier of the pad mode used in certificate signature generation. '01': PKCS#1 v1.5 method (EMSA-PKCS1-v1_5)						
Public key encoding	2 N	Encoding rules for the public key contained in the certificate.						
Public key offset	4 N	Offset to the first byte of the public key field contained in the certificate						
The following section applies only when using a Variant LMK.								
Authentication data	n B	Optional. Additional data to be included in the MAC calculation (must not include ';').						
Delimiter	1 A	Value ';'. Used to indicate the end of the authentication data field.						

Field	Length & Type	Details						
Private Key length	4 N	Optional. Must be present if the Private Key field is present. For a Variant LMK: Length (in bytes) of the next field.						
	or 4 H	For a Key Block LMK: This field is ignored, and should be set to 'FFFF'.						
Private Key	n B	Optional. The Private Key that should correspond to the public key contained within the certificate.						
	or 'S' + n B	For a Variant LMK, the 'Private Key' is encrypted under LMK pair 34-35. For a Key Block LMK, the 'Private Key' must comply with the following:						
<table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'03'</td><td>'R'</td><td>'S', 'D', 'N'</td></tr> </tbody> </table>			Key Usage	Algorithm	Mode of Use	'03'	'R'	'S', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'03'	'R'	'S', 'D', 'N'						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
The following section applies only when using a Key Block LMK.								
Delimiter	1 A	Value '#'. Required when using a Key Block LMK. If present, the following fields must be present.						
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> . Note: The value supplied must be compatible with the Mode Of Use of the Private Key (if supplied).						
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.						
Exportability	1 A	Exportability field, to be included in the key block header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in the <i>payShield 10K Host Programmer's manual</i> .						
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.						
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.								
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.						
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.						
Optional Block Data	n A	Optional block data.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ET'.
Error Code	2 A	'00': No error '01': MAC verification failure '02': Certificate validation failure '03': Invalid public key encoding type '04': Public key does not conform to encoding rules '05': Invalid hash identifier '06': Invalid signature identifier '07': Invalid pad mode identifier '47': Algorithm not licensed '68': Command disabled '74': Invalid digest info syntax (no-hash mode only) '76': Public key length error '77': Clear data block error '78': Private key length error '79': Hash algorithm object identifier error '80': Certificate length error '81': Invalid certificate header or a standard error code.
MAC	4 B	For use with a Variant LMK only. MAC on the public key and authentication data, calculated using LMK pair 36-37.
Public key	n B	The imported Public Key.
	or 'S' + n B	For a Variant LMK, the 'Public Key' is DER encoded in ASN.1 format (sequence of modulus, exponent). For a Key Block LMK, the 'Public Key' is stored (without encryption) in key block format (which includes the MAC).
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate a Public Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Translate an RSA or ECC Public Key from protection under an 'old' LMK to protection under the 'new' LMK. The 'old' or 'new' LMK must have previously been loaded into Key Change Storage.

Note: For information about support for the RSA algorithm, see the *payShield 10K Host Programmer's manual*.

Field	Length & Type	Details									
COMMAND MESSAGE											
Message Header	m A	Subsequently returned to the Host unchanged.									
Command Code	2 A	Value 'EU'.									
The following section applies only when using a Variant LMK.											
MAC	4 B	MAC on the public key and authentication data, calculated using the old LMK pair 36-37.									
Public Key	n B	The Public Key; DER encoded in ASN.1 format (sequence of modulus, exponent).									
Authentication data	n B	Optional. Additional data included in the MAC calculation (must not include ';' or '~').									
Delimiter	1 A	Value '~'. Optional; must be present if either the '%' or '#' delimiter is present.									
The following section applies only when using a Key Block LMK.											
Public Key	'S' + n B	<p>The Public Key; must be in key block format (using the old LMK), and comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'02'</td> <td>'R'</td> <td>'V', 'E', 'N'</td> </tr> <tr> <td>'02'</td> <td>'E'</td> <td>'V', 'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'02'	'R'	'V', 'E', 'N'	'02'	'E'	'V', 'X', 'N'
Key Usage	Algorithm	Mode of Use									
'02'	'R'	'V', 'E', 'N'									
'02'	'E'	'V', 'X', 'N'									
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.									
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.									
The following section applies only when translating from an old Variant LMK to a new Key Block LMK.											
Delimiter	1 A	Value '#'. Required when using a Key Block LMK. If present, the following fields must be present.									
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .									
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.									
Exportability	1 A	Exportability field, to be included in the key block header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in the <i>payShield 10K Host Programmer's manual</i> .									
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.									
For each optional block, the following three fields must be specified.											
Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.											
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.									
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.									
Optional Block Data	n A	Optional block data.									
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.									

Field	Length & Type	Details
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'EV'.
Error Code	2 A	'00': No error '01': MAC verification failure '04': Public key does not conform to encoding rules '47': Algorithm not licensed '68': Command disabled or a standard error code.
MAC	4 B	For use with a Variant LMK only. MAC on the public key and authentication data, calculated using the current LMK pair 36-37.
Public key	'S' + n B	For use with a Key Block LMK only. The translated Public Key, stored (without encryption) in key block format (which includes the MAC), using the current LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Import Key or data under an RSA Public Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: See Text	
Activity: command.gi.host	

Function: To translate a DES, AES or HMAC key from encryption under a public key to encryption under the LMK. A signature over the encrypted key is verified if present.

This command can also be used to decrypt data in place of the key where the EI command was used to generate an RSA key pair with Key Type Indicator = 4.

Notes: This command's requirement for Authorized State depends on the settings of the Configure Security console function:

Authorized State required when importing DES key under RSA key: Yes or No

This command's ability to import a ZMK is controlled by the following security setting:

Enable import of a ZMK: Yes or No

Refer to the Key Type Table in the *payShield 10K Host Programmer's manual* for key types and restrictions on key import.

For information about support for the RSA algorithm, see the *payShield 10K Host Programmer's manual*.

If the HSM is not in the Authorised state, the command will only allow import of an AES key (Import Key Type = '1') with Key Usage '55' and Mode Of Use 'E'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'GI'.
Encryption identifier	2 A	Identifier of algorithm used to decrypt the key: '01': RSA
Pad Mode Identifier	2 N	Identifier of the Pad Mode used in the encryption process: '01': PKCS#1 v1.5 method (EME-PKCS1-v1_5) '02': PKCS#1 v2.2 OAEP method (EME-OAEP-ENCODE)
Mask Generation Function	2 N	Identifier of the Mask Generation Function: '01': MGF1 as defined in PKCS#1 v2.2. Optional, only present if Pad Mode Identifier = '02' (OAEP).
MGF Hash Function	2 N	Identifier of the MGF hash function: '01': SHA-1 '05': SHA-224 '06': SHA-256 '07': SHA-384 '08': SHA-512 Optional, only present if Pad Mode Identifier = '02' (OAEP). This field defines the hash function to be used in the MGF.
OAEP Encoding Parameters Length	2 N	Optional, only present if Pad Mode Identifier = '02' (OAEP).
OAEP Encoding Parameters	n B	Optional, only present if Pad Mode Identifier = '02' (OAEP). If present, this field should be encoded according to PKCS#1 v2.2 Section A.2.1. The HSM does not interpret or validate the contents of this field. If OAEP padding is used, but no Encoding Parameters are provided, then OAEP Parameters Length should be '00', and this field will be empty.
OAEP Encoding Parameters Delimiter	1 A	Value ';'.
Key Type	4 N	For a Variant LMK: Used to indicate the required LMK pair & variant to use when encrypting the imported key. Format is 'PPVV', where 'P' are digits indicating the key pair, and 'V' are digits indicating the variant). For HMAC keys, Key Type should have the value '3401'. For data (e.g. TLS/SSL premaster) decryption with RSA Key Type Indicator '04', Key Type should have the value '3400'.
	or 4 H	For a Key Block LMK: This field is ignored; should be set to 'FFFF'.
The following section applies only when providing a signature on the key to be imported		
Signature Indicator	1 A	Value '='. Only present if the following signature related fields are also present.
Signature Hash Identifier	2 N	Identifier of hash algorithm used to hash message: '01': SHA-1 '02': MD5 '03': ISO 10118-2 '04': No Hash '05': SHA-224 '06': SHA-256 '07': SHA-384 '08': SHA-512
Signature Identifier	2 N	Identifier of the signature algorithm used to sign the message: '01': RSA
Signature Pad Mode Identifier	2 N	Identifier of the Pad Mode used in the signature process. 01 : PKCS#1 v1.5 method (EMSA-PKCS1-v1_5)
Encrypted Key Offset	4 N	Offset (in bytes) to first byte of encrypted key within the Data Block field.
Encrypted Key Length	4 N	Length (in bytes) of encrypted key within the Data Block field.
Signature Length	4 N	Length (in bytes) of the following Signature field.
Signature	n B	The signature which authenticates the encrypted key.
Delimiter	1 A	Value ';'.
		Used to indicate the end of the Signature field.

payShield 10K Core Host Commands

Field	Length & Type	Details						
The following section applies only when using a Variant LMK.								
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.						
Public Key	n B	The Public Key, used to validate the signature; DER encoded in ASN.1 format (sequence of modulus, exponent).						
Authentication data	n B	Optional. Additional data included in the MAC calculation (must not include ';' or '~').						
Delimiter	1 A	Value ';'. Used to indicate the end of the authentication data field.						
The following section applies only when using a Key Block LMK.								
Public Key	'S' + n B	<p>The Public Key used to validate the signature; must be in key block format, and comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'02'</td> <td>'R'</td> <td>'S', 'B', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'02'	'R'	'S', 'B', 'N'
Key Usage	Algorithm	Mode of Use						
'02'	'R'	'S', 'B', 'N'						
Data Block Length	4 N	Length (in bytes) of Data Block field.						
Data Block	n B	The Data Block field consists of either: <ul style="list-style-type: none"> • the encrypted key, or • the data (e.g. TLS/SSL premaster secret) when RSA Key Type Indicator is '04'. <i>Note: The format of the encrypted key is described in the payShield 10K Host Programmer's manual.</i> 						
Delimiter	1 A	Value ';'. Used to indicate end of the Data Block field.						
Private Key Flag	2 N	Flag to indicate location of the private key to decrypt the encrypted key; '00' ... '20': index of stored private key '99': use private key provided with command.						
Private Key Length	4 N	Optional. Must be present if the Private key flag = '99'.						
Private Key	or 4 H	<p>For a Variant LMK: Length (in bytes) of the next field.</p> <p>For a Key Block LMK: This field is ignored, and should be set to 'FFFF'.</p>						
	n B or 'S' + n B	<p>Optional. Must be present if the Private Key Flag = '99'. The Private Key, used to decrypt the imported key.</p> <p>For a Variant LMK, the 'Private Key' is encrypted under LMK pair 34-35. For a Key Block LMK, the 'Private Key' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'03', '06'</td> <td>'R'</td> <td>'D', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'03', '06'	'R'	'D', 'N'
Key Usage	Algorithm	Mode of Use						
'03', '06'	'R'	'D', 'N'						
The following 4 fields are only required when importing a DES/AES Key:								
1) Delimiter	1 A	Only present if the following fields are also present. Value ';'. The type of key to import. Valid values are: '0' – DES/3DES key '1' – AES key						
2) Import Key Type	1 A	Key Scheme for imported key when encrypted under LMK.						
3) Key Scheme LMK	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV						
4) Key Check Value Type	1 A							

Field	Length & Type	Details
The following 4 fields are only required when importing an HMAC key:		
1) Delimiter	1 A	Only present if the following HMAC fields are also present. For a Variant LMK: Value '#' or ' ' (ASCII X'7C). For a Key Block LMK: Value ' ' (ASCII X'7C).
2) HMAC Hash Identifier	2 N	Identifier of the Hash Algorithm: '01': SHA-1 '05': SHA-224 '06': SHA-256 '07': SHA-384 '08': SHA-512.
3) HMAC Key Usage	2 N	Key Usage value identifier: '01': HMAC Generation '02': HMAC Verification '03': HMAC Generation and Verification
4) HMAC Key Format	2 N	The format of the HMAC key when stored encrypted under the LMK. For a Variant LMK: '00': Thales HMAC Key format. For a Key Block LMK: '04': Thales Key Block format.
Delimiter	1 A	Value '='. Only present if the Key Data Block Type follows. Note: The '=' delimiter is used to distinguish from the normal ';' delimiter.
Key Data Block Type	2 N	'01': Legacy Key Data Block format (does not support HMAC keys) '02': Key Data Block Template (format of template is specified below). '03': Unformatted Key Data Block. '04': ASN.1 Encoded Key Data Block. Key Data Block Types '01', '02', and '03' may be used for importing DES/AES keys. Key Data Block Types '02', '03', and '04' may be used for importing HMAC keys. Only present if the '=' delimiter above is present. When not present, the value of Key Data Block Type will be '01'.
Key Data Block Template Length	4 N	Length of Key Data Block data. Only present if Key Data Block Type = '02'.
Key Data Block Template	n H	Key Data Block, DER encoded in ASN.1 format. Key data zero filled. Only present if Key Data Block Type = '02'.
Delimiter	1 A	Value ';'.
Key Length	2 A	Length of the Key within the Key Data Block. Only present if Key Data Block Type is '02'.
Key Offset	4 N	Offset to the location of the Key within the Key Data Block. Only present if Key Data Block Type = '02'.
Check value length	2 N	Length in bytes of Check value field. Permitted values '00' ... '08'. If no check value is supplied then this field will be '00'. If Check Value is supplied then the HSM will perform a validation check using the extracted key. If Key Data Block Type = '02' then Check Value is expected at position indicated by Check Value Offset.
Check value offset	4 N	Only present when importing DES/AES keys and if Key Data Block Type = '02'. Offset to the location of the check value within the Key Data Block. If Check Value length is '00' then this field is ignored. Only present when importing DES/AES keys and if Key Data Block Type = '02'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.

Field	Length & Type	Details
This section applies only when importing a DES/AES key and using a Key Block LMK.		
Delimiter	1 A	Value '#'. Must only be present when importing a DES/AES key, and returning it in key block format. If this delimiter is present, the following fields must also be present.
Key Usage	2 A	Key Usage field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Key Usage Table in the <i>payShield 10K Host Programmer's manual</i> .
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; only permitted value is 'N' or 'S'; must be present if the above Delimiter is present.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
The following section applies when importing an HMAC key and using a Key Block LMK.		
Delimiter	1 A	Value '#'. Must only be present when importing an HMAC key, and returning it in key block format. If this delimiter is present, the following fields must also be present.
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; only permitted value is 'N' or 'S'; must be present if the above Delimiter is present.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'GJ'.
Error Code	2 A	<p>'00': No error '01': MAC verification failure '02': Signature verification failure '03': Invalid private key type '04': Invalid private key flag '05': Invalid Key Type '06': Invalid encryption identifier '07': Invalid pad mode identifier '34': Invalid HMAC hash identifier value '35': Invalid HMAC key usage value '36': Invalid HMAC key format value '37': Invalid HMAC key block type value '47': Algorithm not licensed '50': Public key does not conform to encoding rules '51': Invalid message header '52': Invalid signature identifier '53': Invalid signature pad mode identifier '54': Invalid Encrypted Key Offset '55': Invalid Encrypted Key length '56': Signature/Signature Length mismatch '57': Invalid Key Check Value Type '68': Command disabled '74': Invalid Digest info syntax (no hash mode only) '76': Public Key length error '77': Clear data block error '78': Private key length error '79': Hash Algorithm Object Identifier error '80': Data Block length error '81': Invalid key data block type '82': Invalid check value length '83': Key block format error '84': Key block check value error '85': Invalid OAEP Mask Generation Function '86': Invalid OAEP MGF Hash Function '87': OAEP Parameter Error '88': OAEP Error or a standard error code.</p>
When importing a DES/AES key, the following 3 fields will be present:		
1) Initialization value	16 / 32 H	Initialization value for the DES/AES key. Optional. Only present if Key Data Block Type = '01'. The IV for a DES key is 16 H; the IV for an AES key is 32 H.
2) Key	16 / 32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The imported DES/AES Key, encrypted under the LMK. For a Variant LMK, the 'Key' is encrypted under the appropriate LMK pair/variant (as defined by the 'Key Type'). For a Key Block LMK, the 'Key' is encrypted under the LMK.
3) Key Check Value	16 / 6 H	The key check value of the imported key. 16 / 6 H depending on chosen Key Check Value option. 16 H if the Key Check Value Type field is absent.
When importing an HMAC key, the following 2 fields will be present:		
HMAC Key Length	4 N	For a Variant LMK: Length (in bytes) of the next field.
Key	or 4 H	For a Key Block LMK: This field is reserved, and set to 'FFFF'.
		The imported HMAC Key, encrypted under the LMK.
	n B	For a Variant LMK, the 'HMAC Key' is encrypted under the LMK pair 34-35 variant 1.
	or n A	For a Key Block LMK, the 'HMAC Key' is encrypted under the LMK.

Field	Length & Type	Details
When importing data (e.g. TLS/SSL pre-master secret) using RSA Key Type Indicator '04', the following 2 fields will be present:		
TLS Data Length	4 N	Data or TLS/SSL clear-text premaster length.
TLS Data	n B	Data or TLS/SSL clear-text premaster.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Export Key under an RSA Public Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Variant LMK	Authorization: Determined by KTT(E) Activity: export.{key}.host
Key Block LMK	Authorization: Not required

Function: Translate a DES, AES or HMAC key from encryption under an LMK pair to encryption under a public key. A signature is optionally generated over the encrypted Key.

Notes: The requirement for authorization for this command depends on the type of LMK being used. When using a Variant LMK, this command examines the Key Type Table (see the *payShield 10K Host Programmer's manual*) to determine the authorization requirement.

This command does not require authorization when using a Key Block LMK.

For information about support for the RSA algorithm, see the *payShield 10K Host Programmer's manual*.

This command's ability to export DES or AES keys is controlled by the following security setting:

Enforce PCI HSMv3 Key Equivalence for Key Wrapping: YES or NO

When set to 'YES', the RSA key must have equivalent or greater strength than the key being exported, and Pad Mode Identifier '01' (PKCS#1 v1.5 method (EME-PKCS1-v1_5)) cannot be used.

This command's ability to export a ZMK is controlled by the following security setting:

Enable export of a ZMK: YES or NO

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'GK'.
Encryption Identifier	2 N	Identifier of algorithm used to encrypt the key: '01': RSA
Pad Mode Identifier	2 N	Identifier of the padding mode used in the encryption process: '01': PKCS#1 v1.5 method (EME-PKCS1-v1_5) '02': PKCS#1 v2.2 OAEP method (EME-OAEP-ENCODE)
Mask Generation Function	2 N	Identifier of the mask generation function: '01': MGF1 as defined in PKCS#1 v2.2. Optional, only present if Pad Mode Identifier = '02' (OAEP).

Field	Length & Type	Details
MGF Hash Function	2 N	Identifier of the MGF Hash Function: '01': SHA-1 '05': SHA-224 '06': SHA-256 '07': SHA-384 '08': SHA-512
OAEP Encoding Parameters Length	2 N	Optional, only present if Pad Mode Identifier = '02' (OAEP). This field defines the hash function to be used in the MGF.
OAEP Encoding Parameters	n B	Optional, only present if Pad Mode Identifier = '02' (OAEP).
OAEP Encoding Parameters Delimiter	1 A	Value ';'. Optional, only present if Pad Mode Identifier = '02' (OAEP).
Key Type	4 N	For a Variant LMK: Used to indicate the required LMK pair & variant to use for the exported key. Format is 'PPVV', where 'P' are digits indicating the key pair, and 'V' are digits indicating the variant. For HMAC keys, Key Type should have the value '3401'.
	or 4 H	For a Key Block LMK: This field is ignored; should be set to 'FFFF'.

The following section applies only when generating a signature over the exported key

Signature Indicator	1 A	Value '='. Only present if the following signature related fields are also present.
Signature Hash Identifier	2 A	Identifier of the hash algorithm used to hash the message: '01': SHA-1 '02': MD5 '03': ISO 10118-2 '04': No Hash '05': SHA-224 '06': SHA-256 '07': SHA-384 '08': SHA-512
Signature Identifier	2 A	Identifier of the signature algorithm used to sign the message: '01': RSA
Signature Pad Mode Identifier	2 N	Identifier of the Pad Mode to be used in the signature process: '01': PKCS#1 v1.5 method (EMSA-PKCS1-v1_5)
Header Data Block Length	4 N	Length (in bytes) of following field. If no Header Data Block is to be supplied, then this field should be set to '0000'.
Header Data Block Delimiter	n B	Block of data to be pre-pended to the encrypted key, prior to signing.
Footer Data Block Length	1 A	Value ';'.
Footer Data Block	4 N	Length (in bytes) of following field. If no Footer Data Block is to be supplied, then this field should be set to '0000'.
Footer Data Block Delimiter	n B	Block of data to be appended to the encrypted key, prior to signing.
Private Key Flag	1 A	Value '='.
Private Key Length	2 N	Flag to indicate location of the private key; '00' ... '20': index of stored private key '99': use private key provided with command
	4 N	Optional. Must be present if Private Key Flag = '99'. For a Variant LMK: Length (in bytes) of the next field.
Private Key	or 4 H	For a Key Block LMK: This field is ignored, and should be set to 'FFFF'. Optional. Must be present if the Private Key Flag = '99'. The Private Key, used to generate the signature.
	n B	For a Variant LMK, the 'Private Key' is encrypted under LMK pair 34-35.

Field	Length & Type	Details						
Delimiter	or 'S' + n B	For a Key Block LMK, the 'Private Key' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'03'</td><td>'R'</td><td>'S', 'B', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'03'	'R'	'S', 'B', 'N'
Key Usage	Algorithm	Mode of Use						
'03'	'R'	'S', 'B', 'N'						
Delimiter	1 A	Optional. Must be present if the Private Key Flag = '99'. Value ';'. The following section applies only when exporting a DES/AES key						
The following section applies only when exporting a DES/AES key								
DES Key Flag	1 N	For a Variant LMK: This field indicates length of the DES key: '0': single length '1': double length '2': triple length						
DES/AES Key (under LMK)	1 A	For a Key Block LMK: This field is ignored, and should be set to 'F'. The DES/AES key to be exported, encrypted under the LMK.						
Check Value	16 / 32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	For a Variant LMK, the 'Key' must be encrypted under the appropriate LMK pair/variant (as defined by the 'Key Type'). For a Key Block LMK, the 'Key' must be encrypted under the LMK.						
Check Value	16 H or 6 H	Check value on the DES/AES key. For DES keys: This field is always 16 H. For AES keys: This field is always 6 H.						
The following section applies only when exporting an HMAC key								
HMAC Key Format	2 N	The format of the HMAC key when stored encrypted under the LMK. For a Variant LMK: '00': Thales HMAC Key format.						
HMAC Key Length	4 N	For a Key Block LMK: '04': Thales Key Block format.						
HMAC Key (under LMK)	4 H or n B or n A	For a Variant LMK: Length (in bytes) of the next field. For a Key Block LMK: This field is reserved, and set to 'FFFF'. The HMAC key to be exported, encrypted under the LMK. For a Variant LMK, the 'HMAC Key' is encrypted under the LMK pair 34-35 variant 1. For a Key Block LMK, the 'HMAC Key' is encrypted under the LMK.						
Delimiter	1 A	Only present when using a Variant LMK. Value ';'. The following section applies only when using a Variant LMK.						
The following section applies only when using a Variant LMK.								
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37 variant 0.						
Public Key	n B	The Public Key, used to encrypt the key to be exported; DER encoded in ASN.1 format (sequence of modulus, exponent).						
Authentication data	n B	Optional. Additional data to be included in the MAC calculation (must not include ';' or '-').						
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present, below.						
The following section applies only when using a Key Block LMK.								
Public Key	'S' + n B	The Public Key used to encrypt the key to be exported; must be in key block format, and comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'02'</td><td>'R'</td><td>'E', 'B', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'02'	'R'	'E', 'B', 'N'
Key Usage	Algorithm	Mode of Use						
'02'	'R'	'E', 'B', 'N'						

Field	Length & Type	Details
Delimiter	1 A	Value ':'. Only present if the Key Block Type field below is present.
Key Block Type	2 N	'01': Legacy Key Data Block format (does not support HMAC keys). '02': Key Data Block Template (format of template is specified below). '03': Unformatted Key Data Block. '04': ASN.1 Encoded Key Data Block. Key Data Block Types '01', '02', and '03' may be used for exporting DES/AES keys. Key Data Block Types '02', '03', and '04' may be used for exporting HMAC keys. This field is optional. When not present, the value of Key Data Block Type will be '01'.
Key Data Block Template Length	4 N	Length of Key Data Block data. Optional, only present if Key Data Block Type = '02'.
Key Data Block Template	n H	Key Data Block, DER encoded in ASN.1 format. Key data and Check Value data (if present) zero filled. Optional, only present if Key Data Block Type = '02'.
Delimiter	1 A	Value ':'. Optional, only present if Key Data Block Type = '02'.
Key Offset	4 N	Offset to the position within the Key Data Block to insert the key. Optional, only present if Key Data Block Type = '02'.
Check Value Length	2 N	Length in bytes of Check Value field. Permitted values are '00' ... '08'. If no check value is required then this field should be set to 0. If a check value length is specified, then the HSM will generate a check value and include it in the Key Data Block, inserted at the position indicated by Check Value Offset. Optional, only present when exporting a DES/AES key and if Key Data Block Type = '02'.
Check Value Offset	4 N	Offset to the position within the Key Data Block to insert a check value. If Check Value length = '00', then this field is ignored. Optional, only present when exporting a DES/AES key and if Key Data Block Type = '02'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'GL'.
Error Code	2 A	<p>'00': No error '01': MAC verification failure '02': Check value verification failure '03': Invalid Private key type '04': Invalid Private key flag '05': Invalid DES/AES key type '06': Invalid encryption identifier '07': Invalid pad mode identifier '08': HMAC Key Block error '10': DES Key parity error '34': Invalid HMAC hash identifier value '35': Invalid HMAC key usage value '36': Invalid HMAC key format value '47': Algorithm not licensed '50': Public key does not conform to encoding rules '51': Invalid message header '52': Invalid signature identifier '53': Invalid signature pad mode identifier '54': Header Data Block error '55': Footer Data Block error '56': Invalid DES key flag '68': Command disabled '74': Invalid DigestInfo syntax (no hash mode only) '76': Key Data Block length error '78': Private key length error '81': Invalid key data block type '82': Invalid check value length '83': Key block format error '84': Key block check value error '85': Invalid OAEP Mask Generation Function '86': Invalid OAEP MGF Hash Function '87': OAEP Parameter Error '88': OAEP Error 'D3': Key Error / PCI HSM V3 Key Equivalence criteria not met or a standard error code.</p>
Initialization value	16 / 32 H	<p>Initialization value for DES/AES key. Only present when exporting a DES/AES key using Key Data Block Type '01'. The IV for a DES key is 16 H; the IV for an AES key is 32 H.</p>
Encrypted Key Length	4 N	Length (in bytes) of the next field.
Encrypted Key	n B	Key, encrypted under the public key.
Signature Length	4 N	Length (in bytes) of the next field. Only present when the Signature Indicator is present.
Signature	n B	Signature of concatenation of header data block, encrypted key, and footer data block. Only present when the Signature Indicator is present.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a Certificate Request

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not Required	

Function: This command generates a Certificate Signing Request (CSR) by signing the Subject and Public Key information with the corresponding Private Key to create a Self-Signed Certificate in PKCS#10 format.

Notes: The command either accepts individual Subject fields and builds the DER encoded Subject field or accepts a DER encoded Subject template. For example:

31 0B

 30 09

 06 03 550406 [2.5.4.6 - countryName]

 13 02 554B

31 0E

 30 0C

 06 03 550408 [2.5.4.8 - state]

 13 05 4275636B73

31 15

 3013

 06 03 550407 [2.5.4.7 - localityName]

 13 0C 4C6F6E67204372656E646F6E

31 19

 30 17

 06 03 55040A [2.5.4.10 - organisationName]

 1310 5468616C65732D655365637572697479

31 14

 30 12

 06 03 55040B [2.5.4.11 - organisationUnitName]

 13 0B 456E67696E656572696E67

31 20

 30 1E

 06 03 550403 [2.5.4.3 - commonName]

 13 17 7777772E7468616C65732D73656375726974792E636F6D

Field	Length & Type	Details									
COMMAND MESSAGE											
Message Header	m A	Subsequently returned to the Host unchanged.									
Command Code	2 A	Value 'QE'.									
CSR Type	1 N	The format for the certificate request: '0': PKCS#10									
CSR Output Format	1 N	'0': Base 64 encoded PEM '1': Hexadecimal DER encoding									
Signature ID	2 N	Identifier of the signature algorithm used to sign the message: '01': RSA '02': ECC									
Public Key Encoding	2 N	Encoding rules for the Public Key. For Signature ID = '01' (RSA): '01': DER encoded ASN.1 RSA Public Key (INTEGER using unsigned representation). '02': DER encoded ASN.1 RSA Public Key (INTEGER using 2's complement representation). For Signature ID = '02' (ECC): '03': DER encoded ASN.1 ECC Public Key in X9.62 format.									
Public Key	n B	Public Key, encoded as specified above.									
Private Key	'S' + n A	The subject private key must be in LMK key block format, and must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'03', '06'</td><td>'R'</td><td>'S', 'D', 'N'</td></tr> <tr> <td>'03'</td><td>'E'</td><td>'S', 'X', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'03', '06'	'R'	'S', 'D', 'N'	'03'	'E'	'S', 'X', 'N'
Key Usage	Algorithm	Mode of Use									
'03', '06'	'R'	'S', 'D', 'N'									
'03'	'E'	'S', 'X', 'N'									
Pad Mode Identifier	2 N	Only present if Signature ID = '01' (RSA): Identifier of the padding mode used in signature generation. '01': PKCS#1 v1.5 method (EMSA-PKCS1-v1_5) '04': PKCS#1 v2.2 method RSASSA-PSS									
Hash Identifier	2 N	Identifier of the hash algorithm used in CSR. Valid values are: '01': SHA-1 (RSA only) '06': SHA-256 '07': SHA-384 '08': SHA-512									
MGF Function	1 N	Only present if Pad Mode Identifier is '04'. The Mask Generation Function. Valid values are: '1': MGF1 as defined in PKCS1 V2.1									
Subject Data Type	1 N	'0': Use supplied template '1': Specify subject									
If Subject Data Type is '0', the following 3 fields must be present:											
Subject Template Length	4 N	Length of the following field.									
Subject Template	n H	ASN.1 DER encoded Subject.									
Delimiter	1 A	Value ';'.									
If Subject Data Type is '1', the following 12 fields must be present:											
Common Name	n A	Between 1 and 64 characters.									
Delimiter	1 A	Value ';'.									
Organization	n A	Between 1 and 64 characters.									
Delimiter	1 A	Value ';'.									
Organizational Unit Name	n A	Between 1 and 64 characters.									
Delimiter	1 A	Value ';'.									
Locality	n A	Between 1 and 64 characters.									
Delimiter	1 A	Value ';'.									
State	n A	Between 1 and 64 characters.									
Delimiter	1 A	Value ';'.									
Country	2 A	The ISO country code.									
Delimiter	1 A	Value ';'.									

Field	Length & Type	Details
Delimiter	1 A	Value '='. Optional; if present, the following field must also be present.
CSR attribute SET OF	1 N	Allows the user to specify the precise format of the SET OF attribute in the CSR. Valid values are: '0': Omit the SET OF structure from the Attributes section of the CSR '1': Include the SET OF structure in the Attributes section of the CSR
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'QF'.
Error Code	2 A	'00': No error '05': Invalid hash identifier '07': Invalid pad mode identifier 'D2': Invalid curve reference value 'E0': Invalid CSR type value 'E1': Invalid CSR Output format 'E2': Invalid Public Key Format value 'E3': Public Key block error 'E4': Invalid public key 'E5': Private Key block error 'E6': Invalid MGF Function 'E7': Invalid Subject Data Type 'E8': Subject Data is not valid DER encoding 'E9': CSR attribute SET OF field is missing after '=' delimiter or a standard error code.
If Error Code is 'E3', 'E5', the following field will be present:		
Additional Error Code	2 N	The key block specific error code
If Error Code is '00', the following fields will be present:		
CSR Length	4 N	The length of the certificate request
CSR	n A or n H	If the CSR output format is '0' If the CSR output format is '1'
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Key Derivation using Elliptic Curve Key Agreement

This command derives symmetric keys using an Elliptic Curve Key Agreement Algorithm (ECKA). The command supports either ECKA-EG using ephemeral/static keys or ECKA-DH using ephemeral keys only.

Note: The host application is responsible for the authentication of the initiator's ephemeral ECC public key.

This command has three modes (initiate, process, complete) for each of the two agreement types (ECKA-EG and ECKA-DH), and each of these 6 possible permutations are described as separate entries in this document.

When the Security Setting "Enforce PCI HSMv3 Key Equivalence for Key Wrapping" set to YES, it will not be possible to derive symmetric keys that have a higher cryptographic strength than the supplied ECC keys.

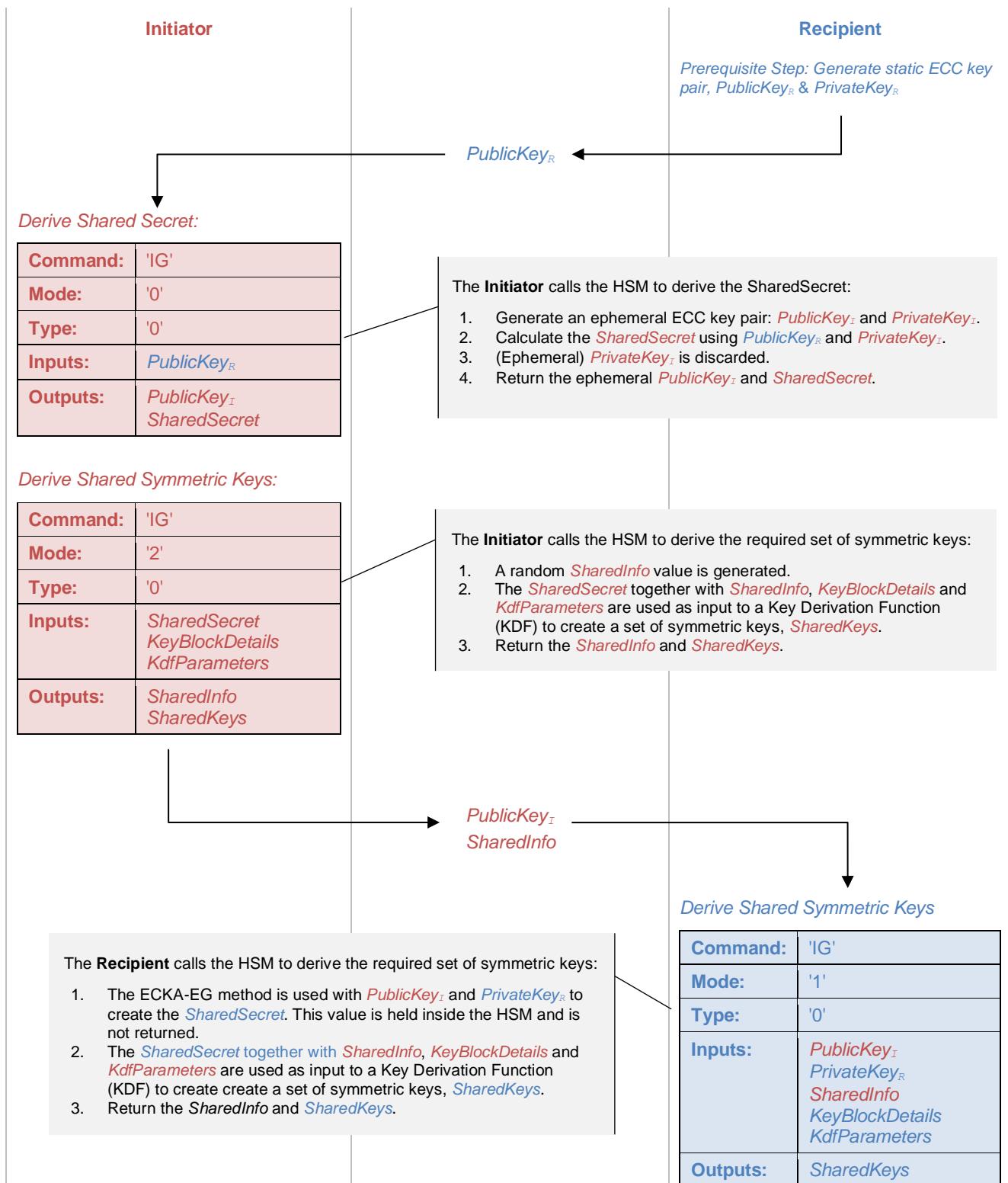
For information about support for the ECC algorithm, see the *payShield 10K Host Programmer's manual*.

Function	Command	Page
<i>Key Derivation using ECKA-EG (Initiator: Derive Shared Secret)</i>	'IG'	225
<i>Key Derivation using ECKA-EG (Recipient: Derive Shared Secret/Keys)</i>	'IG'	227
<i>Key Derivation using ECKA-EG/DH (Derive Shared Keys)</i>	'IG'	231
<i>Key Derivation using ECKA-DH (Initiator: Create Ephemeral Keys)</i>	'IG'	234
<i>Key Derivation using ECKA-DH (Recipient: Derive Shared Secret/Keys)</i>	'IG'	236
<i>Key Derivation using ECKA-DH (Initiator: Derive Shared Keys)</i>	'IG'	240

ECKA-EG Example

In this example, two independent parties (**Initiator** and **Recipient**) each use their own payShield 10K to securely derive the same set of shared symmetric keys using the ECKA-EG method. The **Initiator** uses an ephemeral ECC key pair, whereas the **Recipient** uses a static ECC key pair.

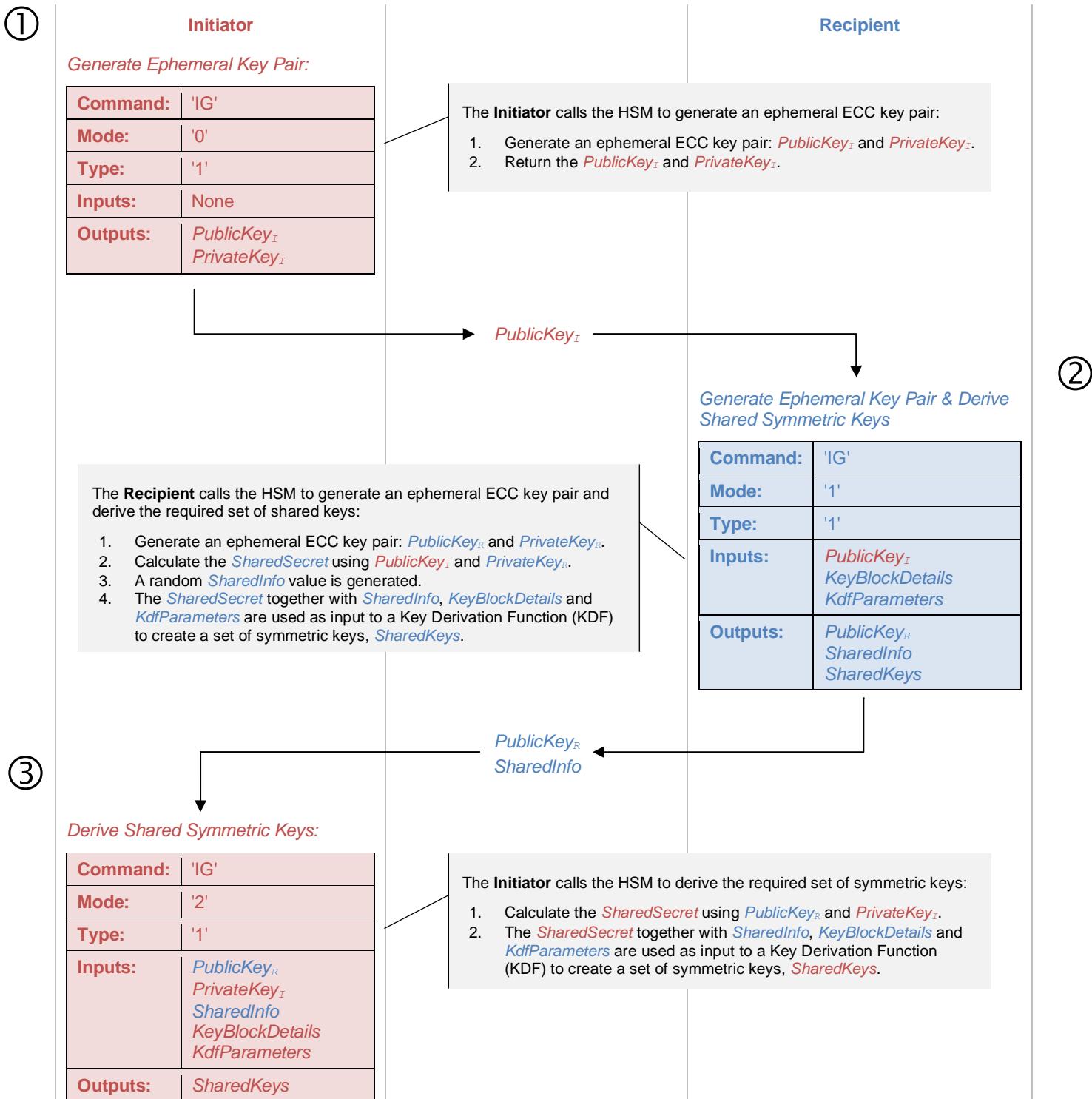
Note that the **Initiator** and **Recipient** must use the same set of input parameters (except ECC keys) in order to derive the same set of symmetric keys. In other words, they must use the same values for *SharedInfo*, *KeyBlockDetails*, *KdfParameters*, etc.



ECKA-DH Example

In this example, two independent parties (**Initiator** and **Recipient**) each use their own payShield 10K to securely derive the same set of shared symmetric keys using the ECKA-DH method. Both the **Initiator** and the **Recipient** use ephemeral ECC key pairs.

Note that the **Initiator** and **Recipient** must use the same set of input parameters (except ECC keys) in order to derive the same set of symmetric keys. In other words, they must use the same values for *SharedInfo*, *KeyBlockDetails*, *KdfParameters*, etc.



Key Derivation using ECKA-EG (Initiator: Derive Shared Secret)

Variant LMK <input checked="" type="checkbox"/>	AES Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not Required	

Function: This command derives and returns a shared secret using the Elliptic Curve Key Agreement / El-Gamal (static/ephemeral) method. The initiator of the key agreement will use an ephemeral ECC key pair, while the recipient will use a static ECC key pair.

Prior to this call, the initiator will need to obtain a copy of the recipient's (static) ECC public key.

The initiator's shared secret is calculated by performing an ECC point multiplication of the recipient's static ECC public key and the initiator's ephemeral ECC private key. The initiator's ephemeral ECC public key is returned – to be shared with the recipient.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IG'.						
Mode	1 N	'0': Initiator: Start ECKA-EG						
Agreement Type	1 N	'0': Ephemeral-Static (El-Gamal)						
Public Key Encoding	2 N	The encoding of the Recipient's static Public Key. Valid values are: '03': X9.62 ASN.1 format '04': Uncompressed encoding '05': ISO 7816 format '06': Public Key in key block format						
Curve Reference	2 H	Only present if Public Key Encoding = '04' or '05'. The ECC curve of the following Public Key. Valid values are: '00': FIPS 186-3 – NIST P-256 curve '01': FIPS 186-3 – NIST P-384 curve '02': FIPS 186-3 – NIST P-521 curve						
Public Key Length	4 N	Only present if Public Key Encoding = '04'. The length of the following field.						
Public Key	n B or 'S' + n A	The Recipient's static Public Key. For Public Key Encoding = '03', '04', '05', the raw public key is provided in the specified format. For Public Key Encoding = '06', the public key is provided in Thales Key Block format, which should comply with the following:						
		<table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'02'</td> <td>'E'</td> <td>'X'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'02'	'E'	'X'
Key Usage	Algorithm	Mode of Use						
'02'	'E'	'X'						
Output Public Key Encoding	2 N	The format for the output ephemeral ECC Public Key. Valid values are: '03': X9.62 ASN.1 format '04': Uncompressed encoding '05': ISO 7816 format						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IH'.
Error Code	2 N	<p>'00': No error '01': SHS CMAC verification failed. '79': Invalid hash identifier 'A1': Invalid LMK scheme 'A5': Incompatible key length/algorithm combination 'B2': Bad end of keys delimiter 'D0': Invalid Mode 'D1': Invalid Agreement Type 'D2': Invalid curve reference 'D3': Invalid public key block 'D4': Invalid public key 'D5': Curve not supported 'D6': Invalid Public Key Input format 'D7': Invalid Public Key, does not conform to ASN1 encoding. 'D8': Invalid Public Key, does not conform to TLV format. 'D9': Private key block error 'DA': Invalid Shared Info length 'DB': Public key is not uncompressed format 'DD': Invalid KDF value 'DE': Invalid Single Hash mode value 'DF': Invalid Salt Length 'E0': Invalid Hash Option 'E1': Invalid Shared Information Flag 'E2': Invalid Number of SHS value 'E3': Invalid Key derivation Flag 'E4': Invalid number of keys specified 'E5': Invalid salt value 'E8': Invalid Shared Secret length 'E9': Invalid SHS value 'EA': ECC Curve not strong enough to derive keys 'EB': Invalid public key output format 'EC': Invalid Key Strength value in SHS or a standard error code </p>
If Error Code = 'D3' or 'D9', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
Public Key Length	4 N	The length (in bytes) of the following field.
Ephemeral Public Key	n B	The Initiator's ephemeral ECC Public Key in Public Key Output Format.
SHS Length	3 N	The length (in bytes) of the following field.
SHS	n B	The Shared Secret, encrypted under the LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Key Derivation using ECKA-EG (Recipient: Derive Shared Secret/Keys)

Variant LMK <input checked="" type="checkbox"/>	AES Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not Required	

Function: This command returns a shared secret or a set of shared keys using the Elliptic Curve Key Agreement / El-Gamal (static/ephemeral) method. The initiator of the key agreement will use an ephemeral ECC key pair, while the recipient will use a static ECC key pair.

Note: The host application is responsible for the authentication of the initiator's ephemeral ECC public key.

The recipient's shared secret is calculated by performing an ECC point multiplication of the initiator's ephemeral ECC public key and the recipient's static ECC private key.

The shared keys are optionally derived from the shared secret using a specified Key Derivation Function (KDF). Up to 99 shared symmetric (DES/AES/HMAC) keys may be derived from the shared secret(s).

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IG'.						
Mode	1 N	'1': Recipient:Process ECKA-EG						
Agreement Type	1 N	'0': Ephemeral-Static (El-Gamal)						
Public Key Encoding	2 N	The encoding of the following Public Key. Valid values are: '03': X9.62 ASN.1 format '04': Uncompressed encoding '05': ISO 7816 format						
Curve Reference	2 H	Only present if Public Key Encoding = '04' or '05'. The ECC curve of the following Initiator's Public Key. Valid values are: '00': FIPS 186-3 – NIST P-256 curve '01': FIPS 186-3 – NIST P-384 curve '02': FIPS 186-3 – NIST P-521 curve						
Public Key Length	4 N	Only present if Public Key Encoding = '04'. The length of the following field.						
Public Key	n B	The Initiator's ephemeral Public Key. For Public Key Encoding = '03', '04', '05', the raw public key is provided in the specified format.						
Private Key	'S' + n A	The Recipient's static Private Key, encrypted under the LMK, which must comply with:						
		<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'03'</td> <td>'E'</td> <td>'X'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'03'	'E'	'X'
Key Usage	Algorithm	Mode of Use						
'03'	'E'	'X'						
Key Derivation Flag	1 N	Indicates whether to perform the key derivation, or to output the Shared Secret. '0': Defer key derivation and output Shared Secret '1': Perform key derivation						
If Key Derivation Flag = '1', the following section applies:								
KDF Method	1 N	Indicates the Key Derivation Function. Valid values are: '0': HKDF (RFC 5869) '1': Single Step KDF (NIST SP800-56A) '2': KDF (ANSI X9.63)						
Hash Identifier	2 N	Identifier of the hash algorithm used in the KDF. Valid values are: '06': SHA-256						

Field	Length & Type	Details
Single Hash Mode	1 N	Only present if KDF Method is '0'. Valid values are: '0': Include ephemeral public key in KDF.
Salt Length	2 N	Only present if KDF Method is '0'. The length of the following field. If a Salt value is not required, then the Salt Length should be set to '00'.
Salt	n H	Only present if KDF Method is '0'. The Salt value to be used in the KDF.
Delimiter	1 A	Only present if KDF Method is '0'. Value ';'.
Hash Option	1 N	Only present if KDF Method is '1'. Valid values are: '1': Use hash function (H(x) = hash(x))
Shared Information Flag	1 N	Valid values are: '0': Use supplied Shared Information in KDF '1': Use random Shared Information in KDF
Shared Information Length	3 N	If Shared Information Flag = '0', this field specifies the length (in hex characters) of the following field. If Shared Information Flag = '1', this field specifies the required length (in bytes) of the randomly generated Shared Information. If not required, this field should be set to '000'.
Shared Information	n H	Only present if Shared Information Flag = '0'. The Shared Information between the two parties and used in the key derivation process. Example: if using "Thales" as the Shared Information, this would be presented as the following sequence of hex digits: 5468616C6573 and the Shared Information Length field should then contain 012 indicating a length of 12 hex digits. Note: When sharing this information with another system, ensure that the two systems use the same representation of the Shared Information – i.e. both systems must use hex-encoded ASCII or both systems must use a byte string.
Delimiter	1 A	Only present if Shared Information Flag = '0'. Value ';'.

Field	Length & Type	Details
Number of Keys	2 N	The number of symmetric keys to derive and output. Must be greater than '00'.
The following section will be repeated for the Number of Keys to be derived:		
Key Length	5 N	The key length in bits.
Key Usage	2 A	Key Usage field, to be included in the Key Block header. Any valid Thales Key Block Key Usage value is permitted, but it must be compatible with the following Algorithm and Mode of Use fields.
Algorithm	2 A	Algorithm and Key Length; the first character will be included in the algorithm field in the Key Block header (byte 7): <ul style="list-style-type: none"> • 'D1' – single length DES key • 'T2' – double length DES key • 'T3' – triple length DES key • 'A1' – 128-bit AES key • 'A2' – 192-bit AES key • 'A3' – 256-bit AES key • 'H0' – HMAC key
Mode of Use	1 A	Mode of Use field, to be included in the key block header. Any valid Thales Key Block Mode of Use value is permitted, but it must be compatible with the Key Usage and Algorithm fields specified above.
Key Version Number	2 N	Key Version Number field to be included in the key block header. Permitted values: '00' to '99'.
Exportability	1 A	Exportability field to be included in the key block header. Permitted values: 'N', 'E' or 'S'.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Block Identifier	2 A	Block Identifier; any permitted value except 'PB'.
Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Block Data	n A	The block data.
Delimiter	1 A	Value ':'. Denotes the end of a single key definition.
Delimiter	1 A	Value '%'. Denotes the end of all key definitions.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19'.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IH'.
Error Code	2 N	<p>'00': No error '01': SHS CMAC verification failed. '79': Invalid hash identifier 'A1': Invalid LMK scheme 'A5': Incompatible key length/algorithm combination 'B2': Bad end of keys delimiter 'D0': Invalid Mode 'D1': Invalid Agreement Type 'D2': Invalid curve reference 'D3': Invalid public key block 'D4': Invalid public key 'D5': Curve not supported 'D6': Invalid Public Key Input format 'D7': Invalid Public Key, does not conform to ASN1 encoding. 'D8': Invalid Public Key, does not conform to TLV format. 'D9': Private key block error 'DA': Invalid Shared Info length 'DB': Public key is not uncompressed format 'DD': Invalid KDF value 'DE': Invalid Single Hash mode value 'DF': Invalid Salt Length 'E0': Invalid Hash Option 'E1': Invalid Shared Information Flag 'E2': Invalid Number of SHS value 'E3': Invalid Key derivation Flag 'E4': Invalid number of keys specified 'E5': Invalid salt value 'E8': Invalid Shared Secret length 'E9': Invalid SHS value 'EA': ECC Curve not strong enough to derive keys 'EB': Invalid public key output format 'EC': Invalid Key Strength value in SHS or a standard error code </p>
If Error Code = 'D3' or 'D9', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
SHS Length	3 N	Only present if Key Derivation Flag is '0'. The length (in bytes) of the following field.
SHS	n B	Only present if Key Derivation Flag is '0'. The Shared Secret, encrypted under the LMK.
The following section will be repeated for the Number of Keys requested:		
Key	'S' + n B	The derived key, encrypted under the LMK.
Key Check Value	3 B or 6 B	The check value of the derived key.
Shared Information	n H	Only present if Shared Information Flag is '1'. The randomly generated Shared Information used in the KDF.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Key Derivation using ECKA-EG/DH (Derive Shared Keys)

Variant LMK <input checked="" type="checkbox"/>	AES Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not Required	

Function: This command returns a set of shared keys using the Elliptic Curve Key Agreement / El-Gamal (static/ephemeral) or Diffie-Hellman (ephemeral/ephemeral) methods.

This command can be used by both the initiator and the recipient to derive keys from one or more shared secrets which have been returned from previous calls to the 'IG' command.

The shared keys are derived from the shared secret using a specified Key Derivation Function (KDF). Up to 99 shared symmetric (DES/AES/HMAC) keys may be derived from the shared secret(s).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'IG'.
Mode	1 N	'2': Initiator/Recipient: Complete ECKA
Agreement Type	1 N	'0': Ephemeral-Static (El-Gamal) or Ephemeral-Ephemeral (Diffie-Hellman)
Number of SHS	1 N	The number of Shared Secrets for key derivation
The following section will be repeated for the Number of SHS:		
SHS Length	3 N	The length (in bytes) of the following field.
SHS	n B	The Shared Secret, encrypted under the LMK.
Delimiter	1 A	Value ';'.
KDF Method	1 N	Indicates the Key Derivation Function. Valid values are: '0': HKDF (RFC 5869) '1': Single Step KDF (NIST SP800-56A) '2': KDF (ANSI X9.63)
Hash Identifier	2 N	Identifier of the hash algorithm used in the KDF. Valid values are: '06': SHA-256
Public Key Encoding	2 N	Only present if KDF Method is '0'. The encoding of the following Initiator's Public Key. Valid values are: '03': X9.62 ASN.1 format '04': Uncompressed encoding '05': ISO 7816 format
Public Key Length	4 N	Only present if KDF Method is '0' and if Public Key Encoding = '04'. The length of the following field.
Public Key	n B	Only present if KDF Method is '0'. The Initiator's Public Key to be used during the KDF process.
Single Hash Mode	1 N	Only present if KDF Method is '0'. Valid values are: '0': Include ephemeral public key in KDF.
Salt Length	2 N	Only present if KDF Method is '0'. The length of the following field. If a Salt value is not required, then the Salt Length should be set to '00'.
Salt	n H	Only present if KDF Method is '0'. The Salt value to be used in the KDF.
Delimiter	1 A	Only present if KDF Method is '0'. Value ';'.
Hash Option	1 N	Only present if KDF Method is '1'. Valid values are: '1': Use hash function (H(x) = hash(x))

Field	Length & Type	Details
Shared Information Flag	1 N	Valid values are: '0': Use supplied Shared Information in KDF '1': Use random Shared Information in KDF
Shared Information Length	3 N	If Shared Information Flag = '0', this field specifies the length (in hex characters) of the following field. If Shared Information Flag = '1', this field specifies the required length (in bytes) of the randomly generated Shared Information. If not required, this field should be set to '000'.
Shared Information	n H	Only present if Shared Information Flag = '0'. The Shared Information between the two parties and used in the key derivation process. Example: if using "Thales" as the Shared Information, this would be presented as the following sequence of hex digits: 5468616C6573 and the Shared Information Length field should then contain 012 indicating a length of 12 hex digits. Note: When sharing this information with another system, ensure that the two systems use the same representation of the Shared Information – i.e. both systems must use hex-encoded ASCII or both systems must use a byte string.
Delimiter	1 A	Only present if Shared Information Flag = '0'. Value ';'.
Number of Keys	2 N	The number of symmetric keys to derive and output. Must be greater than '00'.
The following section will be repeated for the Number of Keys to be derived:		
Key Length	5 N	The key length in bits.
Key Usage	2 A	Key Usage field, to be included in the Key Block header. Any valid Thales Key Block Key Usage value is permitted, but it must be compatible with the following Algorithm and Mode of Use fields.
Algorithm	2 A	Algorithm and Key Length; the first character will be included in the algorithm field in the Key Block header (byte 7): <ul style="list-style-type: none">• 'D1' – single length DES key• 'T2' – double length DES key• 'T3' – triple length DES key• 'A1' – 128-bit AES key• 'A2' – 192-bit AES key• 'A3' – 256-bit AES key• 'H0' – HMAC key
Mode of Use	1 A	Mode of Use field, to be included in the key block header. Any valid Thales Key Block Mode of Use value is permitted, but it must be compatible with the Key Usage and Algorithm fields specified above.
Key Version Number	2 N	Key Version Number field to be included in the key block header. Permitted values: '00' to '99'.
Exportability	1 A	Exportability field to be included in the key block header. Permitted values: 'N', 'E' or 'S'.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Block Identifier	2 A	Block Identifier; any permitted value except 'PB'.
Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Block Data	n A	The block data.
Delimiter	1 A	Value ';'. Denotes the end of a single key definition.
Delimiter	1 A	Value ':'. Denotes the end of all key definitions.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IH'.
Error Code	2 N	<p>'00': No error '01': SHS CMAC verification failed. '79': Invalid hash identifier 'A1': Invalid LMK scheme 'A5': Incompatible key length/algorithm combination 'B2': Bad end of keys delimiter 'D0': Invalid Mode 'D1': Invalid Agreement Type 'D2': Invalid curve reference 'D3': Invalid public key block 'D4': Invalid public key 'D5': Curve not supported 'D6': Invalid Public Key Input format 'D7': Invalid Public Key, does not conform to ASN1 encoding. 'D8': Invalid Public Key, does not conform to TLV format. 'D9': Private key block error 'DA': Invalid Shared Info length 'DB': Public key is not uncompressed format 'DD': Invalid KDF value 'DE': Invalid Single Hash mode value 'DF': Invalid Salt Length 'E0': Invalid Hash Option 'E1': Invalid Shared Information Flag 'E2': Invalid Number of SHS value 'E3': Invalid Key derivation Flag 'E4': Invalid number of keys specified 'E5': Invalid salt value 'E8': Invalid Shared Secret length 'E9': Invalid SHS value 'EA': ECC Curve not strong enough to derive keys 'EB': Invalid public key output format 'EC': Invalid Key Strength value in SHS or a standard error code </p>
If Error Code = 'D3' or 'D9', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
The following section will be repeated for the Number of Keys requested:		
Key	'S' + n B	The derived key, encrypted under the LMK.
Key Check Value	3 B or 6 B	The check value of the derived key.
Shared Information	n H	<p>Only present if Shared Information Flag is '1'. The randomly generated Shared Information used in the KDF.</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Key Derivation using ECKA-DH (Initiator: Create Ephemeral Keys)

Variant LMK <input checked="" type="checkbox"/>	AES Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not Required	

Function: This command creates the ephemeral ECC key pair required by the initiator in order to begin the Elliptic Curve Key Agreement / El-Gamal (ephemeral/ephemeral) method. The initiator and the recipient will each use an ephemeral ECC key pair.

Once generated, the initiator's ephemeral ECC public key should be shared with the recipient.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'IG'.
Mode	1 N	'0': Initiator: Start ECKA-DH
Agreement Type	1 N	'1': Ephemeral-Ephemeral (Diffie-Hellman)
Curve Reference	2 H	The ECC curve to be selected for generating the Initiator's ephemeral ECC Public Key. Valid values are: '00': FIPS 186-3 – NIST P-256 curve '01': FIPS 186-3 – NIST P-384 curve '02': FIPS 186-3 – NIST P-521 curve
Output Public Key Encoding	2 N	The format for the output Initiator's ephemeral ECC Public Key. Valid values are: '03': X9.62 ASN.1 format '04': Uncompressed encoding '05': ISO 7816 format
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details						
RESPONSE MESSAGE								
Message Header	m A	Returned to the Host unchanged.						
Response Code	2 A	Value 'IH'.						
Error Code	2 N	<p>'00': No error '01': SHS CMAC verification failed. '79': Invalid hash identifier 'A1': Invalid LMK scheme 'A5': Incompatible key length/algorithm combination 'B2': Bad end of keys delimiter 'D0': Invalid Mode 'D1': Invalid Agreement Type 'D2': Invalid curve reference 'D3': Invalid public key block 'D4': Invalid public key 'D5': Curve not supported 'D6': Invalid Public Key Input format 'D7': Invalid Public Key, does not conform to ASN1 encoding. 'D8': Invalid Public Key, does not conform to TLV format. 'D9': Private key block error 'DA': Invalid Shared Info length 'DB': Public key is not uncompressed format 'DD': Invalid KDF value 'DE': Invalid Single Hash mode value 'DF': Invalid Salt Length 'E0': Invalid Hash Option 'E1': Invalid Shared Information Flag 'E2': Invalid Number of SHS value 'E3': Invalid Key derivation Flag 'E4': Invalid number of keys specified 'E5': Invalid salt value 'E8': Invalid Shared Secret length 'E9': Invalid SHS value 'EA': ECC Curve not strong enough to derive keys 'EB': Invalid public key output format 'EC': Invalid Key Strength value in SHS or a standard error code </p>						
If Error Code = 'D3' or 'D9', the following field will be present:								
Additional Error Code	2 A	The key block specific error code.						
Public Key Length	4 N	The length (in bytes) of the following field.						
Ephemeral Public Key	n B	The Initiator's ephemeral ECC Public Key in Public Key Output Format.						
Ephemeral Private Key	'S' + n A	The Initiator's ephemeral ECC Private Key will be encrypted under the LMK, and conform to: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'03'</td> <td>'E'</td> <td>'X'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'03'	'E'	'X'
Key Usage	Algorithm	Mode of Use						
'03'	'E'	'X'						
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.						
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.						

Key Derivation using ECKA-DH (Recipient: Derive Shared Secret/Keys)

Variant LMK <input checked="" type="checkbox"/>	AES Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not Required	

Function: This command returns a shared secret or a set of shared keys using the Elliptic Curve Key Agreement / Diffie-Hellman (ephemeral/ephemeral) method. The initiator of the key agreement and the recipient will use a (unique) ephemeral ECC key pair.

Note: The host application is responsible for the authentication of the initiator's ephemeral ECC public key.

The recipient's shared secret is calculated by performing an ECC point multiplication of the initiator's ephemeral ECC public key and the recipient's ephemeral ECC private key.

The shared keys are optionally derived from the shared secret using a specified Key Derivation Function (KDF). Up to 99 shared symmetric (DES/AES/HMAC) keys may be derived from the shared secret(s).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'IG'.
Mode	1 N	'1': Recipient: Process ECKA-DH
Agreement Type	1 N	'1': Ephemeral-Ephemeral (Diffie-Hellman)
Public Key Encoding	2 N	The encoding of the Initiator's Public Key. Valid values are: '03': X9.62 ASN.1 format '04': Uncompressed encoding '05': ISO 7816 format
Curve Reference	2 H	Only present if Public Key Encoding = '04' or '05'. The ECC curve of the following Public Key. '00': FIPS 186-3 – NIST P-256 curve '01': FIPS 186-3 – NIST P-384 curve '02': FIPS 186-3 – NIST P-521 curve
Public Key Length	4 N	Only present if Public Key Encoding = '04'. The length of the following field.
Public Key	n B	The Initiator's ephemeral Public Key (For Public Key Encoding = '03', '04', '05', the raw public key is provided in the specified format.)
Output Public Key Encoding	2 N	The format for the output ephemeral ECC Public Key. Valid values are: '03': X9.62 ASN.1 format '04': Uncompressed encoding '05': ISO 7816 format
Key Derivation Flag	1 N	Indicates whether to perform the key derivation, or to output the Shared Secret. '0': Defer key derivation and output Shared Secret '1': Perform key derivation
If Key Derivation Flag = '1', the following section applies:		
KDF Method	1 N	Indicates the Key Derivation Function. Valid values are: '0': HKDF (RFC 5869) '1': Single Step KDF (NIST SP800-56A) '2': KDF (ANSI X9.63)
Hash Identifier	2 N	Identifier of the hash algorithm used in the KDF. Valid values are: '06': SHA-256
Single Hash Mode	1 N	Only present if KDF Method is '0'. Valid values are: '0': Include ephemeral public key in KDF.

Field	Length & Type	Details
Salt Length	2 N	Only present if KDF Method is '0'. The length of the following field. If a Salt value is not required, then the Salt Length should be set to '00'.
Salt	n H	Only present if KDF Method is '0'. The Salt value to be used in the KDF.
Delimiter	1 A	Only present if KDF Method is '0'. Value ';'.
Hash Option	1 N	Only present if KDF Method is '1'. Valid values are: '1': Use hash function ($H(x) = \text{hash}(x)$)
Shared Information Flag	1 N	Valid values are: '0': Use supplied Shared Information in KDF '1': Use random Shared Information in KDF
Shared Information Length	3 N	If Shared Information Flag = '0', this field specifies the length (in hex characters) of the following field. If Shared Information Flag = '1', this field specifies the required length (in bytes) of the randomly generated Shared Information. If not required, this field should be set to '000'.
Shared Information	n H	Only present if Shared Information Flag = '0'. The Shared Information between the two parties and used in the key derivation process. Example: if using "Thales" as the Shared Information, this would be presented as the following sequence of hex digits: 5468616C6573 and the Shared Information Length field should then contain 012 indicating a length of 12 hex digits. Note: When sharing this information with another system, ensure that the two systems use the same representation of the Shared Information – i.e. both systems must use hex-encoded ASCII or both systems must use a byte string.
Delimiter	1 A	Only present if Shared Information Flag = '0'. Value ';'.

Field	Length & Type	Details
Number of Keys	2 N	The number of symmetric keys to derive and output. Must be greater than '00'.
The following section will be repeated for the Number of Keys to be derived:		
Key Length	5 N	The key length in bits.
Key Usage	2 A	Key Usage field, to be included in the Key Block header. Any valid Thales Key Block Key Usage value is permitted, but it must be compatible with the following Algorithm and Mode of Use fields.
Algorithm	2 A	Algorithm and Key Length; the first character will be included in the algorithm field in the Key Block header (byte 7): <ul style="list-style-type: none"> • 'D1' – single length DES key • 'T2' – double length DES key • 'T3' – triple length DES key • 'A1' – 128-bit AES key • 'A2' – 192-bit AES key • 'A3' – 256-bit AES key • 'H0' – HMAC key
Mode of Use	1 A	Mode of Use field, to be included in the key block header. Any valid Thales Key Block Mode of Use value is permitted, but it must be compatible with the Key Usage and Algorithm fields specified above.
Key Version Number	2 N	Key Version Number field to be included in the key block header. Permitted values: '00' to '99'.
Exportability	1 A	Exportability field to be included in the key block header. Permitted values: 'N', 'E' or 'S'.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Block Identifier	2 A	Block Identifier; any permitted value except 'PB'.
Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Block Data	n A	The block data.
Delimiter	1 A	Value ';'. Denotes the end of a single key definition.
Delimiter	1 A	Value '>'. Denotes the end of all key definitions.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IH'.
Error Code	2 N	<p>'00': No error '01': SHS CMAC verification failed. '79': Invalid hash identifier 'A1': Invalid LMK scheme 'A5': Incompatible key length/algorithm combination 'B2': Bad end of keys delimiter 'D0': Invalid Mode 'D1': Invalid Agreement Type 'D2': Invalid curve reference 'D3': Invalid public key block 'D4': Invalid public key 'D5': Curve not supported 'D6': Invalid Public Key Input format 'D7': Invalid Public Key, does not conform to ASN1 encoding. 'D8': Invalid Public Key, does not conform to TLV format. 'D9': Private key block error 'DA': Invalid Shared Info length 'DB': Public key is not uncompressed format 'DD': Invalid KDF value 'DE': Invalid Single Hash mode value 'DF': Invalid Salt Length 'E0': Invalid Hash Option 'E1': Invalid Shared Information Flag 'E2': Invalid Number of SHS value 'E3': Invalid Key derivation Flag 'E4': Invalid number of keys specified 'E5': Invalid salt value 'E8': Invalid Shared Secret length 'E9': Invalid SHS value 'EA': ECC Curve not strong enough to derive keys 'EB': Invalid public key output format 'EC': Invalid Key Strength value in SHS or a standard error code </p>
If Error Code = 'D3' or 'D9', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
Public Key Length	4 N	The length (in bytes) of the following field.
Ephemeral Public Key	n B	The Recipient's ephemeral ECC Public Key in Public Key Output Format.
SHS Length	3 N	Only present if Key Derivation Flag is '0'. The length (in bytes) of the following field.
SHS	n B	Only present if Key Derivation Flag is '0'. The Shared Secret, encrypted under the LMK.
The following section will be repeated for the Number of Keys requested:		
Key	'S' + n B	The derived key, encrypted under the LMK.
Key Check Value	3 B or 6 B	The check value of the derived key.
Shared Information	n H	Only present if Shared Information Flag is '1'. The randomly generated Shared Information used in the KDF.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Key Derivation using ECKA-DH (Initiator: Derive Shared Keys)

Variant LMK <input checked="" type="checkbox"/>	AES Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not Required	

Function: This command returns a set of shared keys using the Elliptic Curve Key Agreement / Diffie-Hellman (ephemeral/ephemeral) method.

This command is called by the initiator of the key agreement process to (internally) derive a shared secret, and then to derive and return a set of shared keys.

The shared keys are derived from the shared secret using a specified Key Derivation Function (KDF). Up to 99 shared symmetric (DES/AES/HMAC) keys may be derived from the shared secret(s).

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IG'.						
Mode	1 N	'2': Initiator: Complete ECKA-DH						
Agreement Type	1 N	'1': Ephemeral-Ephemeral (Diffie-Hellman)						
Public Key Encoding	2 N	The encoding of the Recipient's Public Key. Valid values are: '03': X9.62 ASN.1 format '04': Uncompressed encoding '05': ISO 7816 format						
Curve Reference	2 H	Only present if Public Key Encoding = '04' or '05'. The ECC curve of the following Public Key. Valid values are: '00': FIPS 186-3 – NIST P-256 curve '01': FIPS 186-3 – NIST P-384 curve '02': FIPS 186-3 – NIST P-521 curve						
Public Key Length	4 N	Only present if Public Key Encoding = '04'. The length of the following field.						
Public Key	n B	The Recipient's ephemeral Public Key. For Public Key Encoding = '03', '04', '05', the raw public key is provided in the specified format.						
Private Key	'S' + n A	The Initiator's ephemeral Private Key (output from a previous call to IG with Mode = '0', Agreement Type = '1'), encrypted under the LMK, which must comply with:						
		<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'03'</td> <td>'E'</td> <td>'X'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'03'	'E'	'X'
Key Usage	Algorithm	Mode of Use						
'03'	'E'	'X'						
KDF Method	1 N	Indicates the Key Derivation Function. Valid values are: '0': HKDF (RFC 5869) '1': Single Step KDF (NIST SP800-56A) '2': KDF (ANSI X9.63)						
Hash Identifier	2 N	Identifier of the hash algorithm used in the KDF. Valid values are: '06': SHA-256						
KDF Public Key Encoding	2 N	Only present if KDF Method is '0'. The encoding of the following KDF Public Key. Valid values are: '03': X9.62 ASN.1 format '04': Uncompressed encoding '05': ISO 7816 format						
KDF Public Key Length	4 N	Only present if KDF Method is '0' and if KDF Public Key Encoding = '04'. The length of the following field.						
KDF Public Key	n B	Only present if KDF Method is '0'. The Initiator's Public Key to be used during the KDF process.						

Field	Length & Type	Details
Single Hash Mode	1 N	Only present if KDF Method is '0'. Valid values are: '0': Include ephemeral public key in KDF.
Salt Length	2 N	Only present if KDF Method is '0'. The length of the following field. If a Salt value is not required, then the Salt Length should be set to '00'.
Salt	n H	Only present if KDF Method is '0'. The Salt value to be used in the KDF.
Delimiter	1 A	Only present if KDF Method is '0'. Value ';'.
Hash Option	1 N	Only present if KDF Method is '1'. Valid values are: '1': Use hash function ($H(x) = \text{hash}(x)$)
Shared Information Flag	1 N	Valid values are: '0': Use supplied Shared Information in KDF '1': Use random Shared Information in KDF
Shared Information Length	3 N	If Shared Information Flag = '0', this field specifies the length (in hex characters) of the following field. If Shared Information Flag = '1', this field specifies the required length (in bytes) of the randomly generated Shared Information. If not required, this field should be set to '000'.
Shared Information	n H	Only present if Shared Information Flag = '0'. The Shared Information between the two parties and used in the key derivation process. Example: if using "Thales" as the Shared Information, this would be presented as the following sequence of hex digits: 5468616C6573 and the Shared Information Length field should then contain 012 indicating a length of 12 hex digits. Note: When sharing this information with another system, ensure that the two systems use the same representation of the Shared Information – i.e. both systems must use hex-encoded ASCII or both systems must use a byte string.
Delimiter	1 A	Only present if Shared Information Flag = '0'. Value ';'.

Field	Length & Type	Details
Number of Keys	2 N	The number of symmetric keys to derive and output. Must be greater than '00'.
The following section will be repeated for the Number of Keys to be derived:		
Key Length	5 N	The key length in bits.
Key Usage	2 A	Key Usage field, to be included in the Key Block header. Any valid Thales Key Block Key Usage value is permitted, but it must be compatible with the following Algorithm and Mode of Use fields.
Algorithm	2 A	Algorithm and Key Length; the first character will be included in the algorithm field in the Key Block header (byte 7): <ul style="list-style-type: none">• 'D1' – single length DES key• 'T2' – double length DES key• 'T3' – triple length DES key• 'A1' – 128-bit AES key• 'A2' – 192-bit AES key• 'A3' – 256-bit AES key• 'H0' – HMAC key
Mode of Use	1 A	Mode of Use field, to be included in the key block header. Any valid Thales Key Block Mode of Use value is permitted, but it must be compatible with the Key Usage and Algorithm fields specified above.
Key Version Number	2 N	Key Version Number field to be included in the key block header. Permitted values: '00' to '99'.
Exportability	1 A	Exportability field to be included in the key block header. Permitted values: 'N', 'E' or 'S'.
Number of Optional Blocks	2 N	Number of Optional Blocks specified below.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Block Identifier	2 A	Block Identifier; any permitted value except 'PB'.
Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Block Data	n A	The block data.
Delimiter	1 A	Value ';'. Denotes the end of a single key definition.
Delimiter	1 A	Value '!. Denotes the end of all key definitions.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IH'.
Error Code	2 N	'00': No error '01': SHS CMAC verification failed. '79': Invalid hash identifier 'A1': Invalid LMK scheme 'A5': Incompatible key length/algorithm combination 'B2': Bad end of keys delimiter 'D0': Invalid Mode 'D1': Invalid Agreement Type 'D2': Invalid curve reference 'D3': Invalid public key block 'D4': Invalid public key 'D5': Curve not supported 'D6': Invalid Public Key Input format 'D7': Invalid Public Key, does not conform to ASN1 encoding. 'D8': Invalid Public Key, does not conform to TLV format. 'D9': Private key block error 'DA': Invalid Shared Info length

Field	Length & Type	Details
		'DB': Public key is not uncompressed format 'DD': Invalid KDF value 'DE': Invalid Single Hash mode value 'DF': Invalid Salt Length 'E0': Invalid Hash Option 'E1': Invalid Shared Information Flag 'E2': Invalid Number of SHS value 'E3': Invalid Key derivation Flag 'E4': Invalid number of keys specified 'E5': Invalid salt value 'E8': Invalid Shared Secret length 'E9': Invalid SHS value 'EA': ECC Curve not strong enough to derive keys 'EB': Invalid public key output format 'EC': Invalid Key Strength value in SHS or a standard error code
If Error Code = 'D3' or 'D9', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
The following section will be repeated for the Number of Keys requested:		
Key	'S' + n B	The derived key, encrypted under the LMK.
Key Check Value	3 B or 6 B	The check value of the derived key.
Shared Information	n H	Only present if Shared Information Flag is '1'. The randomly generated Shared Information used in the KDF.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

TR-34 Key Export

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Determined by KTT(E)	
Activity: export. {key}.host	

Function: This command supports the export of a symmetric key using asymmetric techniques from a single Key Distribution Host (KDH) to many Key Receiving Device (KRD) as described in X9 TR-34:2019.

The following symmetric key types are supported:

- 112-bit / 168-bit DES key
- 128-bit / 192-bit / 256-bit AES key

Notes: For information about support for the RSA algorithm, see the *payShield 10K Host Programmer's manual*.

This command's ability to export AES keys is controlled by the following security setting:

Enforce PCI HSMv3 Key Equivalence for Key Wrapping: Yes or No

When set to Yes, the RSA key must have equivalent or greater strength than the Ephemeral Key and the Ephemeral Key must have equivalent or greater strength than the key being exported. Key strength is defined in NIST SP800-57.

Note that while the output TR-34 key block incorporates a TR-31 key block header, it does not include the full TR-31 key block, and so the length field of the TR-31 header will always be set to "0000".

When Scheme = '0', this command calculates the hash over the enveloped data excluding the sequence tag and length fields.

When Scheme = '1', this command calculates the hash over the enveloped data including the sequence tag and length fields.

When Scheme = '2', this is identical to Scheme = '1', but in the Response Message, the ASN.1 encoded `encryptedContent` element is a sibling of the `contentEncryptionAlgorithm` element instead of a child of the `content` element. This supports the update included in the ASC X9 TR 34-2019 Draft Errata (ASC X9 TR 34-2019 Corrigendum). All new applications should use Scheme = '2'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'B8'.
Scheme	1 N	Valid values are: '0': X9 TR-34:2019 (Enveloped Data hash excludes sequence tag & length fields) '1': X9 TR-34:2019 (Enveloped Data hash includes sequence tag & length fields) '2': X9 TR-34:2019 including Corrigendum (<code>encryptedContent</code> element is a sibling of the <code>contentEncryptionAlgorithm</code> element).
Key Type Code	3 H	Indicates the key type of the key to be exported. For a list of possible values, see <i>Available Key Types/Usages</i> . Note: The key For LMK Key Block this should be set to 'FFF'.
Key	32 H or 1 A + 32 H	The key for exporting from the KDH to KRD encrypted under the LMK according to Key Type. For Variant LMK, the Key is encrypted under LMK pair according to 'Key type'.

Field	Length & Type	Details						
	'S' + n A	<p>For Key Block LMK, the Key must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode Of Use</th></tr> <tr> <td>Any valid value</td><td>'D', 'T', 'A'</td><td>Any valid value</td></tr> </table> <p>The Key must have the exportable byte in the key block header as 'E' or 'S'</p>	Key Usage	Algorithm	Mode Of Use	Any valid value	'D', 'T', 'A'	Any valid value
Key Usage	Algorithm	Mode Of Use						
Any valid value	'D', 'T', 'A'	Any valid value						
The following section contains the CMS Enveloped Data fields								
KDH Credential	n B	<p>The BER encoded distinguished name and serial used to uniquely identify the KDH.</p> <p>KDH Credential ::= SEQUENCE { issuer Name, serialNumber CertificateSerialNumber }</p>						
Key Block Encryption Algorithm	2 N	<p>The cipher for encrypting the key block to create the encrypted key block (BE):</p> <p>'00': 192-bit TDES key – CBC '01': 128-bit AES key - CBC</p>						
Ephemeral Key Encryption Algorithm	2 N	<p>Identifier of algorithm used to encipher the ephemeral key:</p> <p>'00': RSA OAEP</p>						
The number of KRD recipients	2 N	<p>Valid values: '01'.</p>						
For each KRD recipient, the following 5 fields must be present:								
KRD Credential	n B	<p>The BER encoded distinguished name and serial number identifier used to uniquely identify the recipient KRD:</p> <p>KRD Credential ::= SEQUENCE { issuer Name, serialNumber CertificateSerialNumber }</p>						
If Ephemeral Key Encryption Algorithm = '00', the following fields must be present:								
KRD Public key	n B	<p>The BER encoded KRD's public key in ASN.1 format (sequence of modulus, exponent). Modulus length must be 2048 and exponent 65537.</p>						
OAEP Encoding Parameters Length	2 N	<p>Optional. If not required set to '00'.</p>						
OAEP Encoding Parameters	n B	<p>Optional, only present if OAEP Encoding Parameters Length is not '00'.</p>						
OAEP Encoding Parameters Delimiter	1 A	<p>Value ':'.</p> <p>Optional, only present if OAEP Encoding Parameters is present.</p>						

Field	Length & Type	Details						
The following section contains the CMS Signed Data Type fields.								
Private Key Flag	2 N	Flag to indicate location of the private key to decrypt the encrypted key: '00' ... '20': index of stored private key '99': use private key provided with command. The length of the KDH Private Key, if Private Key Flag is '99'.						
KDH Private Key Length	4 N	If Variant LMK, the length in bytes of the next field.						
	4 H	If Key Block LMK, this field should be set to 'FFFF'.						
KDH Private Key	n B	The private key of the KDH used to sign the key block.						
	'S' + n A	Must be present if the Private Key Flag = '99'. For Key Block LMK, the Private Key must comply with the following: <table border="1"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode Of Use</th></tr> <tr> <td>'03'</td><td>'R'</td><td>'S', 'D', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode Of Use	'03'	'R'	'S', 'D', 'N'
Key Usage	Algorithm	Mode Of Use						
'03'	'R'	'S', 'D', 'N'						
Signed Data Pad Mode	2 N	Valid values are: '01': PKCS#1 V1.5						
Signed Data Digest Algorithm	1 N	Valid values are: '0': SHA 256						
Time Stamp Delimiter	1 A	Value '<'. Optional; if present, the following field specifies the Time Stamp (and the RandomNonce is not supplied).						
Time Stamp	13 A	Must be present if the Time Stamp Delimiter is present. Format is UTC time as defined by RFC 5652, i.e. YYMMDDHHMMSSZ						
RandomNonce Length	2 N	Not present if Time Stamp Delimiter is present. The length of the RandomNonce						
RandomNonce	n B	If a RandomNonce is not required, this field should be set to '00'. Not present if Time Stamp Delimiter is present. The RandomNonce supplied by the KRD.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
When using a Variant LMK, the following fields apply:								
Delimiter	1 A	Value '&'. Optional; can only be present when exporting a key under variant LMK. If specified the following 5 or 9 fields will be present.						
Key Usage	2 A	Key Usage field, to be included in the TR-31 key block header (within the TR-34 exported key); any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Key Usage Table in the <i>payShield 10K Host Programmer's manual</i> .						
Mode Of Use	1 A	Mode of Use field, to be included in the TR-31 key block header (within the TR-34 exported key); any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .						
Key Version Number	2 N	Key Version Number field, to be included in the TR-31 key block header (within the TR-34 exported key); permitted values: '00' to '99'; must be present if the above Delimiter is present.						
Exportability	1 A	Exportability field, to be included in the TR-31 key block header (within the TR-34 exported key); must be present if the above Delimiter is present.						
Number of optional blocks	2 N	Number of Optional Blocks specified below, to be included in the TR-31 key block header (within the TR-34 exported key); permitted values '00' to '02'; must be present if the above Delimiter is present.						
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.								
Optional Block Identifier	2 A	Optional Block Identifier; to be included in the TR-31 key block header (within the TR-34 exported key); any permitted value except 'PB'.						
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); to be included in the TR-31 key block header (within the TR-34 exported key); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.						
Optional Block Data	n A	Optional block data; to be included in the TR-31 key block header (within the TR-34 exported key).						

Field	Length & Type	Details
Delimiter	1 A	Value '!'. Optional; if present, the following field must also be present
Key Block Version ID	1 A	The Key Block Version ID for the TR-31 key block header within the TR-34 key block: 'A': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'B': Key block protected using the Key Derivation Binding Method (see Ref 8 §5.3.2.1) 'C': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'D': Key block protected using the AES Key Derivation Binding Method (see Ref 8 §5.3.2.3).
When using a Key Block LMK, the following fields apply:		
Delimiter	1 A	Value '&'. Optional; can only be present when the exported key is in keyblock format; if present, the following field must also be present
Modified exportability	1 A	Exportability field, to be included in the key block header; only permitted value is "N"; must be present if the above Delimiter is present
Delimiter	1 A	Value '!'. Optional; if present, the following field must also be present
Key Block Version ID	1 A	The Key Block Version ID for the TR-31 key block header within the TR-34 key block: 'A': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'B': Key block protected using the Key Derivation Binding Method (see Ref 8 §5.3.2.1) 'C': Key block protected using the Key Variant Binding Method (see Ref 8 §5.3.3.1) 'D': Key block protected using the AES Key Derivation Binding Method (see Ref 8 §5.3.2.3).
Delimiter	1 A	Value '*'. Optional; if present, the following field is present.
Optional Key Usage	2 A	Value 'K0' or 'K1'. The Key Usage for the TR-31 key block header within the TR-34 key block (used when exporting a Thales Key Block with Key Usage '51', '52' or '54').
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'B9'.
Error Code	2 A	<p>'00': No error '04': Invalid Key Type Code 'D1': Invalid Scheme 'D3': Key error / PCI HSM V3 Key Equivalence criteria not met 'D4': Invalid number of recipients 'D5': KDH Credential does not conform to BER encoding rules 'D6': Invalid Key Block Algorithm 'D7': Invalid Ephemeral Key Encryption Algorithm 'D8': KRD Credential does not conform to BER encoding rules 'D9': KRD Public Key does not conform to BER encoding rules 'DA': Invalid KRD modulus length or exponent 'DB': Invalid OAEP Encoding Parameters Length 'DC': Invalid Private Key 'DD': Invalid Signed data Pad mode 'DE': Invalid Signed Data digest Algorithm 'DF': Invalid random nonce length 'E0': Invalid Key Block Version ID 'E1': Invalid Modified Exportability value or a standard error code.</p>
If Error Code is 'DC' or 'DD', the following field will be present:		
Additional Error Code	2 A	The key block specific error code
If Error Code is '00', the following fields will be present:		
Authenticated Attributes	n B	<p>The BER encoded string containing the attributes that were SHA256 hashed and then signed:</p> <ul style="list-style-type: none"> • The random nonce • The key block header • The digest computed over the enveloped data
KCV	3 B or 6 B	The KCV of the exported key
Enveloped Data	n B	The BER encoded Enveloped Data
Signature Length	4 N	The length in bytes of the Signature
Signature	n B	The Signature (or encryptedDigest) over the Authenticated Attributes
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

3.7 Bancontact Session Key Commands

Two host commands are provided to allow import and export of AES session keys in accordance with the specifications from Bancontact.

Function	Command	Page
<i>Import Bancontact Session Key</i>	N6 (N7)	251
<i>Export Bancontact Session Key</i>	N8 (N9)	256

Bancontact manages the standards for the Bancontact debit card used widely in Belgium. Bancontact specifies their own standards for key management and the host commands specified here are designed to support those standards. To meet the requirements, AES keys are required to be transferred between parties as specified by Bancontact. The keys are used for encryption of PINs, cardholder data and to generate and verify a MAC to protect the integrity of the messages.

To use these host commands, the specifications from Bancontact will be required for reference by the application developer. These provide details of the message format and keys.

Notes:

- The commands are designed to ensure key separation is maintained and the session keys can only be used for the purpose for which they are intended. For this reason the entire message protected by the MAC must be input into the import function, and the entire message protected by the MAC is output from the export function.
- To prevent the exported message being changed and the MAC on the message regenerated, the key used to generate the MAC is randomly generated in the export command. In addition the key used to generate the MAC is returned in the import command, if required, with the mode of use set to allow the key to be used for MAC verification only.
- Only the following algorithms are supported:

○ PIN encryption algorithm identifier:	04 AES 128 bits ECB/KeyWrap 05 AES 192 bits ECB/KeyWrap 06 AES 256 bits ECB/KeyWrap
○ Data encryption algorithm identifier:	04 AES 128 bits CBC/KeyWrap 05 AES 192 bits CBC/KeyWrap 06 AES 256 bits CBC/KeyWrap
○ MAC generation algorithm identifier:	04 AES 128 bits CMAC/KeyWrap 05 AES 192 bits CMAC/KeyWrap 06 AES 256 bits CMAC/KeyWrap
○ MAC Truncation:	01 Truncated left half MAC

- For the Session Key Export function, it is assumed that the following Session Keys are generated randomly using the A0 Host Command where required: ZPK, New PIN ZPK, ZEK. Note that the MAC Key is generated by the command.
- Support for derived session keys (i.e. where the ZPK, New PIN ZPK, ZEK and MAC Key) are derived from the ZMK (Master Key)) are currently not supported by the specification from Bancontact in 2018 and so are not supported in these functions.

- As only AES keys are supported, an AES Key Block LMK is required to be installed in order to use these commands.
- The message format is detailed in:
 - ISO 8583-1: 2003 Financial transaction card originated message – Interchange message specification – Part 1: Messages, data elements and code values. (Ref. 1)
 - Security Related BSP Extract, Bancontact. (Ref. 2).
- Only the format of the Security Field (P53) in the input message will be checked by these host commands. It is the responsibility of the application to ensure the format of the other aspects of the message are correct.
- The following table maps the terminology used in the payShield to that used by Bancontact:

payShield	Bancontact
ZMK (Zone Master Key)	Master Key
ZPK (Zone PIN Key)	PIN Session Key
New PIN ZPK (Zone PIN Key)	New PIN Session Key
ZEK (Zone Encryption Key)	Data Encryption (Session) Key
MAC Key (Message Authentication Code Key)	MAC (Session) Key

Import Bancontact Session Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: None	
Activity: None	

Function: This host command imports the AES session keys (ZPK, New PIN ZPK, ZEK and optionally the MAC Key) from a message complying with the Bancontact specification.

The message included in the MAC computation is input to the command together with an offset for the start of the Security Field P53. The MAC is verified. The session keys (if included) are decrypted from encryption under the relevant ZMK using the NIST SP800-38F standard and returned encrypted under the LMK.

Notes: The application must specify which session keys are required to be returned.

The same ZMK is assumed to be used to encrypt the ZPK and the New PIN ZPK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'N6'.
Scheme and Version	1 N	Valid values are: '0': Bancontact P53 Field Version 2018.
ZPK Flag	1 N	'0': Not required '1': Required
New PIN ZPK Flag	1 N	'0': Not required '1': Required
ZEK Flag	1 N	'0': Not required '1': Required
MAC Key Flag	1 N	'0': Not required '1': Required
ZMK for ZPK	'S' + n A	Only present when ZPK flag = 1 or New PIN ZPK = 1; The Zone Master Key for use with the ZPK and New PIN ZPK. For a Key Block LMK, the 'ZMK' must comply with the following:
ZMK for ZEK	'S' + n A	Only present when ZEK flag = 1; The Zone Master Key for use with the ZEK. For a Key Block LMK, the 'ZMK' must comply with the following:
ZMK for MAC Key	'S' + n A	The Zone Master Key for use with the MAC Key. Must be present whether MAC Key Flag is 0 or 1. For a Key Block LMK, the 'ZMK' must comply with the following:
MAC	8 B	Left half of the CMAC (64 bits) which is supplied in Field P128 of the Bancontact Message. The CMAC is calculated over the Input Message.
Security Field Offset	4 H	Offset to the first byte in the Message containing the Security Field – P53.

Field	Length & Type	Details
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes.
Message	n B	The message containing the Security Field (P53). This must be the message that is included in the MAC calculation only (i.e. it does not include transport header and does not include field P128). This should be in the format required by Bancontact and consists of fields in binary, numeric and alphanumeric formats as given in the Bancontact specification.
Delimiter	1 A	Value '#'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
Additional key block fields for importing a Zone PIN Key (ZPK)		
Delimiter	1 A	Value '#'; Only present when ZPK flag = 1; if present the following fields must be included;
Key Usage	2 A	Key Usage field, to be included in the key block header, must be present if the above Delimiter is present; permitted values: <ul style="list-style-type: none"> • 'P0' (PIN Encryption Key (Generic)) • '71' (Terminal PIN Encryption Key (TPK)) • '72' (Zone PIN Encryption Key (ZPK))
Mode of Use	1 A	Mode of Use field, to be included in the key block header; must be present if the above Delimiter is present; permitted values: <ul style="list-style-type: none"> • 'B' (Both encryption and decryption) • 'D' (Decrypt only) • 'E' (Encrypt only) • 'N' (No special restrictions apply)
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; must be present if the above Delimiter is present; permitted values: <ul style="list-style-type: none"> • 'E' (May only be exported in a trusted key block, provided the wrapping key itself is in a trusted format) • 'N' (No export permitted) • 'S' (Sensitive; all other export possibilities are permitted, provided such export has been enabled (existing Authorized State requirements remain)).
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
Additional key block fields for importing a New PIN Zone PIN Key (New PIN ZPK)		
Delimiter	1 A	Value '#'; Only present when New PIN ZPK flag = 1; if present the following fields must be included;

Field	Length & Type	Details
Key Usage	2 A	Key Usage field, to be included in the key block header, must be present if the above Delimiter is present; permitted values: <ul style="list-style-type: none">• 'P0' (PIN Encryption Key (Generic))• '71' (Terminal PIN Encryption Key (TPK))• '72' (Zone PIN Encryption Key (ZPK))
Mode of Use	1 A	Mode of Use field, to be included in the key block header; must be present if the above Delimiter is present; permitted values: <ul style="list-style-type: none">• 'B' (Both encryption and decryption)• 'D' (Decrypt only)• 'E' (Encrypt only)• 'N' (No special restrictions apply)
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; must be present if the above Delimiter is present; permitted values: <ul style="list-style-type: none">• 'E' (May only be exported in a trusted key block, provided the wrapping key itself is in a trusted format)• 'N' (No export permitted)• 'S' (Sensitive; all other export possibilities are permitted, provided such export has been enabled (existing Authorized State requirements remain)).
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
Additional key block fields for importing a Zone Encryption Key (ZEK)		
Delimiter	1 A	Value '#'; Only present when ZEK flag = 1; if present the following fields must be included;
Key Usage	2 A	Key Usage field, to be included in the key block header, must be present if the above Delimiter is present; permitted values: <ul style="list-style-type: none">• 'D0' (Data Encryption Key (Generic))• '21' (Data Encryption Key (DEK))• '22' (Data Encryption Key (ZEK))• '23' (Data Encryption Key (TEK))
Mode of Use	1 A	Mode of Use field, to be included in the key block header; must be present if the above Delimiter is present; permitted values: <ul style="list-style-type: none">• 'B' (Both encryption and decryption)• 'D' (Decrypt only)• 'E' (Encrypt only)• 'N' (No special restrictions apply)
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; must be present if the above Delimiter is present; permitted values: <ul style="list-style-type: none">• 'E' (May only be exported in a trusted key block, provided the wrapping key itself is in a trusted format)• 'N' (No export permitted)• 'S' (Sensitive; all other export possibilities are permitted, provided such export has been enabled (existing Authorized State requirements remain)).
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.

Field	Length & Type	Details
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
Additional key block fields for importing a Message Authentication Code Key (MAC Key)		
Delimiter	1 A	Value '#'; Only present when MAC Key flag = 1; if present the following fields must be included;
Key Usage	2 A	Key Usage field, to be included in the key block header, must be present if the above Delimiter is present; permitted values: <ul style="list-style-type: none">• 'M6' (AES CMAC)
Mode of Use	1 A	Mode of Use field, to be included in the key block header; must be present if the above Delimiter is present; permitted values: <ul style="list-style-type: none">• 'V' (Verify only)
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; must be present if the above Delimiter is present; permitted values: <ul style="list-style-type: none">• 'E' (May only be exported in a trusted key block, provided the wrapping key itself is in a trusted format)• 'N' (No export permitted)• 'S' (Sensitive; all other export possibilities are permitted, provided such export has been enabled (existing Authorized State requirements remain)).
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'N7'.
Error Code	2 A	<p>'00': No error '01': MAC verification failure '06': Message Length error '15': Invalid input data (invalid format, invalid characters, or not enough data provided) '85': Invalid Scheme and Version. '86': Invalid ZPK Flag. '87': Invalid New PIN ZPK flag. '88': Invalid ZEK Flag. '89': Invalid MAC Key Flag. '90': Invalid Security Field Offset. '91': Invalid P53 value, MAC Algorithm not supported '92': Invalid P53 value, MAC truncation not supported '93': Invalid P53 value, Invalid key material length '94': Invalid P53 value, Invalid combination of Algorithm and Key length '95': Key Decryption failure '96': Invalid P53 value, Security Format Code in P53 position 0 is not equal to 0. or a standard error code.</p> <p>Where more detailed information can be provided, the following extended error codes will be supplied in place of the command specific or standard error codes. In place of xx a command specific (listed above) or a standard error code will be provided:</p> <p>'C1XX': Problem with ZMK for ZPK 'C3XX': Problem with ZMK for ZEK 'C4XX': Problem with ZMK for MAC Key 'D1XX': Problem with ZPK data in P53 data 'D2XX': Problem with NEW PIN ZPK data in P53 data 'D3XX': Problem with ZEK data in P53 data 'D4XX': Problem with MAC data in P53 data 'E1XX': Problem with additional key block fields for ZPK 'E2XX': Problem with additional key block fields for NEW PIN ZPK 'E3XX': Problem with additional key block fields for ZEK 'E4XX': Problem with additional key block fields for MAC Key where XX is the standard error code for the key specified.</p>
ZPK (PIN Session Key)	'S' + n A	Only present if ZPK Flag = 1, the ZPK (PIN Session Key) encrypted under the LMK.
New PIN ZPK (New PIN Session Key)	'S' + n A	Only present if New PIN ZPK Flag = 1, the ZPK (New PIN Session Key) encrypted under the LMK.
ZEK (Data Encryption Key)	'S' + n A	Only present if ZEK Flag = 1, the ZEK (Data Encryption Key) encrypted under the LMK.
MAC Key	'S' + n A	Only present if MAC Key Flag = 1, the MAC Key (MAC Key), encrypted under the LMK to allow separate verification of the input message if required.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Export Bancontact Session Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: None	
Activity: None	

Function: This host command exports the AES session keys (ZPK, New PIN ZPK, ZEK and MAC Key) in a format complying with the specification from Bancontact.

The required keys, excluding the MAC key, are input into the command. The message included in the MAC computation is input to the command with the position for the encrypted keys required to be exported containing the characters specified in the notes below. In addition an offset for the start of the Security Field P53 is input into the command.

The required session keys are encrypted under the appropriate ZMK using the NIST SP800-38F standard, inserted into the message and the MAC on the message generated. The entire message with encrypted keys is returned to the application together with the MAC ready for export.

Notes: The input message supplied must contain the message included in the MAC computation complying with the Bancontact specification with position for the encrypted keys required to be exported containing the characters as follows:

- The position in the field for the required Session Keys and the MAC Key each contain n x 'K' (i.e. n x X'4B) with n depending on the key length as follows:
 - n = X'18 if AES key length is 128 bits
 - n = X'20 if AES key length is 192 bits
 - n = X'28 if AES key length is 256 bits

The MAC Key and the MAC are generated by the command.

Field	Length & Type	Details					
COMMAND MESSAGE							
Message Header	m A	Subsequently returned to the Host unchanged.					
Command Code	2 A	Value 'N8'.					
Scheme and Version	1 N	Valid values are: '0': Bancontact P53 Field Version 2018					
ZPK Flag	1 N	'0': Not present '1': Present					
New PIN ZPK Flag	1 N	'0': Not present '1': Present					
ZEK Flag	1 N	'0': Not present '1': Present					
ZMK for ZPK	'S' + n A	Only present when ZPK flag = 1 or New PIN ZPK Flag = 1; The Zone Master Key for use with the ZPK and New PIN ZPK.					
ZMK for ZEK		For a Key Block LMK, the 'ZMK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'K0', '52'</td> <td>'A'</td> <td>'B', 'E', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'K0', '52'	'A'
Key Usage	Algorithm	Mode of Use					
'K0', '52'	'A'	'B', 'E', 'N'					
	'S' + n A	Only present when ZEK flag = 1; The Zone Master Key for use with the ZEK.					
		For a Key Block LMK, the 'ZMK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'K0', '52'</td> <td>'A'</td> <td>'B', 'E', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'K0', '52'	'A'
Key Usage	Algorithm	Mode of Use					
'K0', '52'	'A'	'B', 'E', 'N'					

Field	Length & Type	Details						
ZMK for MAC Key	'S' + n A	The Zone Master Key for use with the MAC Key. For a Key Block LMK, the 'ZMK' must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'K0', '52'</td><td>'A'</td><td>'B', 'E', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'K0', '52'	'A'	'B', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'K0', '52'	'A'	'B', 'E', 'N'						
ZPK (PIN Session Key)	'S' + n A	Only present if ZPK Flag = 1. The ZPK (PIN Session Key) encrypted under the LMK. For Key Block LMK, the key must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode Of Use</th></tr> </thead> <tbody> <tr> <td>'P0', '71', '72'</td><td>'A'</td><td>'B', 'D', 'E', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode Of Use	'P0', '71', '72'	'A'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode Of Use						
'P0', '71', '72'	'A'	'B', 'D', 'E', 'N'						
New PIN ZPK (New PIN Session Key)	'S' + n A	The key must have the Exportability byte in the key block header as 'E' or 'S' Only present if New PIN ZPK Flag = 1. The New PIN ZPK (New PIN Session Key) encrypted under the LMK. For Key Block LMK, the key must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode Of Use</th></tr> </thead> <tbody> <tr> <td>'P0', '71', '72'</td><td>'A'</td><td>'B', 'D', 'E', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode Of Use	'P0', '71', '72'	'A'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode Of Use						
'P0', '71', '72'	'A'	'B', 'D', 'E', 'N'						
ZEK (Data Encryption Key)	'S' + n A	The key must have the Exportability byte in the key block header as 'E' or 'S' Only present if ZEK Flag = 1. The ZEK (Data Encryption Key) encrypted under the LMK. For Key Block LMK, the key must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode Of Use</th></tr> </thead> <tbody> <tr> <td>'D0', '21', '22', '23'</td><td>'A'</td><td>'B', 'D', 'E', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode Of Use	'D0', '21', '22', '23'	'A'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode Of Use						
'D0', '21', '22', '23'	'A'	'B', 'D', 'E', 'N'						
Security Field Offset	4 H	The key must have the Exportability byte in the key block header as 'E' or 'S' Offset to the first byte in the Message containing the Security Field – P53.						
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes.						
Message	n B	The message in which the session key(s) are to be inserted (if required) and the MAC to be generated (note it does not include transport header and does not include field P128). This should be in the format required by Bancontact and consists of fields in binary, numeric and alphanumeric formats as given in the Bancontact specification. <ul style="list-style-type: none"> The position in the field for the required Session Keys and the MAC Key must each contain n x 'K' (i.e. n x X'4B) with n depending on the key length as follows: <ul style="list-style-type: none"> n = X'18 if AES key length is 128 bits n = X'20 if AES key length is 192 bits n = X'28 if AES key length is 256 bits 						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'N9'.
Error Code	2 A	<p>'00': No error '01': MAC verification failure '06': Message Length error '15': Invalid input data (invalid format, invalid characters, or not enough data provided) '85': Invalid Scheme and Version. '86': Invalid ZPK Flag. '87': Invalid New PIN ZPK flag. '88': Invalid ZEK Flag. '89': Invalid MAC Key Flag. '90': Invalid Security Field Offset. '91': Invalid P53 value, MAC Algorithm not supported '92': Invalid P53 value, MAC truncation not supported '93': Invalid P53 value, Invalid key material length '94': Invalid P53 value, Invalid combination of Algorithm and Key length '95': Key Decryption failure '96': Invalid P53 value, Security Format Code in P53 position 0 is not equal to 0 or a standard error code.</p> <p>Where more detailed information can be provided, the following extended error codes will be supplied in place of the command specific or standard error codes. In place of xx a command specific (listed above) or a standard error code will be provided:</p> <p>'C1XX': Problem with ZMK for ZPK 'C3XX': Problem with ZMK for ZEK 'C4XX': Problem with ZMK for MAC Key where XX is the standard error code for the key specified.</p>
MAC	8 B	Left half of the CMAC (64 bits) which is calculated over the message with keys inserted as required. This is for insertion into Field P128 of the Bancontact Message.
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes.
Message	n B	The message with the session key(s) inserted as required.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

4 Magnetic Stripe Issuing Commands

4.1 PIN and Offset Generation Commands

The payShield 10K provides support for many PIN verification techniques. The techniques often involve the generation of a PIN using a given algorithm, or an algorithm that requires a value known as an offset.

The commands EE, GA, JA, BK and FW are capable of rejecting newly generated/derived or customer-selected PINs which are determined to be 'weak' (i.e. PINs that are considered easily guessed by someone other than the legitimate cardholder). PINs can be determined to be weak using three methods, each of which can be individually enabled/disabled via the Security Settings:

- By checking the PIN against a global list of excluded PINs, loaded into the HSM using the 'Load the Excluded PIN Table' host command (BM).
- By checking the PIN against a local list of excluded PINs – the local list is supplied with the host command generating or deriving the new PIN.
- By checking the PIN against a set of rules to determine its strength. A PIN is considered weak if any of the following are TRUE:
 - >50% of the PIN's digits have the same value. (e.g. 1111, 0222, 3301, etc.);
 - the PIN consists entirely of ascending or descending digits (e.g. 1234, 2345, etc.).

The payShield 10K provides the following host commands to support PIN/Offset generation:

Function	Command	Page
<i>Derive a PIN and Optionally Generate Offset for New PVK Using the IBM Offset Method</i>	EE (EF)	260
<i>Derive a PIN Using the Diebold Method</i>	GA (GB)	263
<i>Generate a Random PIN</i>	JA (JB)	265
<i>Generate an IBM PIN Offset (of an LMK encrypted PIN)</i>	DE (DF)	267
<i>Generate an IBM PIN Offset (of a customer selected PIN)</i>	BK (BL)	270
<i>Generate a Diebold PIN Offset</i>	CE (CF)	273
<i>Generate an ABA PVV (of an LMK encrypted PIN)</i>	DG (DH)	275
<i>Generate an ABA PVV (of a customer selected PIN)</i>	FW (FX)	277
<i>Load the Excluded PIN Table</i>	BM (BN)	280

Derive a PIN and Optionally Generate Offset for New PVK Using the IBM Offset Method

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate a 4 to 12-digit PIN using the IBM offset method.

Notes: If an offset is included, the PIN is derived from the offset in addition to the other data.

If no offset is included, it can be generated by the IBM PIN offset generation command as detailed in '*Generate an IBM PIN Offset (of an LMK encrypted PIN)*' (DE).

The decimalization table can be stored in user storage and referenced in the same way as keys.

The use of encrypted decimalization tables is strongly recommended. By default the HSM is configured to expect encrypted decimalization tables in PIN commands that use the IBM offset method. For backward compatibility the HSM may be configured to use plaintext decimalization tables using Configure Security.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues, deriving the PIN using 3DES in place of DES. (Double-length PVKs are now acceptable, but the returned error code has not been changed to allow for backward compatibility with existing Host applications which are expecting Error Code 02 to be returned.)

This command will optionally check the input PIN in order to exclude 'weak' PINs.

Note that when using a 3DES LMK, the LMK-encrypted PIN is not simply the PIN encrypted under the LMK. It is effectively an LMK-encrypted proprietary format PIN Block, where the PIN is cryptographically associated with the account number.

When using an AES Key Block LMK, the LMK-encrypted PIN is the result of encrypting the PIN under the LMK using Thales PIN Block format 48 (ISO PIN Block format 4).

Caution: The behavior of this command is affected by the following CS (Configure Security) console command settings:

Decimalization Table: Encrypted/Plaintext [E/P]

- When set to 'E' (the default setting), the supplied decimalization table must be encrypted (using console command ED), and will consist of 16 hexadecimal digits (for a Variant or 3DES Key Block LMK) or 'L' + 32 hexadecimal digits (for an AES Key Block LMK).
- When set to 'P', the supplied decimalization table must be plaintext, and will consist of 16 decimal digits.

Decimalization Table checks enabled? [Yes/No]

- When set to 'Yes' (the default setting), the decimalization table must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, error code 25 is returned.
- When set to 'No', the decimalization table is not checked.

Enable Weak PIN checking? [Yes/No]

Check new PINs using global list of weak PINs: [Yes/No]

Check new PINs using local list of weak PINs: [Yes/No]

Check new PINs using rules: [Yes/No]

- Refer to the payShield 10K Security Operations manual for full details on how these settings can prevent the generation of 'weak' PINs.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'EE'.						
PVK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The PIN Verification Key, used to generate the derived PIN.</p> <p>For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.</p> <p>For a Key Block LMK, the 'PVK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'V1'</td><td>'D', 'T'</td><td>'C', 'G', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'V1'	'D', 'T'	'C', 'G', 'N'
Key Usage	Algorithm	Mode of Use						
'V1'	'D', 'T'	'C', 'G', 'N'						
Delimiter	1 A	Value '#'. Optional; if present, the "New PVK" field must also be present.						
New PVK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The PIN Verification Key, used to migrate the PIN offset.</p> <p>For a Variant LMK, the 'New PVK' must be encrypted under LMK pair 14-15 variant 0.</p> <p>For a Key Block LMK, the 'New PVK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'V1'</td><td>'D', 'T'</td><td>'C', 'G', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'V1'	'D', 'T'	'C', 'G', 'N'
Key Usage	Algorithm	Mode of Use						
'V1'	'D', 'T'	'C', 'G', 'N'						
Offset	12 H	Value 'oo..oFF..F'. This field contains the offset (if there is one), left-justified and padded with 'F's.						
Check Length	2 N	The minimum PIN length.						
Primary Account Number (PAN)	12 N or n N	<p>If a 3DES Key Block or Variant LMK is used: The 12 right-most digits of the PAN, excluding the check digit.</p> <p>If an AES Key Block LMK is used: The full 12-19 digit PAN, including the check digit.</p> <p>If present, the delimiter below must also be present.</p>						
Delimiter	1 A	Value ';'. Only present if an AES Key Block LMK is used.						
Decimalization Table	16 N or 16 H or 'K' + 3 H or 'L' + 32 H	<p>16 N when using Plaintext decimalization tables.</p> <p>16 H when using Encrypted decimalization tables and a Variant LMK or 3DES Key Block LMK.</p> <p>'K' + 3 H when referencing a decimalization table held in the HSM's User Storage Area.</p> <p>'L' + 32 H when using Encrypted decimalization tables and an AES Key Block LMK.</p>						

Field	Length & Type	Details
PIN Validation Data	12 A or 'P' + 16 H	User-defined data consisting of hexadecimal characters and the character 'N', which indicates to the HSM where to insert the last 5 digits of the PAN; or User-defined data consisting of the ASCII character 'P' followed by 16 hexadecimal digits which will be used as input to the PIN generation algorithm.
Delimiter	1 A	Value '*'.
Excluded PIN Count	2 N	'00' ... '99': The number of excluded PINs listed in the following local Excluded PIN Table.
Excluded PIN Length	2 N	'04' ... '12': The length of each excluded PIN in the following local Excluded PIN Table. Only present if the Excluded PIN Count > '00'.
Excluded PIN Table	n N	A local list of PINs to be excluded. The length of this field will be Excluded PIN Count multiplied by Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'EF'.
Error Code	2 A	'00': No error '02': Warning: PVK not single length '06': Invalid offset length '10': PVK parity error '68': Command disabled '81': PIN length mismatch '86': PIN is determined to be 'weak' or a standard error code.
PIN	L N or L H or 'M' + 32 H	The derived PIN encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
New Offset	12 H	The new offset value; left-justified and padded with 'F's. Only present if the 'New PVK' field was present in the request.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Derive a PIN Using the Diebold Method

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Derive a PIN using the Diebold method.

Notes: The Diebold table must be stored in user storage before using this command.

This command will optionally check the input PIN in order to exclude 'weak' PINs.

Note that when using a 3DES LMK, the LMK-encrypted PIN is not simply the PIN encrypted under the LMK. It is effectively an LMK-encrypted proprietary format PIN Block, where the PIN is cryptographically associated with the account number.

When using an AES Key Block LMK, the LMK-encrypted PIN is the result of encrypting the PIN under the LMK using Thales PIN Block format 48 (ISO PIN Block format 4).

Caution: The behavior of this command is affected by the following CS (Configure Security) console command settings:

Enforce key type 002 separation for PCI HSM compliance? [Yes/No]

- When set to 'Yes', the Diebold table is encrypted using LMK pair 14-15 variant 0.
- When set to 'No', the Diebold table is encrypted using LMK pair 36-37 variant 6.

Enable Weak PIN checking? [Yes/No]

Check new PINs using global list of weak PINs: [Yes/No]

Check new PINs using local list of weak PINs: [Yes/No]

Check new PINs using rules: [Yes/No]

- Refer to the payShield 10K Security Operations manual for full details on how these settings can prevent the generation of 'weak' PINs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'GA'.
Index Flag	1 A	Value 'K'.
Table Pointer	3 H	The value of the base location of the Diebold table.
Algorithm Number	2 H	The number of the Diebold algorithm required.
Offset	4 N	For a derived PIN, this is '0000'. Otherwise, an offset can be used.
Primary Account Number (PAN)	12 N or n N	If a 3DES Key Block or Variant LMK is used: The 12 right-most digits of the PAN, excluding the check digit. If an AES Key Block LMK is used: The full 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.
Delimiter	1 A	Value ';'. Only present if an AES Key Block LMK is used.
PIN Validation Data	16 A	User-defined data consisting of hexadecimal characters and the character 'N', which indicates to the HSM where to insert the last 5 digits of the PAN. The data must be right-justified and padded with 'F's.

payShield 10K Core Host Commands

Delimiter	1 A	Value '*'. Only present if the following Excluded PIN fields are present.
Excluded PIN Count	2 N	'00' ... '99': The number of excluded PINs listed in the following local Excluded PIN Table.
Excluded PIN Length	2 N	'04' ... '12': The length of each excluded PIN in the following local Excluded PIN Table. Only present if the Excluded PIN Count > '00'.
Excluded PIN Table	n N	A local list of PINs to be excluded. The length of this field will be Excluded PIN Count multiplied by Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'GB'.
Error Code	2 A	'00': No error '68': Command disabled '81': PIN length mismatch '86': PIN is determined to be 'weak' or a standard error code.
PIN	L N or L H or 'M' + 32 H	The derived PIN encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a Random PIN

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate a random PIN of 4 to 12 digits.

Notes: If the PIN length is not defined, a PIN of four digits is generated.

The PIN length selected must not exceed the value selected in the CS (Configure Security) console command.

This command will optionally ensure that the generated PIN is not a 'weak' PIN.

Note that when using a 3DES LMK, the LMK-encrypted PIN is not simply the PIN encrypted under the LMK. It is effectively an LMK-encrypted proprietary format PIN Block, where the PIN is cryptographically associated with the account number.

When using an AES Key Block LMK, the LMK-encrypted PIN is the result of encrypting the PIN under the LMK using Thales PIN Block format 48 (ISO PIN Block format 4).

Caution: The behavior of this command is affected by the following CS (Configure Security) console command setting:

Enable Weak PIN checking? [Yes/No]

Check new PINs using global list of weak PINs: [Yes/No]

Check new PINs using local list of weak PINs: [Yes/No]

Check new PINs using rules: [Yes/No]

- Refer to the payShield 10K Security Operations manual for full details on how these settings can prevent the generation of 'weak' PINs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'JA'.
Primary Account Number (PAN)	12 N or n N	If a 3DES Key Block or Variant LMK is used: The 12 right-most digits of the PAN, excluding the check digit. If an AES Key Block LMK is used: The full 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.
Delimiter	1 A	Value ';'. Only present if an AES Key Block LMK is used.

payShield 10K Core Host Commands

PIN Length	2 N	Optional. In the range 04 to 12. If not present, a PIN of 4 digits is generated.
Delimiter	1 A	Value '*'.
Excluded PIN Count	2 N	Only present if the following Excluded PIN fields are present. '00' ... '99': The number of excluded PINs listed in the following local Excluded PIN Table.
Excluded PIN Length	2 N	'04' ... '12': The length of each excluded PIN in the following local Excluded PIN Table.
Excluded PIN Table	n N	Only present if the Excluded PIN Count > '00'. A local list of PINs to be excluded. The length of this field will be Excluded PIN Count multiplied by Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'JB'.
Error Code	2 A	'00': No error '68': Command disabled '81': PIN length mismatch or a standard error code.
PIN	L N or L H or 'M' + 32 H	The new PIN encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate an IBM PIN Offset (of an LMK encrypted PIN)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate a PIN offset using the IBM 3624 method. The PIN (for which an offset is required) is supplied encrypted under the LMK.

Notes: The decimalization table can be stored in user storage and referenced in the same way as keys.

The use of encrypted decimalization tables is strongly recommended. By default the HSM is configured to expect encrypted decimalization tables in PIN commands that use the IBM offset method. For backward compatibility the HSM may be configured to use plaintext decimalization tables using Configure Security.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues generating the offset using 3DES in place of DES. (Double-length PVKs are now acceptable, but the returned error code has not been changed to allow for backward compatibility with existing Host applications which are expecting Error Code 02 to be returned.)

Note that when using a 3DES LMK, the LMK-encrypted PIN is not simply the PIN encrypted under the LMK. It is effectively an LMK-encrypted proprietary format PIN Block, where the PIN is cryptographically associated with the account number.

When using an AES Key Block LMK, the LMK-encrypted PIN is the result of encrypting the PIN under the LMK using Thales PIN Block format 48 (ISO PIN Block format 4).

Caution: The behavior of this command is affected by the following CS (Configure Security) console command settings:

Decimalization Table: Encrypted/Plaintext [E/P]

- When set to 'E' (the default setting), the supplied decimalization table must be encrypted (using console command ED), and will consist of 16 hexadecimal digits (for a Variant or 3DES Key Block LMK) or 'L' + 32 hexadecimal digits (for an AES Key Block LMK).
- When set to 'P', the supplied decimalization table must be plaintext, and will consist of 16 decimal digits.

Decimalization Table checks enabled? [Yes/No]

- When set to 'Yes' (the default setting), the decimalization table must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, error code 25 is returned.
- When set to 'No', the decimalization table is not checked.

Enable support for variable length PIN offset? [Yes/No]

- When set to 'No' (the default setting), the length of the generated Offset is determined by the value of the Check Length parameter. This setting makes the command backward compatible with previous versions of software.
- When set to 'Yes', the length of the generated Offset matches the length of the input PIN.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'DE'.						
PVK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The PIN Verification Key, used to generate the offset. For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0. For a Key Block LMK, the 'PVK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'V1'</td><td>'D', 'T'</td><td>'C', 'G', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'V1'	'D', 'T'	'C', 'G', 'N'
Key Usage	Algorithm	Mode of Use						
'V1'	'D', 'T'	'C', 'G', 'N'						
PIN	L N or L H or 'M' + 32 H	The PIN for which an offset is required, encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.						
Check Length	2 N	The minimum PIN length.						
Primary Account Number (PAN)	12 N or n N	If a 3DES Key Block or Variant LMK is used: The 12 right-most digits of the PAN, excluding the check digit. If an AES Key Block LMK is used: The full 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.						
Delimiter	1 A	Value ';'. Only present if an AES Key Block LMK is used.						
Decimalization Table	16 N or 16 H or 'K' + 3 H or 'L' + 32 H	16 N when using Plaintext decimalization tables. 16 H when using Encrypted decimalization tables and a Variant LMK or 3DES Key Block LMK. 'K' + 3 H when referencing a decimalization table held in the HSM's User Storage Area 'L' + 32 H when using Encrypted decimalization tables and an AES Key Block LMK.						
PIN Validation Data	12 A or 'P' + 16 H	User-defined data consisting of hexadecimal characters and the character 'N', which indicates to the HSM where to insert the last 5 digits of the PAN; or User-defined data consisting of the ASCII character 'P' followed by 16 hexadecimal digits which will be used as input to the PIN generation algorithm.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'DF'.
Error Code	2 A	'00': No error '02': Warning: PVK not single length '10': PVK parity error '68': Command disabled '81': PIN length mismatch or a standard error code.
Offset	12 H	The resulting offset value; left-justified and padded with 'F's.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate an IBM PIN Offset (of a customer selected PIN)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate a PIN offset using the IBM 3624 method. The PIN (for which an offset is required) is supplied in an encrypted PIN Block.

Notes: The decimalization table can be stored in user storage and referenced in the same way as keys.

The use of encrypted decimalization tables is strongly recommended. By default the HSM is configured to expect encrypted decimalization tables in PIN commands that use the IBM offset method. For backward compatibility the HSM may be configured to use plaintext decimalization tables using Configure Security.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues generating the offset using 3DES in place of DES. (Double-length PVKs are now acceptable, but the returned error code has not been changed to allow for backward compatibility with existing Host applications which are expecting Error Code 02 to be returned.)

This command will optionally check the input PIN in order to exclude 'weak' PINs.

Caution: The behavior of this command is affected by the following CS (Configure Security) console command settings:

Decimalization Table: Encrypted/Plaintext [E/P]

- When set to 'E' (the default setting), the supplied decimalization table must be encrypted (using console command ED), and will consist of 16 hexadecimal digits (for a Variant or 3DES Key Block LMK) or 'L' + 32 hexadecimal digits (for an AES Key Block LMK).
- When set to 'P', the supplied decimalization table must be plaintext, and will consist of 16 decimal digits.

Decimalization Table checks enabled? [Yes/No]

- When set to 'Yes' (the default setting), the decimalization table must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, error code 25 is returned.
- When set to 'No', the decimalization table is not checked.

Enable support for variable length PIN offset? [Yes/No]

- When set to 'No' (the default setting), the length of the generated Offset is determined by the value of the Check Length parameter. This setting makes the command backward compatible with previous versions of software.
- When set to 'Yes', the length of the generated Offset matches the length of the input PIN.

Enable Weak PIN checking? [Yes/No]

Check new PINs using global list of weak PINs: [Yes/No]

Check new PINs using local list of weak PINs: [Yes/No]

Check new PINs using rules: [Yes/No]

- Refer to the payShield 10K Security Operations manual for full details on how these settings can prevent the generation of 'weak' PINs.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'BK'.						
PIN Block Key Type	3 H	<p>For a Variant LMK:</p> <p>Type of PIN Block Key. The following key types are permitted if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N":</p> <p>'001': ZPK (encrypted under LMK 06-07 variant 0) '002': TPK (encrypted under LMK 14-15 variant 0)</p> <p>The following key types are permitted if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y":</p> <p>'001': ZPK (encrypted under LMK 06-07 variant 0) '70D': TPK (encrypted under LMK 36-37 variant 7)</p>						
PIN Block Key	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>For a Key Block LMK:</p> <p>This field is ignored; should be set to 'FFF'.</p> <p>The Key under which the PIN blocks are encrypted.</p> <p>For a Variant LMK, the 'PIN Block Key' is either a ZPK or TPK, as specified above.</p> <p>For a Key Block LMK, the 'PIN Block Key' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'P0', '71', '72'</td><td>'D', 'T', 'A'</td><td>'B', 'D', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'P0', '71', '72'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '71', '72'	'D', 'T', 'A'	'B', 'D', 'N'						
PVK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The PIN Verification Key, used to generate the offset.</p> <p>For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.</p> <p>For a Key Block LMK, the 'PVK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'V1'</td><td>'D', 'T'</td><td>'C', 'G', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'V1'	'D', 'T'	'C', 'G', 'N'
Key Usage	Algorithm	Mode of Use						
'V1'	'D', 'T'	'C', 'G', 'N'						
PIN Block	16 H or 32 H	The PIN, for which an offset is required, encrypted under the PIN Block Key. When using a DES PIN Block Key, this field will be 16 H. When using an AES PIN Block Key, this field will be 32 H.						
PIN Block Format Code	2 N	<p>One of the valid PIN block format codes.</p> <p>If the security setting "Restrict PIN block usage for PCI HSM compliance" has the value "Y" then the PIN Block Format must be one of:</p> <p>'01': (ISO 9564 / ANSI X9.8 Format 0) '47': (ISO 9564 / ANSI X9.8 Format 3) '48': (ISO 9564 / ANSI X9.8 Format 4)</p>						
Check Length	2 N	The minimum PIN length.						

payShield 10K Core Host Commands

Primary Account Number (PAN)	n N or 18 H or 12 N	The PAN, used to form the PIN Block. If 'PIN Block Format Code' = '48': The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present. If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.
Delimiter	1 A	Value ';'. Only present if 'PIN Block Format Code' = '48'.
Decimalization Table	16 N or 16 H or 'K' + 3 H or 'L' + 32 H	16 N when using Plaintext decimalization tables. 16 H when using Encrypted decimalization tables and a Variant LMK or 3DES Key Block LMK. 'K' + 3 H to reference a table held in the payShield 10K User Storage Area. 'L' + 32 H when using Encrypted decimalization tables and an AES Key Block LMK.
PIN Validation Data	12 A or 'P' + 16 H	User-defined data consisting of hexadecimal characters and the character 'N', which indicates to the HSM where to insert the last 5 digits of the PAN; or User-defined data consisting of the ASCII character 'P' followed by 16 hexadecimal digits which will be used as input to the PIN generation algorithm.
Delimiter	1 A	Value '*'.
Excluded PIN Count	2 N	‘00’ ... ‘99’: The number of excluded PINs listed in the following local Excluded PIN Table.
Excluded PIN Length	2 N	‘04’ ... ‘12’: The length of each excluded PIN in the following local Excluded PIN Table.
Excluded PIN Table	n N	Only present if the Excluded PIN Count > ‘00’. A local list of PINs to be excluded. The length of this field will be Excluded PIN Count multiplied by Excluded PIN Length characters. Only present if the Excluded PIN Count > ‘00’.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = ‘00’; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X‘19’.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'BL'.
Error Code	2 A	‘00’: No error ‘02’: Warning: PVK not single length ‘03’: Excluded PIN count incorrect ‘10’: TPK or ZPK parity error ‘11’: PVK parity error ‘68’: Command disabled ‘69’: PIN Block format has been disabled ‘81’: PIN length mismatch ‘86’: PIN is determined to be ‘weak’ or a standard error code.
PIN Offset	12 H	The resulting offset value; left-justified and padded with 'F's.
End Message Delimiter	1 C	Present only if present in the command message. Value X‘19’.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a Diebold PIN Offset

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate a PIN offset using the Diebold method.

Notes: Requires the Diebold table to be in user storage.

Note that when using a 3DES LMK, the LMK-encrypted PIN is not simply the PIN encrypted under the LMK. It is effectively an LMK-encrypted proprietary format PIN Block, where the PIN is cryptographically associated with the account number.

When using an AES Key Block LMK, the LMK-encrypted PIN is the result of encrypting the PIN under the LMK using Thales PIN Block format 48 (ISO PIN Block format 4).

Caution: The behavior of this command is affected by the following CS (Configure Security) console command settings:

Enforce key type 002 separation for PCI HSM compliance? [Yes/No]

- When set to 'Yes', the Diebold table is encrypted using LMK pair 14-15 variant 0.
- When set to 'No', the Diebold table is encrypted using LMK pair 36-37 variant 6.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'CE'.
Index Flag	1 A	Value 'K'.
Table Pointer	3 H	The value of the base location of the Diebold table in user storage.
Algorithm Number	2 H	The number of the Diebold algorithm required.
PIN	L N or L H or 'M' + 32 H	The PIN encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
Primary Account Number (PAN)	12 N or n N	If a 3DES Key Block or Variant LMK is used: The 12 right-most digits of the PAN, excluding the check digit. If an AES Key Block LMK is used: The full 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.
Delimiter	1 A	Value ';'. Only present if an AES Key Block LMK is used.
PIN Validation Data	16 A	User-defined data consisting of hexadecimal characters and the character 'N', which indicates to the HSM where to insert the last 5 digits of the PAN. The data must be right-justified and padded with 'F's.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'CF'.
Error Code	2 A	'00': No error '14': Encrypted PIN error '68': Command disabled '81': PIN length mismatch or a standard error code.
PIN Offset	4 N	The resulting Diebold offset.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate an ABA PVV (of an LMK encrypted PIN)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate a 4-digit PVV using the ABA method. The PIN (for which a PVV is required) is supplied encrypted under the LMK.

Notes: Visa defines the PIN Verification Key Indicator (PVKI) to be between 0 and 6. The HSM does not enforce this restriction.

Note that when using a 3DES LMK, the LMK-encrypted PIN is not simply the PIN encrypted under the LMK. It is effectively an LMK-encrypted proprietary format PIN Block, where the PIN is cryptographically associated with the account number.

When using an AES Key Block LMK, the LMK-encrypted PIN is the result of encrypting the PIN under the LMK using Thales PIN Block format 48 (ISO PIN Block format 4).

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'DG'.						
PVK	32 H or 'U' + 32 H or 'S' + n A	<p>The PVK, used to generate the PVV.</p> <p>For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.</p> <p>For a Key Block LMK, the 'PVK' is a double-length key, and must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'V2'</td><td>'T'</td><td>'C', 'G', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'V2'	'T'	'C', 'G', 'N'
Key Usage	Algorithm	Mode of Use						
'V2'	'T'	'C', 'G', 'N'						
PIN	L N or L H or 'M' + 32 H	<p>The PIN for which a PVV is required, encrypted under the LMK.</p> <p>When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length".</p> <p>When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.</p>						
Primary Account Number (PAN)	12 N or n N	<p>If a 3DES Key Block or Variant LMK is used:</p> <p>The 12 right-most digits of the PAN, excluding the check digit.</p> <p>If an AES Key Block LMK is used:</p> <p>The full 12-19 digit PAN, including the check digit.</p> <p>If present, the delimiter below must also be present.</p>						
Delimiter	1 A	Value ';' . Only present if an AES Key Block LMK is used.						
PVKI	1 N	The PVKI (should be between '0' and '6').						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'DH'.
Error Code	2 A	'00': No error '10': PVK parity error '27': PVK not double length '68': Command disabled '81': PIN length mismatch or a standard error code.
PVV	4 N	The resulting PVV.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate an ABA PVV (of a customer selected PIN)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate a 4-digit PVV using the ABA method. The PIN (for which a PVV is required) is supplied in an encrypted PIN Block.

Notes: Visa defines the PIN Verification Key Indicator (PVKI) to be between 0 and 6. The HSM does not enforce this restriction.

This command will optionally check the customer-selected PIN in order to exclude 'weak' PINs.

Caution: The behavior of this command is affected by the following CS (Configure Security) console command settings:

Enable Weak PIN checking? [Yes/No]

Check new PINs using global list of weak PINs: [Yes/No]

Check new PINs using local list of weak PINs: [Yes/No]

Check new PINs using rules: [Yes/No]

- Refer to the payShield 10K Security Operations manual for full details on how these settings can prevent the generation of 'weak' PINs.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'FW'.						
PIN Block Key Type	3 H	<p>For a Variant LMK:</p> <p>Type of PIN Block Key. The following key types are permitted:</p> <p>If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N":</p> <ul style="list-style-type: none"> '001': ZPK (encrypted under LMK 06-07 variant 0) '002': TPK (encrypted under LMK 14-15 variant 0) <p>If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y":</p> <ul style="list-style-type: none"> '001': ZPK (encrypted under LMK 06-07 variant 0) '70D': TPK (encrypted under LMK 36-37 variant 7) 						
PIN Block Key		<p>For a Key Block LMK:</p> <p>This field is ignored; should be set to 'FFF'.</p> <p>The Key under which the PIN blocks are encrypted.</p>						
	16 H or 'U' + 32 H or 'T' + 48 H	For a Variant LMK, the 'PIN Block Key' is either a ZPK or TPK, as specified above.						
	or 'S' + n A	For a Key Block LMK, the 'PIN Block Key' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '71', '72'</td> <td>'D', 'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '71', '72'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '71', '72'	'D', 'T', 'A'	'B', 'D', 'N'						
PVK		<p>The PVK, used to generate the PVV.</p>						
	32 H or 'U' + 32 H	For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.						
	or 'S' + n A	For a Key Block LMK, the 'PVK' is a double-length key, and must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'V2'</td> <td>'T'</td> <td>'C', 'G', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'V2'	'T'	'C', 'G', 'N'
Key Usage	Algorithm	Mode of Use						
'V2'	'T'	'C', 'G', 'N'						
PIN Block	16 H or 32 H	The PIN for which a PVV is required; encrypted under the PIN Block Key. When using a DES PIN Block Key, this field will be 16 H. When using an AES PIN Block Key, this field will be 32 H.						
PIN Block Format Code	2 N	<p>One of the valid PIN block format codes.</p> <p>If the security setting "Restrict PIN block usage for PCI HSM compliance" has the value "Y" then the PIN Block Format must be one of:</p> <ul style="list-style-type: none"> '01': (ISO 9564 / ANSI X9.8 Format 0) '47': (ISO 9564 / ANSI X9.8 Format 3) '48': (ISO 9564 / ANSI X9.8 Format 4) 						
Primary Account Number (PAN)	n N	<p>The PAN, used to form the PIN Block.</p> <p>If 'PIN Block Format Code' = '48': The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.</p> <p>If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left.</p> <p>For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.</p>						
Delimiter	1 A	Value ';'. Only present if 'PIN Block Format Code' = '48'.						
PVKI	1 N	The PVKI (should be between '0' and '6').						
Delimiter	1 A	Value '*'.						
Excluded PIN Count	2 N	Only present if the following Excluded PIN fields are present. '00' ... '99': The number of excluded PINs listed in the following local Excluded PIN Table.						
Excluded PIN Length	2 N	'04' ... '12': The length of each excluded PIN in the following local Excluded PIN Table. Only present if the Excluded PIN Count > '00'.						

payShield 10K Core Host Commands

Excluded PIN Table	n N	A local list of PINs to be excluded. The length of this field will be Excluded PIN Count multiplied by Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'FX'.
Error Code	2 A	'00': No error '10': PVK parity error '27': PVK not double length '68': Command disabled '69': PIN Block format has been disabled '81': PIN length mismatch '86': PIN is determined to be 'weak' or a standard error code.
PVV	4 N	The resulting PVV.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Load the Excluded PIN Table

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Load a table of excluded PINs into the memory of the HSM.

Notes: The table will be stored in battery backed memory and will be retained over power cycles. There are a total of 9 unique tables each holding different length PINs (4..12). Each PIN in a table must have the same length. Up to 99 PINs may be stored in each table. Commands which implement Weak PIN functionality will check a PIN against the PINs in these global Excluded PIN Tables if the Security Setting "*Check new PINs using global list of weak PINs*" is set to Yes.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'BM'.
Excluded PIN Count	2 N	'00' ... '99': The number of excluded PINs listed in the global Excluded PIN Table.
Excluded PIN Length	2 N	'04' ... '12': The length of each excluded PIN in the global Excluded PIN Table.
Excluded PIN Table	n N	A global list of PINs to be excluded. The length of this field will be Excluded PIN Count multiplied by Excluded PIN Length characters.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'BN'.
Error Code	2 A	'00': No error '41': File storage error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

4.2 PIN Mailer Printing Commands

The payShield 10K can print PIN mailers (multicopy forms, the contents of which can be read only after the form has been opened) and other types of data that must be kept secret.

PIN mailers can be used to send PINs to cardholders. Also, if the cardholder is to be given the opportunity of selecting his/her own PIN by mail (instead of at an entry device), solicitation data can be sent; it is not necessary to send a PIN if only a solicitation request is to be sent.

Because the values that are printed on a mailer are not available to the Host, the payShield 10K returns check data to the Host to give confidence that the data printed on the mailer is correct (i.e., the payShield 10K has performed the correct cryptographic functions).

To configure the printer, use the CP (Configure Printer) console command.

The payShield 10K provides the following host commands to support PIN mailer printing operations:

Function	Command	Page
<i>Print PIN/PIN and Solicitation Data</i>	PE (PF, PZ)	282
<i>Print a PIN Solicitation Mailer</i>	OA (OB, OZ)	284
<i>Verify PIN/PIN and Solicitation Mailer Cryptography</i>	PG (PH)	286
<i>Verify Solicitation Mailer Cryptography</i>	RC (RD)	287

Print PIN/PIN and Solicitation Data

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Required	
Activity: pin.mailer.host	

Function: Print the PIN/PIN and solicitation data at the HSM-attached terminal.

Notes: A printer must be attached to one of the USB ports on the payShield 10K. Serial-to-USB and parallel-to-USB cables are available from Thales, on request.

The HSM must have a print format already defined.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'PE'.
Document type	1 A	'A': for 1st mailer on a 2-up form 'B': for 2nd mailer on a 2-up form 'C': for a 1-up form
Primary Account Number (PAN)	12 N or n N	If a 3DES Key Block or Variant LMK is used: The 12 right-most digits of the PAN, excluding the check digit. If an AES Key Block LMK is used: The full 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.
Delimiter	1 A	Value ';'. Only present if an AES Key Block LMK is used.
PIN	L N or L H	The PIN encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
Print Field 0	n A	The print field defined as Print Field 0 in the print format definition (must not contain a ';' character).
Delimiter	1 A	Value ';'.
Print Field 1	n A	The print field defined as Print Field 1 in the print format definition (must not contain a ';' character).
Delimiter	1 A	Value ';'.
...
Last print field	n A	The last print field defined in the print format definition (must not contain a ';' or '~' character).
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (before printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'PF'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
PIN check value and Reference number check value	L + 12 N	The cryptographic check on the PIN and solicitation reference number using the LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (after printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'PZ'.
Error Code	2 A	'00': No error '16': Printer not ready/disconnected '41': Internal hardware/software error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.

Print a PIN Solicitation Mailer

Variant LMK <input checked="" type="checkbox"/>	3DES Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Required	
Activity: pin.mailer.host	

Function: Print PIN solicitation data at the HSM-attached terminal.

Notes: A printer must be attached to one of the USB ports on the payShield 10K. Serial-to-USB and parallel-to-USB cables are available from Thales, on request.

The HSM must have a print format already defined.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'OA'.
Document type	1 A	'A': for 1st mailer on a 2-up form. 'B': for 2nd mailer on a 2-up form. 'C': for a 1-up form.
Primary Account Number (PAN)	12 N	The 12 right-most digits of the PAN, excluding the check digit.
Print Field 0	n A	The print field defined as Print Field 0 in the print format definition (must not contain a ';' character).
Delimiter	1 A	Value ';'.
Print Field 1	n A	The print field defined as Print Field 1 in the print format definition (must not contain a ';' character).
Delimiter	1 A	Value ';'.
...
Last print field	n A	The last print field defined in the print format definition (must not contain a ';' or '~' character).
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (before printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'OB'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
Reference number check value	12 N	The cryptographic check on the solicitation reference number using the LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (after printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'OZ'.
Error Code	2 A	'00': No error '16': Printer not ready/disconnected '41': Internal hardware/software error '68': Command disabled or a standard error code..
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.

Verify PIN/PIN and Solicitation Mailer Cryptography

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify the PE command processing performed by the HSM.

Notes: It is suggested that a PE command performed by one HSM is verified by a PG command performed by a different HSM.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'PG'.
Primary Account Number (PAN)	12 N or n N	If a 3DES Key Block or Variant LMK is used: The 12 right-most digits of the PAN, excluding the check digit. If an AES Key Block LMK is used: The full 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.
Delimiter	1 A	Value ';'. Only present if an AES Key Block LMK is used.
PIN	L N or L H or 'M' + 32 H	The PIN encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
PIN check value and Reference number check value	L + 12 N	The cryptographic check on the PIN and solicitation reference number using the LMK.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'PH'.
Error Code	2 A	'00': No error '01': PIN verification failure '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify Solicitation Mailer Cryptography

Variant LMK <input checked="" type="checkbox"/>	3DES Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify the OA command processing performed by the HSM.

Notes: It is suggested that an OA command performed by one HSM is verified by an RC command performed by a different HSM.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RC'.
Primary Account Number (PAN)	12 N	The 12 right-most digits of the PAN, excluding the check digit.
Reference number check value	12 N	The cryptographic check on the solicitation reference number using the LMK.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RD'.
Error Code	2 A	'00': No error '01': Verification failure '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

4.3 PIN Solicitation Data Processing Commands

When a cardholder is given the option of selecting a PIN, he/she returns a form containing a PIN selection and a reference number. For security reasons, the only connection between the PIN and the cardholder's account is this reference number which is a cryptographic representation of the last 10 digits of the account number (excluding the account number check digit).

The HSM processes these values and returns the encrypted PIN and the last 10 digits of the account number (excluding check digit). The Host can match the account number digits and store the encrypted PIN for subsequent processing (for verification purposes or the creation of PIN offsets etc.).

Because the reference number is the only link to the cardholder's PIN, there must be a means of validating the data that is manually entered. There is no way to validate the PIN except through dual entry procedures or through the visual comparison of the value entered and the value recorded on the mailer form.

The 12-digit reference number, unlike the PIN, can be validated by a Host program. This reference number is a 10-digit number, followed by two check digits. The check digits can be validated during or after data entry.

The data is batch processed using Host commands. The number of records entered must be greater than or equal to the minimum batch size set when the HSM is configured. Each batch consists of at least one logical record. Each logical record contains a 12-digit reference number (obtained from the returned solicitation mailer) and the cardholder-selected PIN.

When the batch has been loaded to internal memory, the HSM encrypts the PINs under LMK pair 02-03, and decrypts the reference numbers, yielding a value which contains the 10 right-most digits of the account number (excluding the check digit). The PIN and 10 digits of the account number are returned to the Host.

The payShield 10K provides the following host commands to support solicitation data entry operations:

Function	Command	Page
<i>Load Solicitation Data to User Storage</i>	QA (QB)	289
<i>Final Load of Solicitation Data to User Storage</i>	QC (QD)	290

Load Solicitation Data to User Storage

Variant LMK <input checked="" type="checkbox"/>	3DES Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Load up to 25 records of solicitation data to user storage.

Notes: Solicitation data records are processed in batches. The records in a batch are sent in 0 or more QA commands, with the final records being sent using a single QC command (which can hold 1,260 records). Each QA command can hold up to 25 records. The sequence must be terminated by a QC command.

The total number of records must be at least the minimum batch size as defined in the Configure Security settings. Small batch sizes should be avoided to prevent input and output records from being matched up.

The maximum batch size is 2,520 records.

If all the solicitation data can be included in a single QC command then there is no need to send QA command(s).

The solicitation data overwrites any tables or keys stored in the user storage. Therefore, it is necessary to reload the tables and keys when solicitation processing has been completed.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'QA'.
Solicitation Data 1	n A	The 12-digit reference number. The selected PIN (4 to 12 digits). A semicolon ';' as a delimiter.
Solicitation Data 2	n A	The 12-digit reference number. The selected PIN. A semicolon ';' as a delimiter.
...
Last solicitation data	n A	The 12-digit reference number. The selected PIN. A semicolon ';' as a delimiter.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'QB'.
Error Code	2 A	'00': No error '30': Invalid reference number '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Final Load of Solicitation Data to User Storage

Variant LMK <input checked="" type="checkbox"/>	3DES Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Load the last set of solicitation records to user storage and start processing data.

Notes: The command overwrites any tables or keys stored in user storage. Therefore, it is necessary to reload the tables and keys when solicitation processing has been completed.

The QC command can contain up to 1,260 records.

Where not all the solicitation data can be included in the QC command, the excess data can be included in one or more QA commands **preceding** the QC command.

If the batch contains more than 1,260 records then 2 QD responses will be provided, as each QD response can provide a maximum of 1,260 output records.

The maximum batch size is 2,520 records - i.e. the number of records that can be included in 2 QD responses.

The order of records in the QD response(s) is randomized so that these records cannot be matched up to the input records in the QA and QC commands.

payShield 10K Core Host Commands

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'QC'.
Solicitation Data 1	n A	The 12-digit reference number. The selected PIN (4 to 12 digits). A semicolon ';' as a delimiter.
Solicitation Data 2	n A	The 12-digit reference number. The selected PIN. A semicolon ';' as a delimiter.
...
Last solicitation data	n A	The 12-digit reference number. The selected PIN. A semicolon ';' as a delimiter.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'QD'.
Error Code	2 A	'00': No error '30': Invalid reference number '31': Insufficient entries for batch '68': Command disabled or a standard error code.
Processed Data 1	n N	The 10 right-most digits of the account number and PIN encrypted under the LMK, truncated (if necessary).
Processed Data 2	n N	The 10 right-most digits of the account number and PIN encrypted under the LMK, truncated (if necessary).
...
Last processed data	n N	The 10 right-most digits of the account number and PIN encrypted under the LMK, truncated (if necessary).
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

4.4 Print Output Formatting Commands

Forms for conveying and protecting PINs and keys can be produced on a printer attached to one of the USB ports on the payShield 10K. Serial-to-USB and parallel-to-USB cables are available from Thales, on request.

The documents are printed at the terminal in response to a command from the Host, as defined in the following subsections.

For a complete list of print formatting symbols, please refer to the *payShield 10K Host Programmer's manual*.

The payShield 10K provides the following host commands to support print output formatting operations:

Function	Command	Page
<i>Load Formatting Data to HSM</i>	PA (PB)	293
<i>Load Additional Formatting Data to HSM</i>	PC (PD)	294
<i>Load a PIN Text String</i>	LI (LJ)	295

Load Formatting Data to HSM

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Load formatting data to the HSM.

Notes: The HSM can store a maximum of 299 symbols and constants.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'PA'.
Data	n A	Symbols and constants defined in the <i>payShield 10K Host Programmer's manual</i> .
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'PB'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Load Additional Formatting Data to HSM

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Load additional formatting data to the HSM.

Notes: The PC command must be preceded by a PA command.

The HSM can store a maximum of 299 symbols and constants including the data sent with the PA command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'PC'.
Data	n A	Symbols and constants defined in the <i>payShield 10K Host Programmer's manual</i> .
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'PD'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Load a PIN Text String

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Load a PIN text string.

Notes: The default PIN text string, used by the HSM when printing PINs in words is initialized at Cold-Start to English (ONE, TWO, THREE,). The Load PIN Text String command can be used to re-define the text string which is then stored in battery-backed not tamper-protected memory.

When re-defining the text strings, strings for all characters (0 to 9) must be supplied.

The value for the length fields can be in the range 0,1,2,... to F (Hex), with 0 representing length 16_{10} .

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'LI'.
Length	1 H	The length of the string for Character 0.
Character 0	n B	The text string representing Character 0.
Length	1 H	The length of the string for Character 1.
Character 1	n B	The text string representing Character 1.
Length	1 H	The length of the string for Character 2.
Character 2	n B	The text string representing Character 2.
Length	1 H	The length of the string for Character 3.
...
Character 9	n B	The text string representing Character 9.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'LJ'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

4.5 Clear PIN Commands

**CAUTION!**

THE USE OF CLEAR PIN FACILITIES PRESENTS
A SIGNIFICANT SECURITY RISK.

The payShield 10K provides the following host commands to support clear PIN operations:

Function	Command	Page
<i>Encrypt a Clear PIN</i>	BA (BB)	297
<i>Decrypt an Encrypted PIN</i>	NG (NH)	298

Encrypt a Clear PIN

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Required	
Activity: pin.clear.host	



CAUTION!

THE USE OF THIS COMMAND PRESENTS A SIGNIFICANT SECURITY RISK.

Function: Encrypt a clear text PIN.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'BA'.
PIN	L H	The clear text PIN left-justified and padded with 'F's to the maximum PIN length L. Value set with the CS (Configure Security) console command (range 5 – 13).
Primary Account Number (PAN)	12 N	If a 3DES Key Block or Variant LMK is used: The 12 right-most digits of the PAN, excluding the check digit.
	or n N	If an AES Key Block LMK is used: The full 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.
Delimiter	1 A	Value ';'. Only present if an AES Key Block LMK is used.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'BB'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
PIN	L N or L H or 'M' + 32 H	The PIN encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Decrypt an Encrypted PIN

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Required	
Activity: pin.clear.host	



CAUTION!

THE USE OF THIS COMMAND PRESENTS A SIGNIFICANT SECURITY RISK.

Function: Decrypt an encrypted PIN and return a reference number.

Notes: The command is available only if selected during configuration by enabling the security setting "Select clear PINs?".

The reference number can be used in solicitation data processing.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'NG'.
Primary Account Number (PAN)	12 N or n N	If a 3DES Key Block or Variant LMK is used: The 12 right-most digits of the PAN, excluding the check digit. If an AES Key Block LMK is used: The full 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.
Delimiter	1 A	Value ';'. Only present if an AES Key Block LMK is used.
PIN	L N or L H or 'M' + 32 H	The PIN encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'NH'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
PIN	L H	The clear PIN left-justified and padded with 'F's.
Reference number	12 N	The reference number derived by encrypting the PAN under the LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

4.6 Card Verification Code/Value Generation Commands

The Card Verification Value (CVV) is a cryptographic check value derived from specific fields of data, such as account number, card expiration date, service code, and keys (CVKs).

The CVV is written onto the card. During transactions it is sent to the HSM which recalculates the CVV and compares it with the received CVV to confirm the validity of the card.

The payShield 10K provides the following host commands to support card verification code/value operations:

Function	Command	Page
Generate a Card Verification Code/Value	CW (CX)	300
Calculate Card Security Codes	RY (RZ)	302

Generate a Card Verification Code/Value

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate a Card Verification Code or Value.

Notes: Used to generate a payment card's verification code/value.

This command can be used to generate:

- the Visa CVV1 or Mastercard CVC1 for encoding onto the card's magnetic stripe.
- the Visa CVV2 or Mastercard CVC2 for printing on a card's signature strip. In this case, the Service Code field should be set to "000".
- the Visa iCVV or Mastercard Chip CVC for inclusion on an EMV chip card. In this case, the Service Code field should be set to "999".
- the Visa CAVV or Mastercard AAV for use in the 3-D Secure environment. In this case:

The Expiration date is replaced by a 4-digit Unpredictable number calculated from the Transaction Identifier, as defined in the 3-D Secure process.

The Service Code is replaced by the following 2 fields:

- A 1-digit Authentication Results Code, as defined for the 3-D Secure process
- A 2-digit Second Factor Authentication Results Code, as defined for the 3-D Secure process

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'CW'.						
CVK A / B	32 H or 'U' + 32 H or 'S' + n A	The CVK A / B key, used to calculate the CVV/CVC. For a Variant LMK, the 'CVK A/B' must be encrypted under LMK pair 14-15 variant 4. For a Key Block LMK, the 'CVK A/B' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'C0', '12', '13'</td> <td>'T'</td> <td>'C', 'G', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'C0', '12', '13'	'T'	'C', 'G', 'N'
Key Usage	Algorithm	Mode of Use						
'C0', '12', '13'	'T'	'C', 'G', 'N'						
If specifying the CVV data as a single parameter, the following 2 fields must be present.								
CVV Data Delimiter	1 A	Value '#'. Optional; if present, the following field CVV Data must be present.						
CVV Data	32 N	Card Verification Value data from which the CVV is generated.						
If specifying the CVV data using separate parameters, the following 4 fields must be present.								
Primary account number	n N	The PAN for the card; max 19 digits.						
Delimiter	1 A	Value ':'.						
Expiration date	4 N	The card expiration date (or Unpredictable Number for CAVV/AAV).						
Service code	3 N	The card service code (or Authentication Results Code (1 digit) + Second factor Authentication Results Code (2 digits) for CAVV / AAV).						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'CX'.
Error Code	2 A	'00': No error '10': CVK A or CVK B parity error '27': CVK not double length '68': Command disabled or a standard error code.
CVV	3 N	The Card Verification Value/Code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Calculate Card Security Codes

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate an American Express Card Security Code (CSC).

This command computes and returns the 5-digit, 4-digit and 3-digit Card Security Code Values from the supplied data.

This command supports three algorithms for calculating the CSC:

- Classic CSC Algorithm (CSC Version 1.0)
- Enhanced CSC Algorithm (CSC Version 2.0)
- American Express Verification Value (AEVV). In this case:

The Expiration date is replaced by a 4-digit Unpredictable number calculated from the Transaction Identifier, as defined in the 3-D Secure process.

The Service Code is replaced by the following 2 fields:

- A 1-digit Authentication Results Code, as defined for the AEVV process
- A 2-digit Second Factor Authentication Results Code, as defined for the AEVV process

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'RY'.						
Mode	1 N	Value '3'.						
Flag	1 N	A flag to indicate special processing options: '0': Classic CSC Algorithm (CSC Version 1.0) '2': Enhanced CSC Algorithm (CSC Version 2.0) '3': American Express Verification Value (AEVV)						
CSCK	32 H or 'U' + 32 H or 'S' + n A	<p>For a Variant LMK, the 'CSCK' must be encrypted under LMK pair 14-15 variant 4.</p> <p>For a Key Block LMK, the 'CSCK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'C0', '11'</td> <td>'T'</td> <td>'C', 'G', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'C0', '11'	'T'	'C', 'G', 'N'
Key Usage	Algorithm	Mode of Use						
'C0', '11'	'T'	'C', 'G', 'N'						
Primary Account Number (PAN)	19 N	The full PAN, left-justified and zero-filled if less than 19 digits.						
Expiration date	4 N	If Flag = '0' or '2', this field contains the card's expiration date, in the format YYMM. If Flag = '3', this field contains the AEVV Unpredictable Number.						
Service Code	3 N	Only present if Flag = '2' or '3'. If Flag = '3', this field contains the AEVV Authentication Results Code (1 digit) followed by the AEVV Second Factor Authenticating Code (2 digits).						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RZ'.
Error Code	2 A	'00': No error '10': CSCK parity error '27': CSCK not double length '68': Command disabled or a standard error code.
Mode	1 N	Value '3'.
5-digit CSC/iCSC	5 N	Only present if Flag = '0' or '2'. The 5-digit Card Security Code.
4-digit CSC/iCSC	4 N	Only present if Flag = '0' or '2'. The 4-digit Card Security Code.
3-digit CSC/iCSC/AEVV	3 N	The 3-digit Card Security Code (or the 3-digit AEVV if Flag = '3').
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

5 Magnetic Stripe Transaction Processing

5.1 PIN Change Commands

The PIN change process includes verifying the existing PIN before processing the new PIN.

The existing and new PIN blocks are encrypted under the same key: either a TPK or a ZPK depending on whether it has come from a local ATM (or PIN pad etc.) or from an acquirer. Therefore support is provided for changing a PIN from a "terminal" or from "interchange".

The payShield 10K provides the following host commands to support PIN change operations:

Function	Command	Page
<i>Verify a PIN & Generate an IBM PIN Offset (of customer selected new PIN)</i>	DU (DV)	305
<i>Verify a PIN & Generate an ABA PVV (of a customer selected PIN)</i>	CU (CV)	309

Verify a PIN & Generate an IBM PIN Offset (of customer selected new PIN)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a PIN, and if successful, generate the PIN offset of the customer selected PIN using the IBM 3624 method. The current and new PINs are supplied in an encrypted PIN Block.

Notes: The decimalization table can be stored in user storage and referenced in the same way as keys.

The use of encrypted decimalization tables is strongly recommended. By default the HSM is configured to expect encrypted decimalization tables in PIN commands that use the IBM offset method. For backward compatibility the HSM may be configured to use plaintext decimalization tables using Configure Security.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues generating the offset using 3DES in place of DES. (Double-length PVKs are now acceptable, but the returned error code has not been changed to allow for backward compatibility with existing Host applications which are expecting Error Code 02 to be returned.)

This command will optionally check the input PIN in order to exclude 'weak' PINs.

The PIN change process requires verifying the existing PIN and creating an Offset for the new PIN. The command performs both functions instead of requiring the use of the 3 existing commands:

- Verify Interchange/Terminal PIN Using the IBM Offset Method (EA or DA)
- Translate a PIN from TPK/ZPK to LMK Encryption (JC or JE)
- Generate an IBM PIN Offset (DE)

Caution: The behavior of this command is affected by the following CS (Configure Security) console command settings:

Decimalization Table: Encrypted/Plaintext [E/P]

- When set to 'E' (the default setting), the supplied decimalization table must be encrypted (using console command ED), and will consist of 16 hexadecimal digits (for a Variant or 3DES Key Block LMK) or 'L' + 32 hexadecimal digits (for an AES Key Block LMK).
- When set to 'P', the supplied decimalization table must be plaintext, and will consist of 16 decimal digits.

Decimalization Table checks enabled? [Yes/No]

- When set to 'Yes' (the default setting), the decimalization table must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, error code 25 is returned.
- When set to 'No', the decimalization table is not checked.

Enable support for variable length PIN offset? [Yes/No]

- When set to 'No' (the default setting), the length of the generated Offset is determined by the value of the Check Length parameter. This setting makes the command backward compatible with previous versions of software.
- When set to 'Yes', the length of the generated Offset matches the length of the input PIN.

Enable Weak PIN checking? [Yes/No]

Check new PINs using global list of weak PINs: [Yes/No]

Check new PINs using local list of weak PINs: [Yes/No]

Check new PINs using rules: [Yes/No]

- Refer to the payShield 10K Security Operations manual for full details on how these settings can prevent the generation of 'weak' PINs.

Restrict PIN block usage for PCI HSM compliance? [Yes/No]

- When set to 'Yes', the PIN Block Format Code must be 01 (ISO format 0), 47 (ISO format 3) or 48 (ISO format 4).
- When set to 'No', the PIN Block Format Code may be any supported value.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'DU'.						
Key Type	3 H	<p>For a Variant LMK:</p> <p>Type of PIN Block Key. The following key types are permitted:</p> <p>If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N":</p> <ul style="list-style-type: none"> '001': ZPK (encrypted under LMK 06-07 variant 0) '002': TPK (encrypted under LMK 14-15 variant 0) <p>If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y":</p> <ul style="list-style-type: none"> '001': ZPK (encrypted under LMK 06-07 variant 0) '70D': TPK (encrypted under LMK 14-15 variant 7) <p>For a Key Block LMK:</p> <p>This field is ignored; should be set to 'FFF'.</p>						
PIN Block Key	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The Key under which the PIN blocks are encrypted.</p> <p>For a Variant LMK, the 'PIN Block Key' is either a ZPK or TPK, as specified above.</p> <p>For a Key Block LMK, the 'PIN Block Key' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'P0', '71', '72'</td><td>'D', 'T', 'A'</td><td>'B', 'D', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '71', '72'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '71', '72'	'D', 'T', 'A'	'B', 'D', 'N'						
PVK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The PIN Verification Key, used to generate the offset.</p> <p>For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.</p> <p>For a Key Block LMK, the 'PVK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'V1'</td><td>'D', 'T'</td><td>'C', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'V1'	'D', 'T'	'C', 'N'
Key Usage	Algorithm	Mode of Use						
'V1'	'D', 'T'	'C', 'N'						
Current PIN block	16 H or 32 H	The Current PIN block encrypted under the PIN Block Key. When using a DES PIN Block Key, this field will be 16 H. When using an AES PIN Block Key, this field will be 32 H.						
PIN Block Format Code	2 N	<p>One of the valid PIN block format codes.</p> <p>If the security setting "Restrict PIN block usage for PCI HSM compliance" has the value "Y" then the PIN Block Format must be one of:</p> <ul style="list-style-type: none"> '01': (ISO 9564 / ANSI X9.8 Format 0) '47': (ISO 9564 / ANSI X9.8 Format 3) '48': (ISO 9564 / ANSI X9.8 Format 4) 						
Check Length	2 N	The minimum PIN length.						
Primary Account Number (PAN)	n N	<p>The PAN, used to form the PIN Block.</p> <p>If 'PIN Block Format Code' = '48': The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.</p> <p>If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left.</p> <p>For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.</p>						
Delimiter	1 A	Value ';'. Only present if 'PIN Block Format Code' = '48'.						
Decimalization Table	16 N or 16 H or 'K' + 3 H or 'L' + 32 H	<p>16 N when using Plaintext decimalization tables.</p> <p>16 H when using Encrypted decimalization tables and a Variant LMK or 3DES Key Block LMK.</p> <p>'K' + 3 H when referencing a decimalization table held in the HSM's User Storage Area</p> <p>'L' + 32 H when using Encrypted decimalization tables and an AES Key Block LMK.</p>						

payShield 10K Core Host Commands

Field	Length & Type	Details
PIN Validation Data	12 A or 'P' + 16 H	User-defined data consisting of hexadecimal characters and the character 'N', which indicates to the HSM where to insert the last 5 digits of the PAN; or User-defined data consisting of the ASCII character 'P' followed by 16 hexadecimal digits which will be used as input to the PIN generation algorithm.
Current Offset	12 H	IBM offset value, left-justified and padded with 'F's.
New PIN block	16 H or 32 H	The New PIN block encrypted under the PIN Block Key. When using a DES PIN Block Key, this field will be 16 H. When using an AES PIN Block Key, this field will be 32 H.
Delimiter	1 A	Value '*'.
Excluded PIN Count	2 N	'00' ... '99': The number of excluded PINs listed in the following local Excluded PIN Table.
Excluded PIN Length	2 N	'04' ... '12': The length of each excluded PIN in the following local Excluded PIN Table. Only present if the Excluded PIN Count > '00'.
Excluded PIN Table	n N	A local list of PINs to be excluded. The length of this field will be Excluded PIN Count multiplied by Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'DV'.
Error Code	2 A	'00': No error '01': PIN verification failure '02': Warning: PVK not single length '06': Invalid offset length '10': PIN Block Key parity error '11': PVK parity error '68': Command disabled '69': PIN Block format has been disabled '81': PIN length mismatch '86': PIN is determined to be 'weak' or a standard error code.
New Offset	12 H	The new offset value; left-justified and padded with 'F's.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a PIN & Generate an ABA PVV (of a customer selected PIN)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a PIN, and if successful, generate the PVV of the customer selected PIN using the ABA PVV method. The Current & New PINs are supplied in an encrypted PIN Block.

Notes: This command will optionally check the input PIN against an 'Excluded PIN Table' in order to exclude 'weak' PINs.
The PIN change process requires verifying the existing PIN and creating a PVV for the new PIN. The command performs both functions instead of requiring the use of the 3 existing commands:

- Verify Interchange/Terminal PIN Using the ABA PVV Method (EC or DC)
- Translate a PIN from TPK/ZPK to LMK Encryption (JC or JE)
- Generate a PVV (DG)

Caution: The behavior of this command is affected by the following CS (Configure Security) console command settings:

Enable Weak PIN checking? [Yes/No]

Check new PINs using global list of weak PINs: [Yes/No]

Check new PINs using local list of weak PINs: [Yes/No]

Check new PINs using rules: [Yes/No]

- Refer to the payShield 10K Security Operations manual for full details on how these settings can prevent the generation of 'weak' PINs.

Restrict PIN block usage for PCI HSM compliance? [Yes/No]

- When set to 'Yes', the PIN Block Format Code must be 01 (ISO format 0), 47 (ISO format 3) or 48 (ISO format 4).
- When set to 'No', the PIN Block Format Code may be any supported value.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'CU'.						
Key Type	3 H	<p>For a Variant LMK:</p> <p>Type of PIN Block Key. The following key types are permitted:</p> <p>If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N":</p> <ul style="list-style-type: none"> '001': ZPK (encrypted under LMK 06-07 variant 0) '002': TPK (encrypted under LMK 14-15 variant 0) <p>If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y":</p> <ul style="list-style-type: none"> '001': ZPK (encrypted under LMK 06-07 variant 0) '70D': TPK (encrypted under LMK 36-37 variant 7) <p>For a Key Block LMK:</p> <p>This field is ignored; should be set to 'FFF'.</p>						
PIN Block Key		<p>The Key under which the PIN blocks are encrypted.</p> <p>For a Variant LMK, the 'PIN Block Key' is either a ZPK or TPK, as specified above.</p>						
	16 H or 'U' + 32 H or 'T' + 48 H							
	or 'S' + n A	<p>For a Key Block LMK, the 'PIN Block Key' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'P0', '71', '72'</td><td>'D', 'T', 'A'</td><td>'B', 'D', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '71', '72'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '71', '72'	'D', 'T', 'A'	'B', 'D', 'N'						
PVK		<p>The PVK, used to generate the PVV.</p>						
	32 H or 'U' + 32 H	<p>For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.</p>						
	or 'S' + n A	<p>For a Key Block LMK, the 'PVK' is a double-length key, and must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'V2'</td><td>'T'</td><td>'C', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'V2'	'T'	'C', 'N'
Key Usage	Algorithm	Mode of Use						
'V2'	'T'	'C', 'N'						
Current PIN Block	16 H or 32 H	<p>The Current PIN block encrypted under the PIN Block Key.</p> <p>When using a DES PIN Block Key, this field will be 16 H.</p> <p>When using an AES PIN Block Key, this field will be 32 H.</p>						
PIN Block Format Code	2 N	<p>One of the valid PIN block format codes.</p> <p>If the security setting "Restrict PIN block usage for PCI HSM compliance" has the value "Y" then the PIN Block Format must be one of:</p> <ul style="list-style-type: none"> '01': (ISO 9564 / ANSI X9.8 Format 0) '47': (ISO 9564 / ANSI X9.8 Format 3) '48': (ISO 9564 / ANSI X9.8 Format 4) 						
Primary Account Number (PAN)	n N	<p>The PAN, used to form the PIN Block.</p> <p>If 'PIN Block Format Code' = '48':</p> <p>The 12-19 digit PAN, including the check digit.</p> <p>If present, the delimiter below must also be present.</p>						
	or 18 H	<p>If 'PIN Block Format Code' = '04':</p> <p>The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left.</p>						
	or 12 N	<p>For all other values of 'PIN Block Format Code':</p> <p>The 12 right-most digits of the PAN, excluding the check digit.</p>						
Delimiter	1 A	Value ';'. Only present if 'PIN Block Format Code' = '48'.						
PVKI	1 N	The PIN Verification Key Index.						
Current PVV	4 N	The PVV for the current PIN.						
New PIN block	16 H or 32 H	The New PIN block encrypted under the PIN Block Key.						
		When using a DES PIN Block Key, this field will be 16 H.						
		When using an AES PIN Block Key, this field will be 32 H.						
Delimiter	1 A	Value '*'.						
Excluded PIN Count	2 N	Only present if the following Excluded PIN fields are present. '00' ... '99': The number of excluded PINs listed in the following local Excluded PIN Table.						

payShield 10K Core Host Commands

Field	Length & Type	Details
Excluded PIN Length	2 N	'04' ... '12': The length of each excluded PIN in the following local Excluded PIN Table. Only present if the Excluded PIN Count > '00'.
Excluded PIN Table	n N	A local list of PINs to be excluded. The length of this field will be Excluded PIN Count multiplied by Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'CV'.
Error Code	2 A	'00': No error '01': PIN Verification failure '10': PIN Block Key parity error '11': PVK parity error '27': PVK not double length '68': Command disabled '69': PIN Block format has been disabled '81': PIN length mismatch '86': PIN is determined to be 'weak' or a standard error code.
New PVV	4 N	The PVV for the new PIN.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

5.2 PIN Verification Commands

For PIN verification a payShield 10K requires the PIN to be input as a 16-digit PIN block. The HSM supports a number of PIN block formats, each identified by a 2-digit PIN block format code. Formats 34, 35, 41 and 42 are used for EMV PIN change operations and are only available to the KU command.

The payShield 10K supports four methods of PIN verification:

- IBM 3624.
- Diebold Proprietary Algorithm.
- Visa PVV.
- PIN comparison.

For each type, the PIN block is encrypted under a TPK or a ZPK depending on whether it has come from a local ATM (or PIN pad etc.) or from an acquirer. Therefore, support is provided for verifying a PIN from a "terminal" or from "interchange".

The payShield 10K provides the following host commands to support PIN verification operations:

Function	Command	Page
<i>Verify a Terminal PIN Using the IBM Offset Method</i>	DA (DB)	313
<i>Verify an Interchange PIN Using the IBM Offset Method</i>	EA (EB)	316
<i>Verify a Terminal PIN Using the Diebold Method</i>	CG (CH)	319
<i>Verify an Interchange PIN Using the Diebold Method</i>	EG (EH)	321
<i>Verify a Terminal PIN Using the ABA PVV Method</i>	DC (DD)	322
<i>Verify an Interchange PIN Using the ABA PVV Method</i>	EC (ED)	325
<i>Verify a Terminal PIN Using the Comparison Method</i>	BC (BD)	327
<i>Verify an Interchange PIN Using the Comparison Method</i>	BE (BF)	329

PIN verification commands specific to the DUKPT key management can be found in the section on *DUKPT (X9.24) Transaction Processing Commands*.

Verify a Terminal PIN Using the IBM Offset Method

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a PIN from a local ATM (or PIN pad etc.) using the IBM 3624 method.

Notes: The decimalization table can be stored in user storage and referenced in the same way as keys.

The use of encrypted decimalization tables is strongly recommended. By default the HSM is configured to expect encrypted decimalization tables in PIN commands that use the IBM offset method. For backward compatibility the HSM may be configured to use plaintext decimalization tables using Configure Security.

The plaintext decimalization table of 16 digits must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, Error Code 25 is returned. Checking of the table is the default condition, but may be disabled using the CS console command. Disabling of the check is not recommended.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues verifying the PIN using 3DES in place of DES. (Double-length PVKs are now acceptable, but the returned error code has not been changed to allow for backward compatibility with existing Host applications which are expecting Error Code 02 to be returned.)

Caution: The behavior of this command is affected by the following CS (Configure Security) console command setting:

Decimalization Table: Encrypted/Plaintext [E/P]

- When set to 'E' (the default setting), the supplied decimalization table must be encrypted (using console command ED), and will consist of 16 hexadecimal digits (for a Variant or 3DES Key Block LMK) or 'L' + 32 hexadecimal digits (for an AES Key Block LMK).
- When set to 'P', the supplied decimalization table must be plaintext, and will consist of 16 decimal digits.

The behavior of this command is affected by the following CS (Configure Security) console command setting:

Decimalization Table checks enabled? [Yes/No]

- When set to 'Yes' (the default setting), the decimalization table must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, error code 25 is returned.
- When set to 'No', the decimalization table is not checked.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'DA'.						
TPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The TPK under which the PIN block is encrypted. For a Variant LMK, the 'TPK' must be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y". For a Key Block LMK, the 'TPK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '71'</td> <td>'D', 'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '71'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '71'	'D', 'T', 'A'	'B', 'D', 'N'						
PVK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The PVK used to verify the PIN. For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0. For a Key Block LMK, the 'PVK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'V1'</td> <td>'D', 'T'</td> <td>'C', 'V', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'V1'	'D', 'T'	'C', 'V', 'N'
Key Usage	Algorithm	Mode of Use						
'V1'	'D', 'T'	'C', 'V', 'N'						
Maximum PIN Length	2 N	Value '12'.						
PIN Block	16 H or 32 H	The PIN block encrypted under the TPK. When using a DES TPK, this field will be 16 H. When using an AES TPK, this field will be 32 H.						
PIN Block Format Code	2 N	One of the valid PIN block format codes.						
Check Length	2 N	The minimum PIN length.						
Primary Account Number (PAN)	n N or 18 H or 12 N	The PAN, used to form the PIN Block. If 'PIN Block Format Code' = '48': The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present. If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.						
Delimiter	1 A	Value ':'. Only present if 'PIN Block Format Code' = '48'.						
Decimalization Table	16 N or 16 H or 'K' + 3 H or 'L' + 32 H	16 N when using Plaintext decimalization tables. 16 H when using Encrypted decimalization tables and a Variant LMK or 3DES Key Block LMK. 'K' + 3 H when referencing a decimalization table held in the HSM's User Storage Area. 'L' + 32 H when using Encrypted decimalization tables and an AES Key Block LMK.						
PIN Validation Data	12 A or 'P' + 16 H	User-defined data consisting of hexadecimal characters and the character 'N', which indicates to the HSM where to insert the last 5 digits of the PAN; or User-defined data consisting of the ASCII character 'P' followed by 16 hexadecimal digits which will be used as input to the PIN generation algorithm.						
Offset	12 H	IBM offset value, left-justified and padded with 'F's.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'DB'.
Error Code	2 A	<p>'00': No error '01': PIN verification failure '02': Warning: PVK not single length '06': Invalid offset length '10': TPK parity error '11': PVK parity error '68': Command disabled '69': PIN Block format has been disabled '88': Warning: PIN Block contains a zero length PIN or a standard error code.</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify an Interchange PIN Using the IBM Offset Method

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a PIN from interchange using the IBM 3624 method.

Notes: The decimalization table can be stored in user storage and referenced in the same way as keys.

The use of encrypted decimalization tables is strongly recommended. By default the HSM is configured to expect encrypted decimalization tables in PIN commands that use the IBM offset method. For backward compatibility the HSM may be configured to use plaintext decimalization tables using Configure Security.

The plaintext decimalization table of 16 digits must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, Error Code 25 is returned. Checking of the table is the default condition, but may be disabled using the CS console command. Disabling of the check is not recommended.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues verifying the PIN using 3DES in place of DES. (Double-length PVKs are now acceptable, but the returned error code has not been changed to allow for backward compatibility with existing Host applications which are expecting Error Code 02 to be returned.)

Caution: The behavior of this command is affected by the following CS (Configure Security) console command setting:

Decimalization Table: Encrypted/Plaintext [E/P]

- When set to 'E' (the default setting), the supplied decimalization table must be encrypted (using console command ED), and will consist of 16 hexadecimal digits (for a Variant or 3DES Key Block LMK) or 'L' + 32 hexadecimal digits (for an AES Key Block LMK).
- When set to 'P', the supplied decimalization table must be plaintext, and will consist of 16 decimal digits.

The behavior of this command is affected by the following CS (Configure Security) console command setting:

Decimalization Table checks enabled? [Yes/No]

- When set to 'Yes' (the default setting), the decimalization table must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, error code 25 is returned.
- When set to 'No', the decimalization table is not checked.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'EA'.						
ZPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The ZPK under which the PIN block is encrypted. For a Variant LMK, the 'ZPK' must be encrypted under LMK pair 06-07. For a Key Block LMK, the 'ZPK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'P0', '72'</td><td>'D', 'T', 'A'</td><td>'B', 'D', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '72'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'D', 'T', 'A'	'B', 'D', 'N'						
PVK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The PVK used to verify the PIN. For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0. For a Key Block LMK, the 'PVK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'V1'</td><td>'D', 'T'</td><td>'C', 'V', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'V1'	'D', 'T'	'C', 'V', 'N'
Key Usage	Algorithm	Mode of Use						
'V1'	'D', 'T'	'C', 'V', 'N'						
Maximum PIN Length	2 N	Value '12'.						
PIN Block	16 H or 32 H	The PIN block encrypted under the ZPK. When using a DES ZPK, this field will be 16 H. When using an AES ZPK, this field will be 32 H.						
PIN Block Format Code	2 N	One of the valid PIN block format codes.						
Check Length	2 N	The minimum PIN length.						
Primary Account Number (PAN)	n N or 18 H or 12 N	The PAN, used to form the PIN Block. If 'PIN Block Format Code' = '48': The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present. If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.						
Delimiter	1 A	Value ':' . Only present if 'PIN Block Format Code' = '48'.						
Decimalization Table	16 N or 16 H or 'K' + 3 H or 'L' + 32 H	16 N when using Plaintext decimalization tables. 16 H when using Encrypted decimalization tables and a Variant LMK or 3DES Key Block LMK. 'K' + 3 H when referencing a decimalization table held in the HSM's User Storage Area. 'L' + 32 H when using Encrypted decimalization tables and an AES Key Block LMK.						
PIN Validation Data	12 A or 'P' + 16 H	User-defined data consisting of hexadecimal characters and the character 'N', which indicates to the HSM where to insert the last 5 digits of the PAN; or User-defined data consisting of the ASCII character 'P' followed by 16 hexadecimal digits which will be used as input to the PIN generation algorithm.						
Offset	12 H	IBM offset value, left-justified and padded with 'F's.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'EB'.
Error Code	2 A	<p>'00': No error '01': PIN verification failure '02': Warning: PVK not single length '06': Invalid offset length '10': ZPK parity error '11': PVK parity error '68': Command disabled '69': PIN Block format has been disabled '88': Warning: PIN Block contains a zero length PIN or a standard error code.</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a Terminal PIN Using the Diebold Method

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a PIN from a local ATM (or PIN pad etc.) using the Diebold method.

Notes: The Diebold table must be stored in user storage before using this command.

If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", the Diebold table is encrypted using LMK pair 14-15 variant 0.

If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y", the Diebold table is encrypted using LMK pair 36-37 variant 6.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'CG'.						
TPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The TPK under which the PIN block is encrypted.</p> <p>For a Variant LMK, the 'TPK' must be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y".</p> <p>For a Key Block LMK, the 'TPK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'P0', '71'</td><td>'D', 'T', 'A'</td><td>'B', 'D', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'P0', '71'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '71'	'D', 'T', 'A'	'B', 'D', 'N'						
Index Flag	1 A	Value 'K'.						
Table Pointer	3 H	The value of the base location of the Diebold table in user storage.						
Algorithm Number	2 H	The number of the Diebold algorithm required.						
PIN Block	16 H or 32 H	The PIN block encrypted under the TPK. When using a DES TPK, this field will be 16 H. When using an AES TPK, this field will be 32 H.						
PIN Block Format Code	2 N	One of the valid PIN block format codes.						
Primary Account Number (PAN)	n N or 18 H or 12 N	<p>The PAN, used to form the PIN Block.</p> <p>If 'PIN Block Format Code' = '48': The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.</p> <p>If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left.</p> <p>For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.</p>						
Delimiter	1 A	Value ';'. Only present if 'PIN Block Format Code' = '48'.						
PIN Validation Data	16 A	User-defined data consisting of hexadecimal characters and the character 'N', which indicates to the HSM where to insert the last 5 digits of the PAN. The data must be right-justified and padded with 'F's.						
Offset	4 N	PIN offset.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						

Field	Length & Type	Details
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'CH'.
Error Code	2 A	'00': No error '01': PIN verification failure '10': TPK parity error '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify an Interchange PIN Using the Diebold Method

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a PIN from interchange using the Diebold method.

Notes: The Diebold table must be stored in user storage before using this command.

If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", the Diebold table is encrypted using LMK pair 14-15 variant 0.

If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y", the Diebold table is encrypted using LMK pair 36-37 variant 6.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'EG'.						
ZPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The ZPK under which the PIN block is encrypted. For a Variant LMK, the 'ZPK' must be encrypted under LMK pair 06-07. For a Key Block LMK, the 'ZPK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '72'</td> <td>'D', 'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '72'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'D', 'T', 'A'	'B', 'D', 'N'						
Index Flag	1 A	Value 'K'.						
Table Pointer	3 H	The value of the base location of the Diebold table in user storage.						
Algorithm Number	2 H	The number of the Diebold algorithm required.						
PIN Block	16 H or 32 H	The PIN block encrypted under the ZPK. When using a DES ZPK, this field will be 16 H. When using an AES ZPK, this field will be 32 H.						
PIN Block Format Code	2 N	One of the valid PIN block format codes.						
Primary Account Number (PAN)	n N or 18 H or 12 N	The PAN, used to form the PIN Block. If 'PIN Block Format Code' = '48': The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present. If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.						
Delimiter	1 A	Value ';'. Only present if 'PIN Block Format Code' = '48'.						
PIN Validation Data	16 A	User-defined data consisting of hexadecimal characters and the character 'N', which indicates to the HSM where to insert the last 5 digits of the PAN. The data must be right-justified and padded with 'F's.						
Offset	4 N	PIN offset.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						

Field	Length & Type	Details
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'EH'.
Error Code	2 A	'00': No error '01': PIN verification failure '10': ZPK parity error '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a Terminal PIN Using the ABA PVV Method

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a PIN from a local ATM (or PIN pad etc.) using the ABA PVV method.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'DC'.						
TPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The TPK under which the PIN block is encrypted.</p> <p>For a Variant LMK, the 'TPK' must be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y".</p> <p>For a Key Block LMK, the 'TPK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '71'</td> <td>'D', 'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '71'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '71'	'D', 'T', 'A'	'B', 'D', 'N'						
PVK	32 H or 'U' + 32 H or 'S' + n A	<p>The PVK, used to generate the PVV.</p> <p>For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.</p> <p>For a Key Block LMK, the 'PVK' is a double-length key, and must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'V2'</td> <td>'T'</td> <td>'C', 'V', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'V2'	'T'	'C', 'V', 'N'
Key Usage	Algorithm	Mode of Use						
'V2'	'T'	'C', 'V', 'N'						
PIN Block	16 H or 32 H	The PIN block encrypted under the TPK. When using a DES TPK, this field will be 16 H. When using an AES TPK, this field will be 32 H.						
PIN Block Format Code	2 N	One of the valid PIN block format codes.						
Primary Account Number (PAN)	n N or 18 H or 12 N	<p>The PAN, used to form the PIN Block.</p> <p>If 'PIN Block Format Code' = '48': The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.</p> <p>If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left.</p> <p>For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.</p>						
Delimiter	1 A	Value ':'. Only present if 'PIN Block Format Code' = '48'.						
PVKI	1 N	The PIN Verification Key Index.						
PVV	4 N	The PVV for the PIN.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'DD'.
Error Code	2 A	'00': No error '01': PIN verification failure '10': TPK parity error '11': PVK parity error '27': PVK not double length '68': Command disabled '69': PIN Block format has been disabled '88': Warning: PIN Block contains a zero length PIN or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify an Interchange PIN Using the ABA PVV Method

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a PIN from interchange using the ABA PVV method.

This command supports the verification of PIN blocks built using a Token instead of the real PAN. This functionality is only supported if the security setting "*Enable use of Tokens in PIN Verification*" has the value "Y".

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'EC'.						
ZPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The ZPK under which the PIN block is encrypted.</p> <p>For a Variant LMK, the 'ZPK' must be encrypted under LMK pair 06-07.</p> <p>For a Key Block LMK, the 'ZPK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '72'</td> <td>'D', 'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '72'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'D', 'T', 'A'	'B', 'D', 'N'						
PVK	32 H or 'U' + 32 H or 'S' + n A	<p>The PVK, used to generate the PVV.</p> <p>For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.</p> <p>For a Key Block LMK, the 'PVK' is a double-length key, and must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'V2'</td> <td>'T'</td> <td>'C', 'V', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'V2'	'T'	'C', 'V', 'N'
Key Usage	Algorithm	Mode of Use						
'V2'	'T'	'C', 'V', 'N'						
PIN Block	16 H or 32 H	The PIN block encrypted under the ZPK. When using a DES ZPK, this field will be 16 H. When using an AES ZPK, this field will be 32 H.						
PIN Block Format Code	2 N	One of the valid PIN block format codes.						
Primary Account Number (PAN) or Token	n N or 18 H or 12 N	<p>If 'PIN Block' uses a token instead of the actual PAN, this field will contain the token number. Otherwise, it will contain the PAN.</p> <p>If 'PIN Block Format Code' = '48': The 12-19 digit PAN/Token, including the check digit. If present, the delimiter below must also be present.</p> <p>If 'PIN Block Format Code' = '04': The 18 digit PAN/Token excluding the check digit. If the PAN/Token is less than 18 digits, it must be right-justified and padded with 'F's on the left.</p> <p>For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN/Token, excluding the check digit.</p>						
Delimiter	1 A	Value ';'. Only present if 'PIN Block Format Code' = '48'.						

payShield 10K Core Host Commands

Field	Length & Type	Details
The following 2 or 3 fields are required when the PIN Block was formed using a Token (instead of the real PAN), and the PIN Verification Value (PVV) needs to be formed using the real PAN.		
Verification PAN Delimiter	1 A	Value ';'. Optional; if present, the following field must also be present. Only allowed if the security setting "Enable use of Tokens in PIN Verification" is set to "Y".
Verification PAN	n N or 12 N	Only present if 'Verification PAN Delimiter' is present. If 'PIN Block Format Code' = '48': The 12-19 digit Verification PAN, including the check digit. If present, the delimiter below must also be present. For all other values of 'PIN Block Format Code': The 12 right-most digits of the Verification PAN, excluding the check digit.
Delimiter	1 A	Value ';'. Only present if 'PIN Block Format Code' = '48'.
PVKI	1 N	The PIN Verification Key Index.
PVV	4 N	The PVV for the PIN.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ED'.
Error Code	2 A	'00': No error '01': PIN verification failure '10': ZPK parity error '11': PVK parity error '17': PIN token verification disabled '27': PVK not double length '68': Command disabled '69': PIN Block format has been disabled '88': Warning: PIN Block contains a zero length PIN or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a Terminal PIN Using the Comparison Method

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a PIN received from an ATM (or terminal etc.) by comparing it with a value held on the Host database.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'BC'.						
TPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	For a Variant LMK, the 'TPK' must be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y". For a Key Block LMK, the 'TPK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '71'</td> <td>'D', 'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '71'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '71'	'D', 'T', 'A'	'B', 'D', 'N'						
PIN Block	16 H or 32 H	The PIN block containing the PIN for verification; encrypted under the TPK. When using a DES TPK, this field will be 16 H. When using an AES TPK, this field will be 32 H.						
PIN Block Format Code	2 N	One of the valid PIN block format codes.						
For a 3DES Variant or 3DES Key Block LMK, the following field must be present:								
Primary Account Number (PAN)	18 H or 12 N	The PAN, used to form the PIN Block. If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.						
For an AES Key Block LMK, the following two fields must be present:								
Primary Account Number (PAN)	n N	The PAN, used to form the PIN Block.						
Delimiter	1 A	The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present. Value ';'.						
PIN	L N or L H or 'M' + 32 H	The PIN from the host database, encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'BD'.
Error Code	2 A	'00': No error '01': PIN verification failure '10': TPK parity error '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify an Interchange PIN Using the Comparison Method

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a PIN received from interchange by comparing it with a value held on the Host database.

Notes: 3DES PIN encryption keys cannot be used with PIN block format code 48.
AES PIN encryption keys can only be used with PIN block format code 48.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'BE'.						
ZPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The ZPK under which the PIN block is encrypted. For a Variant LMK, the 'ZPK' must be encrypted under LMK pair 06-07.						
PIN Block	16 H or 32 H	For a Key Block LMK, the 'ZPK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '72'</td> <td>'D', 'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </table> The PIN block containing the PIN for verification; encrypted under the ZPK. When using a DES ZPK, this field will be 16 H. When using an AES ZPK, this field will be 32 H.	Key Usage	Algorithm	Mode of Use	'P0', '72'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'D', 'T', 'A'	'B', 'D', 'N'						
PIN Block Format Code	2 N	One of the valid PIN block format codes.						
For a 3DES Variant or 3DES Key Block LMK, the following field must be present:								
Primary Account Number (PAN)	18 H or 12 N	The PAN, used to form the PIN Block. If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.						
For an AES Key Block LMK, the following two fields must be present:								
Primary Account Number (PAN)	n N	The PAN, used to form the PIN Block.						
Delimiter	1 A	The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present. Value ':'.						
PIN	L N or L H or 'M' + 32 H	The PIN from the host database, encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'BF'.
Error Code	2 A	'00': No error '01': PIN verification failure '10': ZPK parity error '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

5.3 PIN Translation Commands

For PIN PIN translation a payShield 10K HSM requires the PIN to be input as a 16-digit PIN block. The HSM supports a number of PIN block formats, each identified by a 2-digit PIN block format code. Formats 34, 35, 41 and 42 are used for EMV PIN change operations and are only available to the KU command.

Commands are provided to translate PIN blocks from encryption under one key to encryption under another. The commands can also translate the format of a PIN block, with the exception of those that translate to the LMK (where the PIN is not held in a standard format).

The QK host command can be used to translate an LMK-encrypted PIN where the cardholder's account number (PAN) is to be changed but the old PIN is to be retained. Use of this command is preferable to the traditional way of achieving the aim by translating the PIN to an intermediate PIN Block format which does not involve the PAN and then translating this to a new PIN Block involving the new account number: this approach has security issues and contravenes PCI security standards.

The payShield 10K provides the following host commands to support PIN translation operations:

Function	Command	Page
<i>Translate a PIN from One ZPK to Another</i>	CC (CD)	332
<i>Translate a PIN from TPK to ZPK/BDK Encryption (3DES DUKPT)</i>	CA (CB)	335
<i>Translate a PIN from ZPK to LMK Encryption</i>	JE (JF)	339
<i>Translate a PIN from TPK to LMK Encryption</i>	JC (JD)	341
<i>Translate a PIN from LMK to ZPK Encryption</i>	JG (JH)	343
<i>Translate PIN Algorithm</i>	BQ (BR)	345
<i>Translate Account Number for LMK-encrypted PIN</i>	QK (QL)	346
<i>Translate an RSA-encrypted PIN to a ZPK or TPK-encrypted PIN</i>	AQ (AR)	348
<i>Load OPINPad to HSM Memory</i>	P6 (P7)	351
<i>Decode OPIN and translate to ZPK</i>	P8 (P9)	352

PIN translation commands specific to the DUKPT key management can be found in the section on *DUKPT (X9.24) Transaction Processing Commands*.

Translate a PIN from One ZPK to Another

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Translate a PIN block from encryption under one ZPK to encryption under another ZPK and from one format to another. If the same ZPK is defined, only the PIN block is translated, and if the same PIN block format is defined, only the key is translated.

This command supports the translation of PIN blocks built using a Token instead of the real PAN. This functionality is only supported if the security setting "*Enable use of Tokens in PIN Translation*" is "YES".

For a list of PIN block formats permitted for use in this command, please refer to the *payShield 10K Host Programmer's Manual*.

Notes: The PIN block format may also be changed, but refer to the table below for restrictions.

3DES PIN encryption keys cannot be used with PIN block format code 48.

AES PIN encryption keys can only be used with PIN block format code 48.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'CC'.						
Source ZPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The ZPK under which the PIN block is currently encrypted.</p> <p>For a Variant LMK, the 'Source ZPK' must be encrypted under LMK pair 06-07.</p> <p>For a Key Block LMK, the 'Source ZPK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'P0', '72'</td><td>'D', 'T', 'A'</td><td>'B', 'D', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '72'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'D', 'T', 'A'	'B', 'D', 'N'						
Destination ZPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>Destination ZPK under which the PIN block is to be encrypted.</p> <p>For a Variant LMK, the 'Destination ZPK' must be encrypted under LMK pair 06-07.</p> <p>For a Key Block LMK, the 'Destination ZPK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'P0', '72'</td><td>'D', 'T', 'A'</td><td>'B', 'E', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '72'	'D', 'T', 'A'	'B', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'D', 'T', 'A'	'B', 'E', 'N'						
Maximum PIN Length	2 N	Value '12'.						
Source PIN Block	16 H or 32 H	The source PIN block encrypted under the Source ZPK. When using a DES Source ZPK, this field will be 16 H. When using an AES Source ZPK, this field will be 32 H.						
Source PIN Block Format	2 N	The format code for the 'Source PIN Block'. The format code for any currently enabled and permitted PIN block format may be specified.						
Destination PIN Block Format	2 N	The format code for the 'Destination PIN Block'. The format code for any currently enabled and permitted PIN block format may be specified, unless prohibited by one or more of the following security settings: <ul style="list-style-type: none"> • "Restrict PIN block usage for PCI compliance" • "Enable PIN Block Format 34 as output format for PIN translations to ZPK" 						

Field	Length & Type	Details
The following fields are required when the Source PIN Block and the Destination PIN Block use the same PAN.		
Primary Account Number (PAN)	n N or 18 H or 12 N	<p>The PAN that was used to form the Source PIN Block and to be used to form the Destination PIN Block.</p> <p>If 'Source PIN Block Format Code' or 'Destination PIN Block Format Code' is '48': The 12-19 digit PAN.</p> <p>If present, the delimiter below must also be present.</p> <p>If 'Source PIN Block Format Code' or 'Destination PIN Block Format Code' is '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left.</p> <p>For all other values of 'Source PIN Block Format Code' and 'Destination PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.</p>
Delimiter	1 A	<p>Value ';'. Only present if 'Source PIN Block Format Code' = '48' or 'Destination PIN Block Format Code' = '48'.</p>
The following fields are required when the Source PIN Block was formed using a token PAN (instead of the real PAN), and the Destination PIN Block needs to be formed using the real PAN.		
Source PAN	n N or 18 H or 12 N	<p>The PAN that was used to form the Source PIN Block.</p> <p>If 'Source PIN Block Format Code' is '48': The 12-19 digit Source PAN.</p> <p>If present, the delimiter below must also be present.</p> <p>If 'Source PIN Block Format Code' is '04': The 18 digit Source PAN excluding the check digit. If the Source PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left.</p> <p>For all other values of 'Source PIN Block Format Code': The 12 right-most digits of the Source PAN, excluding the check digit.</p>
Delimiter	1 A	Value ';'. Only present if 'Source PIN Block Format Code' = '48'.
Destination PAN Delimiter	1 A	Value ';'. Always required.
Destination PAN	n N or 18 H or 12 N	<p>The PAN to be used to form the Destination PIN Block.</p> <p>If 'Destination PIN Block Format Code' is '48': The 12-19 digit Destination PAN.</p> <p>If present, the delimiter below must also be present.</p> <p>If 'Destination PIN Block Format Code' is '04': The 18 digit Destination PAN excluding the check digit. If the Destination PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left.</p> <p>For all other values of 'Destination PIN Block Format Code': The 12 right-most digits of the Destination PAN, excluding the check digit.</p>
Delimiter	1 A	Value ';'. Only present if 'Destination PIN Block Format Code' is '48'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'CD'.
Error Code	2 A	'00': No error '10': Source ZPK parity error '11': Destination ZPK parity error '17': PIN token translation disabled '68': Command disabled '69': PIN Block format has been disabled '88': Warning: PIN Block contains a zero length PIN or a standard error code.
PIN Length	2 N	Length of the returned PIN. Note: If the security setting "Return PIN length in PIN translation response" is "NO", this field will be set to "00".
Destination PIN block	16 H or 32 H	The destination PIN block encrypted under the Destination ZPK. When using a DES Destination ZPK, this field will be 16 H. When using an AES Destination ZPK, this field will be 32 H.
Destination PIN block format	2 N	As received in the command message.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate a PIN from TPK to ZPK/BDK Encryption (3DES DUKPT)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Translate a PIN from encryption under a TPK to encryption under an interchange key (ZPK) or a DUKPT key for transmission to another node. If the same PIN block format is defined, only the key is translated. Note that translation to BDK encryption is only permitted if the security setting "Enable PIN translation to BDK encryption" is "YES".

This command supports the translation of PIN blocks built using a Token instead of the real PAN. This functionality is only supported if the security setting "Enable use of Tokens in PIN Translation" is "YES".

For a list of PIN block formats permitted for use in this command, please refer to the *payShield 10K Host Programmer's Manual*.

Notes: The PIN block format may also be changed, but refer to the table below for restrictions.

The ANSI X9.24-1:2009 method for DUKPT key derivation is used when a 3DES BDK is supplied. This command does not support the use of an AES BDK.

3DES PIN encryption keys cannot be used with PIN block format code 48.

AES PIN encryption keys can only be used with PIN block format code 48.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'CA'.						
Source TPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The TPK under which the PIN block is currently encrypted.</p> <p>For a Variant LMK, the 'Source TPK' must be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y".</p> <p>For a Key Block LMK, the 'Source TPK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'P0', '71'</td><td>'D', 'T', 'A'</td><td>'B', 'D', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '71'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '71'	'D', 'T', 'A'	'B', 'D', 'N'						
Destination Key Flag	1 A	<p>For a Variant LMK only.</p> <p>Value '*' (X'2A). Optional; if present, this flag indicates that the destination key is a BDK-1.</p> <p>Value '~' (X'7E). Optional; if present, this flag indicates that the destination key is a BDK-2.</p>						
Destination Key	16/32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The key under which the PIN block is to be encrypted.</p> <p>Three types of keys are supported: ZPK, BDK-1 and BDK-2.</p> <p>For a Variant LMK:</p> <p>If 'Destination Key Flag' is not present, then this key must be a ZPK, encrypted under LMK 06-07.</p> <p>If 'Destination Key Flag' is '*', then this key must be a BDK-1, encrypted under LMK 28-29.</p> <p>If 'Destination Key Flag' is '~', then this key must be a BDK-2, encrypted under LMK 28-29/6.</p> <p>For a Key Block LMK:</p> <p>This key must be either a ZPK or BDK-1 or BDK-2, and comply with the following:</p>						

Field	Length & Type	Details		
		Key Usage	Algorithm	Mode of Use
		'P0', '72'	'D', 'T', 'A'	'B', 'E', 'N'
		'B0', '41'	'T'	'X', 'N'
Destination KSN Descriptor	3 H	Only present if the 'Destination Key' is a BDK-1 or BDK-2. The descriptor for the 'Destination KSN' (in the next field). 1st digit: Destination BDK Identifier Length ('0' – 'F') 2nd digit: Reserved. Should be '0'. 3rd digit: Device Identifier Length ('0' – 'F')		
Destination KSN	12 - 20 H	Only present if the 'Destination Key' is a BDK-1 or BDK-2. The Destination Key Serial Number, supplied by the host (emulating a DUKPT terminal).		
Maximum PIN Length	2 N	Valid range is '04' to '12'.		
Source PIN Block	16 H or 32 H	The source PIN block encrypted under the Source TPK. When using a DES Source TPK, this field will be 16 H. When using an AES Source TPK, this field will be 32 H.		
Source PIN Block Format Code	2 N	The format code for the 'Source PIN Block'. The format code for any currently enabled and permitted PIN block format may be specified.		
Destination PIN Block Format Code	2 N	The format code for the 'Destination PIN Block'. The format code for any currently enabled and permitted PIN block format may be specified, unless prohibited by one or more of the following security settings: <ul style="list-style-type: none">• "Restrict PIN block usage for PCI compliance"• "Enable PIN Block Format 34 as output format for PIN translations to ZPK"		

The following fields are required when the Source PIN Block and the Destination PIN Block use the same PAN.

Primary Account Number (PAN)	n N or 18 H or 12 N	The PAN that was used to form the Source PIN Block and to be used to form the Destination PIN Block. If 'Source PIN Block Format Code' or 'Destination PIN Block Format Code' is '48': The 12-19 digit PAN. If present, the delimiter below must also be present. If 'Source PIN Block Format Code' or 'Destination PIN Block Format Code' is '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'Source PIN Block Format Code' and 'Destination PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.
Delimiter	1 A	Value ';'. Only present if 'Source PIN Block Format Code' = '48' or 'Destination PIN Block Format Code' = '48'.

Field	Length & Type	Details
The following fields are required when the Source PIN Block was formed using a token PAN (instead of the real PAN), and the Destination PIN Block needs to be formed using the real PAN.		
Source PAN	n N or 18 H or 12 N	The PAN that was used to form the Source PIN Block. If 'Source PIN Block Format Code' is '48': The 12-19 digit Source PAN. If present, the delimiter below must also be present. If 'Source PIN Block Format Code' is '04': The 18 digit Source PAN excluding the check digit. If the Source PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'Source PIN Block Format Code': The 12 right-most digits of the Source PAN, excluding the check digit.
Delimiter	1 A	Value ';'. Only present if 'Source PIN Block Format Code' = '48'.
Destination PAN Delimiter	1 A	Value ';'. Always required.
Destination PAN	n N or 18 H or 12 N	The PAN to be used to form the Destination PIN Block. If 'Destination PIN Block Format Code' is '48': The 12-19 digit Destination PAN. If present, the delimiter below must also be present. If 'Destination PIN Block Format Code' is '04': The 18 digit Destination PAN excluding the check digit. If the Destination PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'Destination PIN Block Format Code': The 12 right-most digits of the Destination PAN, excluding the check digit.
Delimiter	1 A	Value ';'. Only present if 'Destination PIN Block Format Code' is '48'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'CB'.
Error Code	2 A	'00': No error '10': Source TPK parity error '11': Destination ZPK parity error '17': PIN translation disabled '68': Command disabled '69': PIN Block format has been disabled '88': Warning: PIN Block contains a zero length PIN or a standard error code.
PIN Length	2 N	Length of the returned PIN. Note: If the security setting "Return PIN length in PIN translation response" is "NO", this field will be set to "00".
Destination PIN block	16 H or 32 H	The destination PIN block encrypted under the Destination ZPK. When using a DES Destination ZPK, this field will be 16 H. When using an AES Destination ZPK, this field will be 32 H.
Destination PIN block format	2 N	As received in the command message.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate a PIN from ZPK to LMK Encryption

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Translate a PIN from encryption under a ZPK to encryption under the LMK.

Notes:

When used with a Variant LMK or 3DES Key Block LMK, the PIN encrypted under the LMK will always be using a non-ISO format, and so if the security setting "Restrict PIN block usage for PCI compliance" has the value "Y", this command will always fail with error 23 – regardless of the source PIN Block format.

3DES PIN encryption keys cannot be used with PIN block format code 48.

AES PIN encryption keys can only be used with PIN block format code 48.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'JE'.						
Source ZPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The ZPK under which the PIN block is currently encrypted. For a Variant LMK, the 'Source ZPK' must be encrypted under LMK pair 06-07.						
PIN Block	16 H or 32 H	For a Key Block LMK, the 'Source ZPK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '72'</td> <td>'D', 'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </table> The source PIN block encrypted under the Source ZPK. When using a DES Source ZPK, this field will be 16 H. When using an AES Source ZPK, this field will be 32 H.	Key Usage	Algorithm	Mode of Use	'P0', '72'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'D', 'T', 'A'	'B', 'D', 'N'						
PIN Block Format Code	2 N	One of the valid PIN block format codes.						
For a 3DES Variant or 3DES Key Block LMK, the following field must be present:								
Primary Account Number (PAN)	18 H or 12 N	The PAN, used to form the PIN Block. If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.						
For an AES Key Block LMK, the following two fields must be present:								
Primary Account Number (PAN)	n N	The PAN, used to form the PIN Block. The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.						
Delimiter	1 A	Value ':'.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'JF'.
Error Code	2 A	'00': No error '10': ZPK parity error '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
PIN	L N or L H or 'M' + 32 H	The PIN encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate a PIN from TPK to LMK Encryption

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Translate a PIN from encryption under a TPK to encryption under the LMK.

Notes:

- When used with a Variant LMK or 3DES Key Block LMK, the PIN encrypted under the LMK will always be using a non-ISO format, and so if the security setting "Restrict PIN block usage for PCI compliance" has the value "Y", this command will always fail with error 23 – regardless of the source PIN Block format.
- 3DES PIN encryption keys cannot be used with PIN block format code 48.
- AES PIN encryption keys can only be used with PIN block format code 48.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'JC'.						
Source TPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The TPK under which the PIN block is currently encrypted. For a Variant LMK, the 'Source TPK' must be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y". For a Key Block LMK, the 'Source TPK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '71'</td> <td>'D', 'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '71'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '71'	'D', 'T', 'A'	'B', 'D', 'N'						
PIN Block	16 H or 32 H	The source PIN block encrypted under the Source TPK. When using a DES Source TPK, this field will be 16 H. When using an AES Source TPK, this field will be 32 H.						
PIN Block Format Code	2 N	One of the valid PIN block format codes.						
For a 3DES Variant or 3DES Key Block LMK, the following field must be present:								
Primary Account Number (PAN)	18 H or 12 N	The PAN, used to form the PIN Block. If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.						
For an AES Key Block LMK, the following two fields must be present:								
Primary Account Number (PAN)	n N	The PAN, used to form the PIN Block. The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.						
Delimiter	1 A	Value ':'.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'JD'.
Error Code	2 A	'00': No error '10': TPK parity error '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
PIN	L N or L H or 'M' + 32 H	The PIN encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate a PIN from LMK to ZPK Encryption

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Translate a PIN from encryption under the LMK to encryption under a ZPK.

Notes: 3DES PIN encryption keys cannot be used with PIN block format code 48.
AES PIN encryption keys can only be used with PIN block format code 48.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'JG'.						
Destination ZPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The ZPK under which the PIN block is to be encrypted. For a Variant LMK, the 'Destination ZPK' must be encrypted under LMK pair 06-07.						
PIN Block Format Code	2 N	For a Key Block LMK, the 'Destination ZPK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '72'</td> <td>'D', 'T', 'A'</td> <td>'B', 'E', 'N'</td> </tr> </table> The format code required for the output PIN Block. The code for any currently enabled and permitted PIN block format may be specified, unless prohibited by the following security settings: <ul style="list-style-type: none"> • "Restrict PIN block usage for PCI compliance" 	Key Usage	Algorithm	Mode of Use	'P0', '72'	'D', 'T', 'A'	'B', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'D', 'T', 'A'	'B', 'E', 'N'						
For a 3DES Variant or 3DES Key Block LMK, the following field must be present:								
Primary Account Number (PAN)	18 H or 12 N	The PAN, used to form the PIN Block. If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.						
For an AES Key Block LMK, the following two fields must be present:								
Primary Account Number (PAN)	n N	The PAN, used to form the PIN Block.						
Delimiter	1 A	The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present. Value ';'.						
PIN	L N or L H or 'M' + 32 H	The PIN encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'JH'.
Error Code	2 A	'00': No error '11': ZPK parity error '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
PIN Block	16 H or 32 H	The PIN block encrypted under the Destination ZPK. When using a DES Destination ZPK, this field will be 16 H. When using an AES Destination ZPK, this field will be 32 H.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate PIN Algorithm

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Translate a PIN from encryption using the Visa PIN algorithm to encryption using the Racal algorithm.

This command can only be used when using a Variant LMK or a 3DES Key Block LMK.

Notes: The HSM must be configured for the Racal algorithm.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'BQ'.
Primary Account Number (PAN)	12 N	The 12 right-most digits of the PAN, excluding the check digit.
PIN	L N	The PIN encrypted under the LMK using the Visa algorithm.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'BR'.
Error Code	2 A	'00': No error '17': Racal PIN Algorithm is not enabled '68': Command disabled or a standard error code.
PIN	L H	The PIN encrypted under the LMK using the Racal algorithm.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate Account Number for LMK-encrypted PIN

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To translate the account number for a PIN encrypted under LMK 02-03 from an old account number to a new account number. The customer PIN itself remains unchanged. Note that the security setting "*Enable translation of account number for LMK encrypted PINs*" must be set to "Y" to enable this command.

Notes: Note that when used with a 3DES LMK, the LMK-encrypted PIN is not simply the PIN encrypted under the LMK. It is encrypted using a proprietary algorithm involving the account number. Thus the LMK-encrypted PIN changes when the account number is changed.

When using an AES Key Block LMK, the LMK-encrypted PIN is the result of encrypting the PIN under the LMK using Thales PIN Block format 48 (ISO PIN Block format 4).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'QK'.
PIN	L N or L H or 'M' + 32 H	The PIN encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
Old Primary Account Number (PAN)	12 N	If a 3DES Key Block or Variant LMK is used: The 12 right-most digits of the old PAN, excluding the check digit.
	or n N	If an AES Key Block LMK is used: The full 12-19 digit old PAN, including the check digit. If present, the delimiter below must also be present.
Delimiter	1 A	Value ';'. Only present if an AES Key Block LMK is used.
New Primary Account Number (PAN)	12 N	If a 3DES Key Block or Variant LMK is used: The 12 right-most digits of the new PAN, excluding the check digit.
	or n N	If an AES Key Block LMK is used: The full 12-19 digit new PAN, including the check digit. If present, the delimiter below must also be present.
Delimiter	1 A	Value ';'. Only present if an AES Key Block LMK is used.
Delimiter LMK Identifier	1 A 2 N	Value '%'. Optional; if present, the following field must also be present. LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter Message Trailer	1 C n A	Must be present if a message trailer is present. Value X'19. Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'QL'.
Error Code	2 A	'00': No error '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
PIN	L N or L H or 'M' + 32 H	The PIN encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate an RSA-encrypted PIN to a ZPK or TPK-encrypted PIN

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	



THE USE OF THIS COMMAND PRESENTS A SIGNIFICANT SECURITY RISK. CONTROLS SHOULD BE IN PLACE TO CONTROL A PUBLIC KEY USED TO PROTECT PINS.

Function: Translate an RSA-encrypted (source) PIN to a ZPK or TPK encrypted (destination) PIN.

Notes: Translates an RSA-encrypted (source) PIN to a 3DES ZPK or TPK encrypted (destination) PIN. This command will be similar to the 'GI' host command, but instead of returning the decrypted data in the clear, this command decrypts the RSA-encrypted PIN and re-encrypts it under the supplied ZPK or TPK. PIN Block source and destination formats have been restricted to those enabled by default for PCI Compliance.

This command supports the translation of PIN blocks built using a Token instead of the real PAN. This functionality is only supported if the security setting "*Enable use of Tokens in PIN Translation*" has the value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AQ'.
Pad Mode Identifier	2 N	Identifier of the Pad Mode used in the encryption process: '01': PKCS#1 v1.5 method (EME-PKCS1-v1_5) '02': PKCS#1 v2.2 OAEP method (EME-OAEP-ENCODE)
Mask Generation Function	2 N	Identifier of the mask generation function: '01': MGF1 as defined in PKCS#1 v2.2. Optional, only present if Pad Mode Identifier = '02' (OAEP).
MGF Hash Function	2 N	Identifier of the MGF Hash Function: '01': SHA-1 '05': SHA-224 '06': SHA-256 '07': SHA-384 '08': SHA-512 Optional, only present if Pad Mode Identifier = '02' (OAEP). This field defines the hash function to be used in the MGF.
OAEP Encoding Parameters Length	2 N	Optional, only present if Pad Mode Identifier = '02' (OAEP).
OAEP Encoding Parameters	n B	Optional, only present if Pad Mode Identifier = '02' (OAEP). If present, this field should be encoded according to PKCS#1 v2.2 §A.2. The HSM does not interpret or validate the contents of this field. If OAEP padding is used, but no Encoding Parameters are provided, then OAEP Parameters Length should be '00', and this field will be empty.
OAEP Encoding Parameters Delimiter	1 A	Value ';'.
Encrypted PIN Block Length	4 N	The length of the PIN Block
PIN Block Encrypted under Public Key	n B	The PIN Block Encrypted under the Public Key.
Delimiter	1 A	Value ';'.
		Used to indicate the end of the Data Block Field

Field	Length & Type	Details						
Private Key Flag	2 N	Flag to indicate location of the Private key: If flag = '99' use Private key provided with command else flag = index of stored Issuer Private key.						
Private Key Length		Length of the Private Key. Only present if Private Key Flag = '99'.						
	4 N	For a Variant LMK, the length, in bytes, of the Private Key field. Note: the Private Key must have been generated with Key Type = '5'.						
	or 4 H	For a Key Block LMK, this field is ignored and should be set to 'FFFF'.						
Private Key		The Private Key. Only present if Private Key Flag = '99'.						
	n B	For a Variant LMK, the Private Key is encrypted under LMK 34-35.						
	or 'S' + n B	For a Key Block LMK, the Private Key must comply with:						
		<table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'05'</td> <td>'R'</td> <td>'D', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'05'	'R'	'D', 'N'
Key Usage	Algorithm	Mode of Use						
'05'	'R'	'D', 'N'						
Destination Key Flag	1 N	'0': ZPK '1': TPK						
ZPK		Only present if Destination Key Flag = '0'. The ZPK under which the PIN block is to be encrypted.						
	16 H or 'U' + 32 H or 'T' + 48 H	For a Variant LMK, the ZPK must be encrypted under LMK pair 06-07.						
	or 'S' + n A	For a Key Block LMK, the ZPK must comply with the following:						
		<table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'P0', '72'</td> <td>'D', 'T'</td> <td>'B', 'E', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'P0', '72'	'D', 'T'	'B', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'D', 'T'	'B', 'E', 'N'						
TPK		Only present if Destination Key Flag = '1'. The TPK under which the PIN block is to be encrypted.						
	16 H or 'U' + 32 H or 'T' + 48 H	For a Variant LMK, the TPK must be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y".						
	or 'S' + n A	For a Key Block LMK, the TPK must comply with the following:						
		<table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'P0', '71'</td> <td>'D', 'T'</td> <td>'B', 'E', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'P0', '71'	'D', 'T'	'B', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '71'	'D', 'T'	'B', 'E', 'N'						
Source PIN Block Format Code	2 N	The format code for the source PIN Block. Only these Thales PIN Block formats are supported: '01': ISO 9564-1 & ANSI X9.8 format 0 '05': ISO 9564-1 format 1 '47': ISO 9564-1 & ANSI X9.8 format 3						
Destination PIN Block Format Code	2 N	The format code for the destination PIN block. The choice of destination PIN Block Format is restricted if the security setting "Restrict PIN block usage for PCI compliance" has the value "Y" – see the <i>payShield 10K Host Programmer's manual</i> 's chapter on PCI HSM Compliance.						
Primary Account Number (PAN) or Token	18 H or 12 N	If 'Source PIN Block Format Code' uses a token instead of the actual PAN, this field will contain the token number. Otherwise, it will contain the real PAN. If 'Source PIN Block Format Code' = '04': The 18 digit PAN/Token excluding the check digit. If the PAN/Token is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'Source PIN Block Format Code': The 12 right-most digits of the PAN/Token, excluding the check digit.						

payShield 10K Core Host Commands

Field	Length & Type	Details
The following fields are required when the Source PIN Block was formed using a token (instead of the real PAN), and the Destination PIN Block needs to be formed using the real PAN.		
Destination PAN Delimiter	1 A	Value ':'. Optional; if present, the following field must also be present.
Destination PAN	18 N or 12 N	Only present if 'Destination PAN Delimiter' is present. If 'Destination PIN Block Format Code' = '04': The 18 digit Destination PAN excluding the check digit. If the Destination PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'Destination PIN Block Format Code': The 12 right-most digits of the Destination PAN, excluding the check digit.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'AR'.
Error Code	2 N	'00': No error '17': PIN token translation disabled '68': Command disabled '69': PIN Block format has been disabled '88': OAEP parameter not defined or OAEP parameter delimiter missing or a standard error code.
PIN Length	2 N	Length of the translated PIN. Note: If the security setting "Return PIN length in PIN translation response" is "NO", this field will be set to "00".
PIN Block	16 H	The PIN block encrypted under the interchange key and formatted according to the destination PIN block format code.
Destination PIN block format code	2 N	Returned to the Host unchanged
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Load OPINPad to HSM Memory

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not Required	

Function: To store OPINPad into HSM memory using index GUID.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'P6'.
PAD ID	32 H	The PAD Identifier.
PAD Lifetime	3 N	The lifetime of the PAG0 D in seconds.
PIN Length	2 N	The length of the PIN that the PAD can decode: Valid values from '04' up to '12' characters.
Keys (substitution arrays)	n A	The Substitution keys ({PIN Length} x 10 x 2)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'P7'.
Error Code	2 A	'00': No error '50': Key length incorrect '51': Invalid substitution 2 inputs to 1 output '52': Invalid substitution 1 input to 2 outputs '53': GUID exists or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Decode OPIN and translate to ZPK

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Required	
Activity: command.p8.host	

Function: Decode OPIN and translate it to a PIN block encrypted under a ZPK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'P8'.
PAD ID	32 H	The PAD Identifier
OPIN length	2 N	The length of the obfuscated PIN Valid values from '4' up to '12' characters
OPIN	n N	The source obfuscated PINPIN from the Pad
Destination ZPK	'U' + 32 H or 'T' + 48 H	The ZPK under which the PIN block is to be encrypted. For a Variant LMK, the 'Destination ZPK' must be encrypted under LMK pair 06-07. 'U' indicates Double length Key 'T' indicates Triple length key
Destination PIN Block Format Code	2 N	The format code for the destination PIN block. The choice of destination PIN Block Format is restricted if the security setting "Restrict PIN block usage for PCI compliance" has the value "Y" – see the <i>payShield 10K Host Programmer's manual</i> 's chapter on PCI HSM Compliance. '01': ANSI X.98 '02': Docutel '03': Diebold '04': PLUS '05': ISO 9564-1
Primary Account Number (PAN)	18 H or 12 N	If 'Destination PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'Destination PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'P9'.
Error Code	2 A	'00': No error '11': Destination ZPK parity error '51': Identified PIN PAD not found '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
PIN Block	16 H	The PIN block encrypted under the ZPK and formatted according to the Destination PIN Block Format Code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

5.4 Card Verification Code/Value Commands

The Card Verification Value (CVV) is a cryptographic check value derived from specific fields of data, such as account number, card expiration date, service code, and keys (CVKs).

The CVV is written onto the card. During transactions it is sent to the HSM which recalculates the CVV and compares it with the received CVV to confirm the validity of the card.

The payShield 10K provides the following host commands to support card verification code/value operations:

Function	Command	Page
<i>Verify a Card Verification Code/Value</i>	CY (CZ)	355
<i>Generate a Dynamic CVV</i>	QY (QZ)	358
<i>Verify a Dynamic CVV/CVC</i>	PM (PN)	360
<i>Verify Card Security Codes</i>	RY (RZ)	368

Verify a Card Verification Code/Value

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a Card Verification Code or Value.

Notes: Used to verify a payment card's verification code/value.

This command can also be used to verify:

- the Visa CVV1 or Mastercard CVC1 encoded onto the card's magnetic stripe.
- the Visa CVV2 or Mastercard CVC2 printed on a card's signature strip. In this case, the Service Code field should be set to "000".
- the Visa iCVV or Mastercard Chip CVC included on an EMV chip card. In this case, the Service Code field should be set to "999".
- the Visa CAVV or Mastercard AVV or Discover OTPK used in the 3-D Secure environment. In this case:

The Expiration date is replaced by a 4-digit Unpredictable number calculated from the Transaction Identifier, as defined in the 3-D Secure process.

The Service Code is replaced by the following 2 fields:

- A 1-digit Authentication Results Code, as defined for the 3-D Secure process
- A 2-digit Second Factor Authentication Results Code, as defined for the 3-D Secure process

Field	Length & Type	Details												
COMMAND MESSAGE														
Message Header	m A	Subsequently returned to the Host unchanged.												
Command Code	2 A	Value 'CY'.												
CVK	32 H or 'U' + 32 H	<p>For a Variant LMK: If Scheme ID is not specified, the 'CVK' must be encrypted under LMK pair 14-15 variant 4. If Scheme ID = '0' and OTPK Key Derivation Method = '0' or '1', then the 'CVK' must be encrypted under LMK pair 28-29 variant 1.</p> <p>For a Key Block LMK: If Scheme ID is not specified, the 'CVK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'C0', '12', '13'</td><td>'T'</td><td>'C', 'V', 'N'</td></tr> </table> <p>If Scheme ID = '0' and OTPK Key Derivation Method = '0' or '1', then the 'CVK' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'E0'</td><td>'T'</td><td>'X', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'C0', '12', '13'	'T'	'C', 'V', 'N'	Key Usage	Algorithm	Mode of Use	'E0'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use												
'C0', '12', '13'	'T'	'C', 'V', 'N'												
Key Usage	Algorithm	Mode of Use												
'E0'	'T'	'X', 'N'												
CVV	3 N	CVV for verification.												
If specifying the CVV data as a single parameter, the following 2 fields must be present.														
CVV Data Delimiter	1 A	Value '#'. Optional; if present, the following field CVV Data must be present.												
CVV Data	32 N	Card Verification Value data from which the CVV is generated.												
If specifying the CVV data using separate parameters, the following 6 fields must be present.														
Primary account number	n N	The PAN for the card; max 19 digits.												
Delimiter	1 A	Value ';'.												
Expiration date	4 N	The card expiration date (or Unpredictable Number for CAVV/AAV).												
Service code	3 N	The card service code (or Authentication Results Code (1 digit) + Second factor Authentication Results Code (2 digits) for CAVV / AAV).												
Delimiter	1 A	Value '!'. Optional. If present, the following fields must be present.												
Scheme ID	1 N	Only present if the preceding delimiter is present. '0': Discover OTPK												
OTPK Key Derivation Method	1 A	<p>Only present if Scheme ID = '0':</p> <p>'0': Default EMV or Server PIN based white box using IMK AC, EMV 4.3 option A, EMV CSK</p> <p>'1': Local CVM using IMK AC, EMV 4.3 option A, EMV CSK and further EMV CSK using CVD</p> <p>'2': Default EMV or Server PIN based white box using CVK, EMV 4.3 option A, EMV CSK</p> <p>'3': Local CVM using CVK, EMV 4.3 option A, EMV CSK and further EMV CSK using CVD</p>												
ATC	2 B	Only present if Scheme ID = '0': Application Transaction Counter.												
PSN	2 N	Only present if Scheme ID = '0': The PAN Sequence Number.												
CVD	3 B	Only present if Scheme ID = '0' and OTPK Key Derivation Method = '1' or '3': Card Verification Data.												
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.												
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.												
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.												
Message Trailer	n A	Optional. Maximum length 32 characters.												

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'CZ'.
Error Code	2 A	'00': No error '01': CVV failed verification '10': CVK A or B parity error '27': CVK not double length '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a Dynamic CVV

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate a Dynamic Card Verification Value (dCVV).

Notes: This command supports schemes for generating a dCVV.

The Visa dCVV (Scheme ID='0', will always append a zero byte to the supplied PAN when generating the DK-DCVV).

For Scheme ID = '0', the only acceptable value for the Service Code is "998". All other values will result in error code 07 being returned.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'QY'.						
Scheme ID	1 N	Identifier for Card Scheme: '0': Visa dCVV '1': Visa Authentication Value (AV) '2': Reserved '3': Reserved '4': Reserved '5': Visa dCVV2 Time Based '6' ... '9': Reserved for future use.						
Master Key	32 H or 'U' + 32 H or T' + 48 H or 'S' + n A	<p>Master Key from which card-unique key is derived.</p> <p>For a Variant LMK: For scheme ID = '0' or '1', the 'Master Key' must be a MK-AC, encrypted under LMK 28-29 variant 1.</p> <p>For a Key Block LMK: For scheme ID = '0' or '1', the 'Master Key' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'E0'</td> <td>'T'</td> <td>'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'E0'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E0'	'T'	'X', 'N'						
Key Derivation Method	1 A	Method to be used to derive a card-unique key from the Master Key: 'A': EMV 4.1 Book 2 Option A method 'B': EMV 4.1 Book 2 Option B method.						
Primary Account Number (PAN)	n N	The primary account number. The maximum PAN Length for Scheme '0' or '1' (Visa) is 19 digits.						
Delimiter	1 A	Value ';'.						
		Identifies the end of the PAN field.						

Field	Length & Type	Details
The following section applies only when Scheme '0' (Visa dCVV)		
1) Expiration Date	4 N	The Card Expiry Date.
2) Service Code	3 N	The Service Code to be used for dCVV generation. NOTE: must be '998' for Scheme 0 (Visa).
3) ATC	6 N	Application Transaction Counter. If the ATC provided on Track 2 is less than 6 digits, it should be right justified and padded on the left with zeros.
The following section applies only when Scheme '1' (Visa AV)		
1) Transaction Data Length	2 H	Length of the next field. Can be any length from 1 to 255 bytes.
2) Transaction Data	n B	Variable length data. If the data supplied is a multiple of 8 bytes, no extra padding is added. If it is not a multiple of 8 bytes, additional zero padding is added.
3) Delimiter	1 A	Delimiter, to indicate the end of Transaction Data. Value ':'.
The following section applies only when Scheme '5' (Visa dCVV2)		
1) Expiration Date	4 N	Expiration Date (YYMM format)
2) TWU	6 N	Time Window Unit (in seconds)
3) Current Time	8 H	Time in seconds since 00:00:00 1st January 1970
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'QZ'.
Error Code	2 A	'00': No error '05': Unrecognized Scheme or Key Derivation Method '07': Invalid Service Code '10': Master Key Parity Error or a standard error code.
The following section applies only when using Scheme '0'.		
dCVV	3 N	The calculated dCVV.
The following section applies only when using Scheme '1'.		
AV	8 B	The calculated Authentication Value cryptogram.
The following section applies only when using Scheme '5'.		
dCVV2	3 N	The calculated dCVV2.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a Dynamic CVV/CVC

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Optional (see text)	
Activity: diag.host	

Function: Verify a dynamically generated card verification value.

Notes: The EMV "Track 2 Equivalent Data", provided in the authorization message and originating from the contactless smart card, is the source for the following data fields for the PM Function:

- PAN
- Expiration Date
- Service Code
- ATC
- DCVV

Notes for the various different supported methods are below:

Visa (dCVV)	The PAN sequence number is assumed to be zero for the calculation of the UDK. This command will append a zero to the supplied PAN when generating the <i>DK-AC</i> .
Visa (dCVV2)	This function verifies a time-based dynamic card verification value, using the Visa dCVV2 algorithm. The MK-DCVV master key is used to derive a card key using derivation data, and a dCVV2 is calculated and compared to the supplied dCVV2.
Visa (LUC)	The Visa cloud-based payments method uses a Limited Use Key (LUK) to create a Limited Use Cryptogram (LUC).
Mastercard (CVC3)	If the PAN sequence number is omitted, this command will append a zero to the supplied PAN when generating the DK-CVC3. Verification of the CVC3 requires the IVCVC3 which is a MAC calculated over the static part of Track1 or Track2 data using the DK-CVC3. This command offers the option of providing this parameter for verification of the CVC3 or it can create the IVCVC3 during the verification process if the appropriate Track Data is provided.
Mastercard (PINCVC3)	This is a variant of the standard CVC3 scheme. A Mobile Mastercard PayPass M/Chip application generates a PINCVC3 instead of a CVC3 when the PIN has been entered on the mobile device. A different IV (known as a PINIVCVC3) is used in this calculation. The calculation of the PINCVC3 is otherwise identical to the CVC3.
American Express	The American Express contactless scheme uses a dynamically generated 5-digit cryptogram.

ExpressPay Cryptogram	
Discover ZIP (DCVV & DCVV Plus & OTPK)	The DCVV & OTPK methods use a 3-digit cryptogram. The DCVV Plus method uses a variable-length cryptogram.
Oberthur (OdCVV)	This function verifies a time-based dynamic card verification value, using the OATH algorithm. The MK-DCVV master key is used to derive a card key using derivation data, and an OdCVV is calculated and compared to the supplied OdCVV. The Oberthur method uses an AES MK-DCVV, and therefore requires the use of an (AES) Key Block LMK. This method is not supported under the Variant LMK scheme.
JCB Dynamic CAV	This function verifies a dynamic CAV using the Dynamic CAV session key.
Gemalto dCV	This function verifies a time-based dynamic card verification value, using the OATH algorithm, as defined by the Gemalto Optelio dCV specification.

To assist in development of host applications, the calculated Dynamic CVV will be provided in the response data if Error Code 01 is returned and the HSM is in Authorized State.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'PM'.
Scheme ID	1 N	Identifier for Card Scheme: '0': Visa '1': Mastercard '2': American Express '3': Discover '4': Oberthur '5': Visa dCVV2 '6': JCB Contactless Mobile Payment Application '7': Gemalto dCV '8' ... '9': Reserved for future use.
Version	1 N	<p>For Scheme ID = '0': '0': Visa DCVV verification '1': Visa LUC verification '2': Visa LUC verification with host provided value '3': Visa LUC verification with consumer device reporting</p> <p>For Scheme ID = '1': '0': Mastercard PayPass CVC3 verification. IVCVC3 provided in input (PSN=00). '1': Mastercard PayPass CVC3 verification. PSN and IVCVC3 provided in input. '2': Mastercard PayPass CVC3 verification. PSN provided in input and IVCVC3 calculated from provided magnetic stripe data. '3': Mastercard PayPass PINCVC3 verification. PSN provided in input and PINIVCVC3 calculated from provided magnetic stripe data. '4': Mastercard HCE CVC3 verification. PSN provided in input and PINIVCVC3 calculated from provided magnetic stripe data.</p> <p>For Scheme ID = '2': '0': American Express ExpressPay verification as defined in ExpressPay 2.0 specifications.</p> <p>For Scheme ID = '3': '0': Discover ZIP DCVV '1': Discover ZIP DCVV Plus '2': Discover OTPK</p> <p>For Scheme ID = '4': '0': Oberthur OdCVV</p> <p>For Scheme ID = '5': '0': Visa dCVV2</p> <p>For Scheme ID = '6': '0': JCB J-Speedy verification method as defined in JCB IC Card Application Specification v3.0.</p> <p>For Scheme ID = '7': '0': Gemalto Optelio dCV</p> <p>Other values are RFU.</p> <p>Master Key from which card-unique key is derived.</p>
MK-DCVV	32 H or 'U' + 32 H or 'T' + 48 H	<p>For a Variant LMK:</p> <p>For Scheme ID = '0', '2' or '5', the 'MK-DCVV' must be a MK-AC, encrypted under LMK 28-29 variant 1.</p> <p>For Scheme ID = '1', the 'MK-DCVV' must be a MK-CVC3, encrypted under LMK 28-29 variant 7.</p> <p>For Scheme ID = '1' and Version = '4', then MK-DCVV must be the MK-AC encrypted under LMK 28-29 variant 1.</p> <p>For Scheme ID = '3' and Version = '0' or '1', the 'MK-DCVV' must be a MK-CVC3, encrypted under LMK 28-29 variant 7.</p> <p>For Scheme ID = '3' and Version = '2' and Key Derivation Method = '6', the MK-DCVV must be encrypted under LMK 28-29 variant 7.</p> <p>For Scheme ID = '6' and Version = '0', the 'MK-DCVV' must be encrypted under LMK 28-29 variant 7.</p> <p>For Scheme ID = '7', the 'MK-DCVV' must be a MK-CVC3, encrypted under LMK 28-29 variant 7.</p>

Field	Length & Type	Details																																																						
	or 'S' + n A	<p>For a Key Block LMK:</p> <p>For scheme ID = '0', '2' or '5', the 'MK-DCVV' must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'E0'</td><td>'T'</td><td>'X', 'N'</td></tr> </tbody> </table> <p>For scheme ID = '1' and Version ≠ '4', the 'MK-DCVV' must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'E6'</td><td>'T'</td><td>'X', 'N'</td></tr> <tr> <td>'32'</td><td>'T'</td><td>'N'</td></tr> </tbody> </table> <p>For scheme ID = '1' and Version = '4', the 'MK-DCVV' must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'E0'</td><td>'T'</td><td>'X', 'N'</td></tr> </tbody> </table> <p>For scheme ID = '3', the 'MK-DCVV' must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'E0', 'E6'</td><td>'T'</td><td>'X', 'N'</td></tr> <tr> <td>'32'</td><td>'T'</td><td>'N'</td></tr> </tbody> </table> <p>For scheme ID = '4', the 'MK-DCVV' must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'E6'</td><td>'A'</td><td>'X', 'N'</td></tr> <tr> <td>'32'</td><td>'A'</td><td>'N'</td></tr> </tbody> </table> <p>For scheme ID = '6', the 'MK-DCVV' must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'E6'</td><td>'T'</td><td>'X', 'N'</td></tr> </tbody> </table> <p>For scheme ID = '7', the 'MK-DCVV' must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'E6'</td><td>'T'</td><td>'X', 'N'</td></tr> <tr> <td>'32'</td><td>'T'</td><td>'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'E0'	'T'	'X', 'N'	Key Usage	Algorithm	Mode of Use	'E6'	'T'	'X', 'N'	'32'	'T'	'N'	Key Usage	Algorithm	Mode of Use	'E0'	'T'	'X', 'N'	Key Usage	Algorithm	Mode of Use	'E0', 'E6'	'T'	'X', 'N'	'32'	'T'	'N'	Key Usage	Algorithm	Mode of Use	'E6'	'A'	'X', 'N'	'32'	'A'	'N'	Key Usage	Algorithm	Mode of Use	'E6'	'T'	'X', 'N'	Key Usage	Algorithm	Mode of Use	'E6'	'T'	'X', 'N'	'32'	'T'	'N'
Key Usage	Algorithm	Mode of Use																																																						
'E0'	'T'	'X', 'N'																																																						
Key Usage	Algorithm	Mode of Use																																																						
'E6'	'T'	'X', 'N'																																																						
'32'	'T'	'N'																																																						
Key Usage	Algorithm	Mode of Use																																																						
'E0'	'T'	'X', 'N'																																																						
Key Usage	Algorithm	Mode of Use																																																						
'E0', 'E6'	'T'	'X', 'N'																																																						
'32'	'T'	'N'																																																						
Key Usage	Algorithm	Mode of Use																																																						
'E6'	'A'	'X', 'N'																																																						
'32'	'A'	'N'																																																						
Key Usage	Algorithm	Mode of Use																																																						
'E6'	'T'	'X', 'N'																																																						
Key Usage	Algorithm	Mode of Use																																																						
'E6'	'T'	'X', 'N'																																																						
'32'	'T'	'N'																																																						
Key Derivation Method	1 A	<p>Method to be used to derive a card-unique key from the Master Key:</p> <p>For Scheme ID = '0', '1' (Version ≠ '4'), '2', '5' or '7':</p> <ul style="list-style-type: none"> 'A': EMV 4.1 Book 2 Option A method 'B': EMV 4.1 Book 2 Option B method. <p>For Scheme ID = '1' and Version = '4':</p> <ul style="list-style-type: none"> '4': Derive card-unique key from the Master Key using EMV 4.1 Book 2 Option A and then derive the session key using EMV Common Session Key derivation. <p>For Scheme ID = '3' and Version = '0' or '1':</p> <ul style="list-style-type: none"> '2': 16-byte Account Unique Key for DCVV (AUK DCVV) '3': 24-byte Account Unique Key for DCVV (AUK DCVV) <p>For Scheme ID = '3' and Version = '2':</p> <ul style="list-style-type: none"> '5': Default EMV or Server PIN based white box using MK AC, EMV 4.3 option A, EMV CSK '6': Enhanced DCVV OTPK or Server PIN based white box using AUK DCVV and EMV CSK <p>For Scheme ID = '4':</p> <ul style="list-style-type: none"> '7': Oberthur Key Derivation Method <p>For Scheme ID = '6' and Version = '0':</p> <ul style="list-style-type: none"> 'A': EMV Option 'A' Method and JCB Session Key Derivation 																																																						
Primary Account Number (PAN)	n N	<p>The primary account number for the card.</p>																																																						
	or 20 N	<p>The maximum PAN length for Scheme ID = '0' is 16 digits.</p> <p>The maximum PAN length for Scheme ID = '1' is 19 digits.</p> <p>If Key Derivation Method = '5', the maximum PAN length is 19 digits.</p>																																																						
	or 16 N	<p>If Key Derivation Method = '2', '3' or '6': Concatenation of the 16-digit Primary Account Number and 4-digit Expiration Date for the card.</p>																																																						
Delimiter	1 A	<p>If Scheme ID = '6', this field consists of 16 digits.</p> <p>Value ':'. Identifies the end of the PAN field.</p>																																																						

Field	Length & Type	Details
PAN Sequence No.	2 N	<p>Only present for:</p> <p>Scheme ID = '0' & Version = '3' Scheme ID = '1' & Version = '1', '2', '3' or '4' Scheme ID = '2' Scheme ID = '3' & Version = '2' & Key Derivation Method = '5' Scheme ID = '4' Scheme ID = '6' Scheme ID = '7'</p> <p>The Sequence Number for the card.</p> <p>If the Sequence Number is not available it should be specified as '00'.</p>
Modified PSN Flag	1 N	<p>Only present when Scheme ID = '1' and Version = '4'.</p> <p>'0': Unmodified PAN Sequence No in input. '1': Modified PAN Sequence No in input.</p>
The following section applies only when using Scheme '0' (Visa) and Version '0' (DCVV).		
1) Expiration Date	4 N	The Card Expiry Date.
2) Service Code	3 N	The Card's Track 2 Service Code.
3) ATC	6 N	<p>Application Transaction Counter.</p> <p>If the ATC provided on Track 2 is less than 6 digits, it should be right justified and padded on the left with zeros.</p>
4) dCVV	3 N	The dCVV to be validated.
The following section applies only when using Scheme '0' (Visa) and Version '1' (LUC).		
1) YHHHHCC	7 N	<p>The Year/Hour/Counter value used to derive the Limited Use Key (LUK) that produced the Limited Use Cryptogram (LUC). Consists of 7 decimal digits, concatenated as follows:</p> <p>Y (0-9) : least significant digit of current year HHHH (0001-8784) : number of hours since Jan 1st CC (00-99) : counter</p>
2) LUC	6 N	Cryptogram to be validated.
The following section applies only when using Scheme '0' (Visa) and Version '2' (LUC w/ host value).		
1) YHHHHCC	7 N	<p>The Year/Hour/Counter value used to derive the Limited Use Key (LUK) that produced the Limited Use Cryptogram (LUC). Consists of 7 decimal digits, concatenated as follows:</p> <p>Y (0-9) : least significant digit of current year HHHH (0001-8784) : number of hours since Jan 1st CC (00-99) : counter</p>
2) Value for LUC	16 N	Value for generation of the cryptogram using LUK.
3) LUC	3 N	Cryptogram to be validated.
The following section applies only when using Scheme '0' (Visa) and Version '3' (LUC w/ consumer dev reporting).		
1) YHHHHCC	7 N	<p>The Year/Hour/Counter value used to derive the Limited Use Key (LUK) that produced the Limited Use Cryptogram (LUC). Consists of 7 decimal digits, concatenated as follows:</p> <p>Y (0-9) : least significant digit of current year HHHH (0001-8784) : number of hours since Jan 1st CC (00-99) : counter</p>
2) Vulnerability Level	1 N	<p>Check for consumer device state reporting when validating the LUC. Valid values are as follows:</p> <p>'0': Normal state '1': Vulnerable state</p>
3) ATC	5 N	<p>Application Transaction Counter.</p> <p>Note the rightmost (least significant) four digits of the ATC will be used in cryptogram validation.</p>
4) LUC	3 N	Cryptogram to be validated.

Field	Length & Type	Details
The following section applies only when using Scheme '1' (Mastercard) and Version '0' & '1'.		
1) IVCVC3	5 N	The issuer proprietary static data element. Max value '65535' (2 byte field).
2) Unpredictable Number	10 N or 8 D	Random number provided to the card by the terminal during a PayPass transaction. Either format results in a 4-byte binary number being used. The HSM determines the length (and then infers the type) of this field by examining the number of characters supplied to this command. Example: To use a 4-byte value of 0x00000256, this field can be supplied with either of the following values: BCD Format: 8 D -- "00000256" → 0x00000256 Decimal Format: 10 N -- "0000000598" → 0x00000256
3) ATC	5 N	Decimal value of Application Transaction Counter. Max value '65535' (2 byte field).
4) CVC3/PINCVC3	5 A	The CVC3 or PINCVC3 to be validated. This field may contain leading 'X' characters, which indicate that the CVC3/PINCVC3 contains less than 5 digits. The 'X' characters are not part of the comparison with the calculated CVC3/PINCVC3. For example, a CVC3/PINCVC3 of 'XX123' matches with a Calculated CVC3/PINCVC3 of '87123'. Max value '65535' (decimal representation of a 2 byte value).
The following section applies only when using Scheme '1' (Mastercard) and Version '2' & '3'.		
1a) Track Data Length	3 N	The length of the following field.
1b) Track Data	n B	Static Track (1 or 2) Data.
2) Unpredictable Number	10 N or 8 D	Random number provided to the card by the terminal during a PayPass transaction. Either format results in a 4-byte binary number being used. Max. value '4294967295' (4 byte field).
3) ATC	5 N	Decimal value of Application Transaction Counter. Max value '65535' (2 byte field).
4) CVC3/PINCVC3	5 A	The CVC3 or PINCVC3 to be validated. This field may contain leading 'X' characters, which indicate that the CVC3/PINCVC3 contains less than 5 digits. The 'X' characters are not part of the comparison with the calculated CVC3/PINCVC3. For example, a CVC3/PINCVC3 of 'XX123' matches with a Calculated CVC3/PINCVC3 of '87123'. Max value '65535' (decimal representation of a 2 byte value).
The following section applies only when using Scheme '1' (Mastercard) and Version '4'.		
1a) Track Data Length	3 N	The length of the following field.
1b) Track Data	n B	Static Track (1 or 2) Data.
2) Unpredictable Number	10 N or 8 D	Random number provided to the card by the terminal during a PayPass transaction. Either format results in a 4-byte binary number being used. Max. value '4294967295' (4 byte field).
3) ATC	5 N	Decimal value of Application Transaction Counter. Max value '65535' (2 byte field).
4) CVC3/PINCVC3	5 A	The CVC3 or PINCVC3 to be validated. This field may contain leading 'X' characters, which indicate that the CVC3/PINCVC3 contains less than 5 digits. The 'X' characters are not part of the comparison with the calculated CVC3/PINCVC3. For example, a CVC3/PINCVC3 of 'XX123' matches with a Calculated CVC3/PINCVC3 of '87123'. Max value '65535' (decimal representation of a 2 byte value).
5) CVC Mask	8 B	The mask is used to extract bytes from the computed CVC3 calculation for comparison. For example 0xFFFF0000 00000000 will compare the 2 MSB and 0x00000000 0000FFFF will compare the 2 LSB.
The following section applies only when using Scheme '2' (American Express) and Version '0' (ExpressPay).		
1) Transaction Data Length	2 H	Length of the following field. Can be any length from '01' (1) to 'FF' (255) bytes.
2) Transaction Data	n B	Variable length data. If the data supplied is not a multiple of 8 bytes, additional zero padding is added.
3) Delimiter	1 A	Delimiter, to indicate the end of Transaction Data, value ':'.

Field	Length & Type	Details
4) Cryptogram	5 N	The Cryptogram to be validated.
The following section applies only when using Scheme '3' (Discover) and Version '0' or '2'.		
1) ATC	4 N	Decimal value of Application Transaction Counter.
2) Unpredictable Number	2 N	Value of random number provided to the card by the terminal during a transaction.
3) DCVV	3 N	The DCVV to be verified.
The following section applies only when using Scheme '3' (Discover) and Version '1'.		
1) ATC	4 N	Decimal value of Application Transaction Counter.
2) Unpredictable Number	2 N	Value of random number provided to the card by the terminal during a transaction.
3) Extended Unpredictable Number	6 N	Value of Extended Unpredictable Number, in BCD format, right-justified and zero-filled.
4) DCVV Plus Length	1 N	Length of DCVV Plus.
5) DCVV Plus	n N	DCVV Plus. Length is determined by preceding field.
The following section applies only when using Scheme '4' (Oberthur).		
1) Expiration Date	4 N	Expiration Date (YYMM format)
2) Service Code	3 N	The service code to use for OdCVV
3) Counter	16 H	Counter value
4) Future Counters	2 H	Max number of future counter values to use
5) Prev Counters	2 H	Max number of previous counter values to use
6) Label	2 H	Diversification value
7) OdCVV Length	2 N	Length of OdCVV
8) OdCVV	n N	The OdCVV to be verified
The following section applies only when using Scheme '5' (Visa dCVV2).		
1) Expiration Date	4 N	Expiration Date (YYMM format)
2) TWU	6 N	Time Window Unit (in seconds)
3) Current Time	8 H	Time in seconds since 00:00:00 1 st Jan 1970
4) dCVV2	3 N	The dCVV2 to be verified
The following section applies only when using Scheme '6' (JCB).		
1) Expiration Date	4 N	Expiration Date (MMYY format)
2) Service Code	3 N	The service code to use
3) ATC	5 N	Application Transaction Counter (decimalized value) Max value is '65535' corresponding to ATC '0xFFFF'
4) Discretionary Data CVS	1 N	Discretionary Data Card Verification Status Valid values: '1', '2', '3', '4'
5) dCAV	3 N	Dynamic CAV
The following section applies only when using Scheme '7' (Gemalto).		
1) TWU	6 N	Time Window Unit (in seconds)
2) Current Time	8 H	Time in seconds since 00:00:00 1 st January 1970
3) dCV	3 N	The dCV to be verified
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'PN'.
Error Code	2 A	'00': No error '01': Cryptogram verification failure '05': Unrecognized Scheme, Version ID or Key Derivation Method '06': Invalid YHHHHCC value '10': MK-DCVV Parity Error '52': Invalid Discretionary Data CVS '68': Command disabled 'E9': Invalid CVC3 mask value 'EA': Invalid Modified PSN Flag or a standard error code.
Diagnostic Data	3 N or 5 N or 6 N or n N	The calculated (correct) value of the cryptogram. Only present if Error Code 01 is returned and the HSM is in Authorised State. If Scheme ID = '0' and Version = '0' or '2', this is a 3N field containing the correct dCVV or LUC respectively. If Scheme ID = '3' and Version = '0' or '2', this is a 3N field containing the correct dCVV. If Scheme ID = '6' and Version = '0', this is a 3N field containing the correct dCAV. If Scheme ID = '7' and Version = '0', this is a 3N field containing the correct dCV. If Scheme ID = '1' and Version = '0', '1', or '2', this is a 5N field containing the correct CVC3. If Scheme ID = '1' and Version = '3' or '4', this is a 5N field containing the correct PINCVC3. If Scheme ID = '2' and Version = '0', this is a 5N field containing the correct Cryptogram. If Scheme ID = '0' and Version = '1', this is a 6N field containing the correct LUC. If Scheme ID = '3' and Version = '1', this is an nN field containing the correct DCVV Plus (where n is specified by the input field "DCVV Plus Length"). If Scheme ID = '4', this is an nN field containing the correct OdCVV. If Scheme ID = '5', this is an nN field containing the correct dCVV2.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify Card Security Codes

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify an American Express Card Security Code (CSC).

This command verifies the 5-digit, 4-digit and 3-digit Card Security Code.

This command supports three algorithms for calculating the CSC:

- Classic CSC Algorithm (CSC Version 1.0)
- Enhanced CSC Algorithm (CSC Version 2.0)
- American Express Verification Value (AEVV). In this case:

The Expiration date is replaced by a 4-digit Unpredictable number calculated from the Transaction Identifier, as defined in the 3-D Secure process.

The Service Code is replaced by the following 2 fields:

- A 1-digit Authentication Results Code, as defined for the AEVV process
- A 2-digit Second Factor Authentication Results Code, as defined for the AEVV process

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'RY'.						
Mode	1 N	Value '4'.						
Flag	1 N	Algorithm indicator: '0': Classic CSC Algorithm (CSC Version 1.0) '2': Enhanced CSC Algorithm (CSC Version 2.0) '3': American Express Verification Value (AEVV)						
CSCK	32 H or 'U' + 32 H or 'S' + n A	The CSCK used to verify the Card Security Code. For a Variant LMK, the 'CSCK' must be encrypted under LMK pair 14-15 variant 4. For a Key Block LMK, the 'CSCK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'C0', '11'</td> <td>'T'</td> <td>'C', 'V', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'C0', '11'	'T'	'C', 'V', 'N'
Key Usage	Algorithm	Mode of Use						
'C0', '11'	'T'	'C', 'V', 'N'						
Primary Account Number (PAN)	19 N	The full PAN, left-justified and zero-filled if less than 19 digits.						
Expiration date	4 N	If Flag = '0' or '2', this field contains the card's expiration date, in the format YYMM. If Flag = '3', this field contains the AEVV Unpredictable Number.						
Service Code	3 N	Only present if Flag = '2' or '3'. If Flag = '3', this field contains the AEVV Authentication Results Code (1 digit) followed by the AEVV Second Factor Authenticating Code (2 digits).						
5-digit CSC/iCSC	5 N	Only present if Flag = '0' or '2'. 5-digit Card Security Code: enter 'FFFFF' if the 5-digit CSC is not to be validated. This field is not present for Flag values other than '0' or '2'.						
4-digit CSC/iCSC	4 N	Only present if Flag = '0' or '2'. 4-digit Card Security Code: enter 'FFFF' if the 4-digit CSC is not to be validated. This field is not present for Flag values other than '0' or '2'.						
3-digit CSC/iCSC/AEVV	3 N	Present for all Flag values. 3-digit Card Security Code (or the 3-digit AEVV if Flag = '3'). If Flag = '0' or '2', this field will be ignored if set to 'FFF'.						

payShield 10K Core Host Commands

Field	Length & Type	Details
COMMAND MESSAGE		
Delimiter	1 A	If Flag = '3' this field will contain the 3-digit iCSC or AEVV.
LMK Identifier	2 N	Value '%'. Optional; if present, the following field must also be present. LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RZ'.
Error Code	2 A	'00': No error '01': Card Security Code verification failure '10': CSCK parity error '27': CSCK not double length '68': Command disabled or a standard error code.
Mode	1 N	Value '4'.
5-digit CSC/iCSC verification	1 N	Only present if Flag = '0' or '2'. '0' if pass '1' if not present '2' if verification failed.
4-digit CSC/iCSC verification	1 N	Only present if Flag = '0' or '2'. '0' if pass '1' if not present '2' if verification failed.
3-digit CSC/iCSC/AEVV verification	1 N	'0' if pass '1' if not present '2' if verification failed.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

5.5 Racal Transaction Key Scheme (RTKS) Commands

The Racal Transaction Key Scheme (RTKS) is a key management technique that is closely coupled with message authentication. The functions provided by the payShield 10K include key management in addition to MAC generation and verification.

The payShield 10K provides the following host commands to support RTKS operations:

Function	Command	Page
<i>Transaction Request With a PIN (T/AQ Key) (when selected Transaction Key Scheme is Racal)</i>	RI (RJ)	371
<i>Transaction Request With a PIN (T/AQ Key) (when selected Transaction Key Scheme is Australian)</i>	HI (HJ)	373
<i>Transaction Request Without a PIN (when selected Transaction Key Scheme is Racal)</i>	RK (RL)	374
<i>Transaction Request Without a PIN (when selected Transaction Key Scheme is Australian)</i>	HK (HL)	376
<i>Transaction Request With a PIN (T/CI Key) (when selected Transaction Key Scheme is Racal)</i>	RU (RV)	377
<i>Transaction Request With a PIN (T/CI Key) (when selected Transaction Key Scheme is Australian)</i>	HU (HV)	379
<i>Translate KEYVAL (when selected Transaction Key Scheme is Racal)</i>	RW (RX)	380
<i>Translate KEYVAL (when selected Transaction Key Scheme is Australian)</i>	HW (HX)	382
<i>Administration Request Message (when selected Transaction Key Scheme is Racal)</i>	RM (RN)	383
<i>Administration Request Message (when selected Transaction Key Scheme is Australian)</i>	HM (HN)	385
<i>Transaction Response with Auth Para from Card Issuer (when selected Transaction Key Scheme is Racal)</i>	RO (RP)	386
<i>Transaction Response with Auth Para from Card Issuer (when selected Transaction Key Scheme is Australian)</i>	HO (HP)	388
<i>Generate Auth Para and Transaction Response (when selected Transaction Key Scheme is Racal)</i>	RQ (RR)	389
<i>Generate Auth Para and Transaction Response (when selected Transaction Key Scheme is Australian)</i>	HQ (HR)	391
<i>Confirmation (when selected Transaction Key Scheme is Racal)</i>	RS (RT)	392
<i>Confirmation (when selected Transaction Key Scheme is Australian)</i>	HS (HT)	394

The Hx and Rx Host commands perform exactly the same functions. The Rx command code must be used when the Racal Transaction Key Scheme is selected in the security setting "*Transaction key scheme: Racal, Australian or None?*". The Hx command code must be used when the Australian Transaction key Scheme is selected. (This allows both Racal and Australian key transaction schemes to be used on the same payShield 10K.)

Transaction Request With a PIN (T/AQ Key) (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Validate a MAC on request from a terminal and return the TPK under the LMK and the MAC residue under the LMK.

Notes: This command is only available if Transaction Key Scheme has been set to Racal in the security setting "*Transaction key scheme: Racal, Australian or None?*". If Transaction Key Scheme has been set to Australian, then the HI Host command can be used, which provides exactly the same functionality as the RI Host command described below. For further details, see the *payShield 10K Host Programmer's manual*.

The command does not accept an all zero account number element of the 'message text' field.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'RI'.						
Terminal Key Register	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The Terminal Key Register, used to validate the MAC. For a Variant LMK, the 'Terminal Key Register' must be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 9 if the setting has the value "Y". For a Key Block LMK, the 'Terminal Key Register' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '73'</td> <td>'D', 'T'</td> <td>'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '73'	'D', 'T'	'N'
Key Usage	Algorithm	Mode of Use						
'P0', '73'	'D', 'T'	'N'						
Primary Account Number (PAN) pointer	2 H	Value '00' if the PAN starts at the first character in the message text field, and one value greater for each subsequent character into the field. The PAN is terminated by the first non-numeric character. This is ignored if extended length messages are used but two hexadecimal digits must still be supplied.						
Fields C & D	16 H	The C & D fields from the magnetic stripe of a card as defined in the Racal Security Scheme.						
PIN block pointer	2 H	Value '00' if the PIN block starts at the first character in the message text field and one value greater for each subsequent character into the field. The PIN block is 16 (hexadecimal) characters and is formatted according to the ANSI X9.8 standard (PIN block format 01). This field is ignored if extended length messages are used, but two hexadecimal digits must still be supplied.						
Message length	2 H	Value '00' to 'A0' (decimal 160) indicating the length of the next field. This field should be set to '00' and the next field omitted if extended length messages are required.						
Message text	n A	The message to be authenticated, as received from the terminal, but excluding STX, ETX and LRC. The last 8 characters are assumed to be the MAC. This field is omitted if extended length messages are required.						
Delimiter	1 C	Optional. Value '!'. Only present if extended length messages to be used.						
Extended account number pointer	4 H	Optional. Only present if extended length messages are to be used. '0000' if the PAN starts at the first character in the message text field, and one value greater for each subsequent character into the field. The PAN is terminated by the first non-numeric character.						
Extended PIN block pointer	4 H	Optional. Only present if extended length messages are to be used. '0000' if the PIN block starts at the first character in the message text field, and one value greater for each subsequent character into the field. The PIN block is 16 (hexadecimal)						

Field	Length & Type	Details
COMMAND MESSAGE		
Extended Message Length	4 H	characters and is formatted according to the ANSI X9.8 standard (PIN block format 01).
Extended Message Text	n A	Optional. Only present if extended length messages are to be used. Defines the length of the next field. Maximum value is determined by the maximum size of the HSM input buffer.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RJ'.
Error Code	2 A	'00': No error '01': MAC verification failure '10': Key register parity error '22': All zero account number used '68': Command disabled or a standard error code.
Request MAC residue	8 H	The Request MAC residue encrypted under the LMK.
TPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The TPK, used to decrypt a PIN block. For a Variant LMK, the 'TPK' will be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y".
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Transaction Request With a PIN (T/AQ Key) (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Validate a MAC on request from a terminal and return the TPK under the LMK and the MAC residue under the LMK.

Notes: This command code should be used where the Transaction Key Scheme has been set to Australian in the security setting "*Transaction key scheme: Racal, Australian or None?*", but it is also required to process commands for the Racal Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RI command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RI Host command described in this manual, except that:

Command Code = HI

Response Code = HJ

If Transaction Key Scheme has been set to Racal, then the RI Host command (as described in this manual) must be used. (With this setting, the HI command code is as described in the AS2805 section of this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command*	Use the Hx variant of the command*
You want to process Australian Transaction Key commands	Use the Hx variant of the command*	Use the Rx variant of the command*

For further details, the *payShield 10K Host Programmer's manual*.

The command does not accept an all zero account number element of the 'message text' field.

Transaction Request Without a PIN (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To validate the MAC on a Request message from a terminal and return the Request MAC Residue, encrypted under the LMK.

Notes: This command is only available if Transaction Key Scheme has been set to Racal in the security setting "*Transaction key scheme: Racal, Australian or None?*". If Transaction Key Scheme has been set to Australian, then the HK Host command can be used, which provides exactly the same functionality as the RK Host command described below. For further details, see the *payShield 10K Host Programmer's manual*.

Similar to the "RI" command, but does not return the derived TPK.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'RK'.						
Terminal Key Register	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The Terminal Key Register, used to validate the MAC. For a Variant LMK, the 'Terminal Key Register' must be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 9 if the setting has the value "Y". For a Key Block LMK, the 'Terminal Key Register' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '73'</td> <td>'D', 'T'</td> <td>'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '73'	'D', 'T'	'N'
Key Usage	Algorithm	Mode of Use						
'P0', '73'	'D', 'T'	'N'						
Primary Account Number (PAN) pointer	2 H	Value '00' if the PAN starts at the first character in the message text field, and one value greater for each subsequent character into the field. The PAN is terminated by the first non-numeric character. This is ignored if extended length messages are used but two hex digits must still be supplied.						
Message length	2 H	Value '00' to 'A0' (decimal 160) indicating the length of the next field. This field should be set to '00' and the next field omitted if extended length messages are required.						
Message text	n A	The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. Omitted if extended length messages are required.						
Delimiter	1 C	Optional. Value '!'. Only present if extended length messages to be used.						
Extended account number pointer	4 H	Optional. Only present if extended length messages are to be used. '0000' if the PAN starts at the first character in the message text field, and one value greater for each subsequent character into the field. The PAN is terminated by the first non-numeric character.						
Extended Message Length	4 H	Optional. Only present if extended length messages are to be used. Defines the length of the next field. Maximum value is determined by the maximum size of the HSM input buffer.						
Extended Message Text	n A	Optional. Only present if extended length messages are to be used. The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						

Field	Length & Type	Details
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RL'.
Error Code	2 A	'00': No error '01': MAC verification failure '10': Key register parity error '68': Command disabled or a standard error code.
Request MAC residue	8 H	The Request MAC residue encrypted under the LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Transaction Request Without a PIN (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To validate the MAC on a Request message from a terminal and return the Request MAC Residue, encrypted under the LMK.

Notes: This command code should be used where the Transaction Key Scheme has been set to Australian in the security setting "*Transaction key scheme: Racal, Australian or None?*", but it is also required to process commands for the Racal Transaction Key Scheme.

In this environment, the HK commands acts exactly like the RK command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RK Host command described in this manual, except that:

Command Code = HK

Response Code = HL

If Transaction Key Scheme has been set to Racal, then the RK Host command (as described in this manual) must be used. (With this setting, the HK command code is as described in the AS2805 section of this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command	Use the Hx variant of the command
You want to process Australian Transaction Key commands	Use the Hx variant of the command	Use the Rx variant of the command

For further details, see the *payShield 10K Host Programmer's manual*.

Similar to the "RI" command, but does not return the derived TPK.

Transaction Request With a PIN (T/CI Key) (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify the MAC and return the MAC residue and KEYVAL encrypted under the LMK.

Notes: This command is only available if Transaction Key Scheme has been set to Racal in the security setting "*Transaction key scheme: Racal, Australian or None?*". If Transaction Key Scheme has been set to Australian, then the HU Host command can be used, which provides exactly the same functionality as the RU Host command described below. For further details, see the *payShield 10K Host Programmer's manual*.

The command does not accept an all zero account number element of the 'message text' field.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'RU'.						
Terminal Key Register	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The Terminal Key Register, used to validate the MAC.</p> <p>For a Variant LMK, the 'Terminal Key Register' must be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 9 if the setting has the value "Y".</p> <p>For a Key Block LMK, the 'Terminal Key Register' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '73'</td> <td>'D', 'T'</td> <td>'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '73'	'D', 'T'	'N'
Key Usage	Algorithm	Mode of Use						
'P0', '73'	'D', 'T'	'N'						
Primary Account Number (PAN) pointer	2 H	Value '00' if the PAN starts at the first character in the message text field, and one value greater for each subsequent character into the field. The PAN is terminated by the first non-numeric character. This field is ignored if extended length messages are used but two hexadecimal digits must still be supplied.						
Message length	2 H	Value '00' to 'A0' (decimal 160) indicating the length of the next field. This field should be set to '00' and the next field omitted if extended length messages required.						
Message text	n A	The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. This field is omitted if extended length messages are required.						
Delimiter	1 C	Optional. Value '!'. Only present if extended length messages to be used.						
Extended account number pointer	4 H	Optional. Only present if extended length messages are to be used. '0000' if the PAN starts at the first character in the message text field, and one value greater for each subsequent character into the field. The PAN is terminated by the first non-numeric character.						
Extended Message Length	4 H	Optional. Only present if extended length messages are to be used. Defines the length of the next field. Maximum value is determined by the maximum size of the HSM input buffer.						
Extended Message Text	n A	Optional. Only present if extended length messages are to be used. The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						

Field	Length & Type	Details
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RV'.
Error Code	2 A	'00': No error '01': MAC verification failure '10': Key register parity error '22': All zero account number '68': Command disabled or a standard error code.
Request MAC residue	8 H	The Request MAC residue encrypted under the LMK.
KEYVAL	16 H or 'U' + 32 H or 'S' + 32 H or 'N' + 32 H	The generated KEYVAL, encrypted under the LMK. When using a Variant LMK, this field is encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y". When using a 3DES Key Block LMK, this field consists of an "S" followed by 32 hex digits. When using an AES Key Block LMK, this field consists of an "N" followed by 32 hex digits.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Transaction Request With a PIN (T/CI Key) (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify the MAC and return the MAC residue and KEYVAL encrypted under the LMK.

Notes: This command code should be used where the Transaction Key Scheme has been set to Australian in the security setting "*Transaction key scheme: Racal, Australian or None?*", but it is also required to process commands for the Racal Transaction Key Scheme.

In this environment, the HU commands acts exactly like the RU command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RU Host command described in this manual, except that:

Command Code = HU

Response Code = HV

If Transaction Key Scheme has been set to Racal, then the RU Host command (as described in this manual) must be used. (With this setting, the HU command code is as described in the AS2805 section of this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command	Use the Hx variant of the command
You want to process Australian Transaction Key commands	Use the Hx variant of the command	Use the Rx variant of the command

For further details, see the *payShield 10K Host Programmer's manual*.

The command does not accept an all zero account number element of the 'message text' field.

Translate KEYVAL (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To translate KEYVAL from encryption under the LMK to encryption under a Zone PIN Key (ZPK).

Notes: This command is only available if Transaction Key Scheme has been set to Racal in the security setting "*Transaction key scheme: Racal, Australian or None?*". If Transaction Key Scheme has been set to Australian, then the HW Host command can be used, which provides exactly the same functionality as the RW Host command described below. For further details, see the *payShield 10K Host Programmer's manual*.

This command is used to send KEYVAL to another party (generally, the Card Issuer).

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'RW'.						
ZPK	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The Zone PIN Key, used to encrypt the KEYVAL. For a Variant LMK, the 'ZPK' must be encrypted under LMK pair 06-07.						
KEYVAL	16 H or 'N' + 32 H or 'S' + 32 H	For a Key Block LMK, the 'ZPK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '72'</td> <td>'D', 'T'</td> <td>'B', 'E', 'N'</td> </tr> </table> The KEYVAL to be translated, encrypted under the LMK. When using a Variant LMK, this field is encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value 'N' or LMK pair 36-37 variant 7 if the setting has the value 'Y'. When using a 3DES Key Block LMK, this field must consist of an 'S' followed by 32 hex digits. When using an AES Key Block LMK, this field must consist of an 'N' followed by 32 hex digits.	Key Usage	Algorithm	Mode of Use	'P0', '72'	'D', 'T'	'B', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'D', 'T'	'B', 'E', 'N'						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RX'.
Error Code	2 A	'00': No error '10': ZPK parity error '11': KEYVAL parity error '68': Command disabled or a standard error code.
KEYVAL	16 H	The KEYVAL, encrypted under the ZPK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate KEYVAL (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To translate KEYVAL from encryption under the LMK to encryption under a Zone PIN Key (ZPK).

Notes: This command code should be used where the Transaction Key Scheme has been set to Australian in the security setting "*Transaction key scheme: Racal, Australian or None?*", but it is also required to process commands for the Racal Transaction Key Scheme.

In this environment, the HW commands acts exactly like the RW command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RW Host command described in this manual, except that:

Command Code = HW

Response Code = HX

If Transaction Key Scheme has been set to Racal, then the RW Host command (as described in this manual) must be used. (With this setting, the HW command code is as described in the AS2805 section of this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command	Use the Hx variant of the command
You want to process Australian Transaction Key commands	Use the Hx variant of the command	Use the Rx variant of the command

For further details, see the *payShield 10K Host Programmer's manual*.

This command is used to send KEYVAL to another party (generally, the Card Issuer).

Administration Request Message (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify the MAC on an Administration Request message and return the Request MAC residue encrypted under the LMK. Used to support terminal administration request messages.

Notes: This command is only available if Transaction Key Scheme has been set to Racal in the security setting "*Transaction key scheme: Racal, Australian or None?*". If Transaction Key Scheme has been set to Australian, then the HM Host command can be used, which provides exactly the same functionality as the RM Host command described below. For further details, see the *payShield 10K Host Programmer's manual*.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'RM'.						
Terminal Key Register	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The Terminal Key Register, used to validate the MAC. For a Variant LMK, the 'Terminal Key Register' must be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 9 if the setting has the value "Y". For a Key Block LMK, the 'Terminal Key Register' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'P0', '73'</td> <td>'D', 'T'</td> <td>'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'P0', '73'	'D', 'T'	'N'
Key Usage	Algorithm	Mode of Use						
'P0', '73'	'D', 'T'	'N'						
Fields A & B	16 H	The A & B fields as defined in the Racal Security Scheme.						
Message length	2 H	Value '00' to 'A0' (decimal 160) indicating the length of the next field. This field should be set to '00' and the next field omitted if extended length messages required.						
Message text	n A	The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. Omitted if extended length messages are required.						
Delimiter	1 C	Optional. Value ';'. Only present if extended length messages to be used.						
Extended Message Length	4 H	Optional. Only present if extended length messages are to be used. Defines the length of the next field. Maximum value is determined by the maximum size of the HSM input buffer.						
Extended Message Text	n A	Optional. Only present if extended length messages are to be used. The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RN'.
Error Code	2 A	'00': No error '01': MAC verification failure '10': Key register parity error '68': Command disabled or a standard error code.
Request MAC Residue	8 H	The Request MAC residue encrypted under the LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Administration Request Message (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify the MAC on an Administration Request message and return the Request MAC residue encrypted under the LMK. Used to support terminal administration request messages.

Notes: This command code should be used where the Transaction Key Scheme has been set to Australian in the security setting "*Transaction key scheme: Racal, Australian or None?*", but it is also required to process commands for the Racal Transaction Key Scheme.

In this environment, the HM commands acts exactly like the RM command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RM Host command described in this manual, except that:

Command Code = HM

Response Code = HN

If Transaction Key Scheme has been set to Racal, then the RM Host command (as described in this manual) must be used. (With this setting, the HM command code is as described in the AS2805 section of this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command	Use the Hx variant of the command
You want to process Australian Transaction Key commands	Use the Hx variant of the command	Use the Rx variant of the command

For further details, see the *payShield 10K Host Programmer's manual*.

Transaction Response with Auth Para from Card Issuer (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate the MAC on a Response message to a terminal, update the Terminal Key Register and return the encrypted value and the encrypted Response MAC Residue to the Host.

Notes: This command is only available if Transaction Key Scheme has been set to Racal in the security setting "*Transaction key scheme: Racal, Australian or None?*". If Transaction Key Scheme has been set to Australian, then the HO Host command can be used, which provides exactly the same functionality as the RO Host command described below. For further details, see the *payShield 10K Host Programmer's manual*.

The command is used to respond to requests from terminals at the acquirer Host.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'RO'.						
Terminal Key Register	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The Terminal Key Register, used to generate the MAC. For a Variant LMK, the 'Terminal Key Register' must be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 9 if the setting has the value "Y". For a Key Block LMK, the 'Terminal Key Register' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '73'</td> <td>'D', 'T'</td> <td>'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '73'	'D', 'T'	'N'
Key Usage	Algorithm	Mode of Use						
'P0', '73'	'D', 'T'	'N'						
Fields A & B	16 H	The A & B fields from the magnetic stripe as defined in the Racal Security Scheme.						
ZPK or flag	1 A or 16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The Zone PIN Key, or the single character 'L' to indicate that Auth Para is encrypted under the LMK (see next field). For a Variant LMK, the 'ZPK' must be encrypted under LMK pair 06-07. For a Key Block LMK, the ZPK must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '72'</td> <td>'D', 'T'</td> <td>'B', 'D', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '72'	'D', 'T'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '72'	'D', 'T'	'B', 'D', 'N'						
Auth Para	16 H	The Authorisation parameter either encrypted under ZPK or under the LMK (as indicated in the previous field).						
Request MAC residue	8 H	The MAC residue from the corresponding transaction request message, encrypted under the LMK.						
Message length	2 H	Value '00' to 'A0' (decimal 160) indicating the length of the next field. This field should be set to '00' and the next field omitted if extended length messages required.						
Message text	n A	The message to be authenticated, as received from the terminal, but excluding STX, ETX and LRC. This field is omitted if extended length messages are required.						
Delimiter	1 C	Optional. Value ';'. Only present if extended length messages to be used.						

Field	Length & Type	Details
Extended Message Length	4 H	Optional. Only present if extended length messages are to be used. Defines the length of the next field. Maximum value is determined by the maximum size of the HSM input buffer.
Extended Message Text	n A	Optional. Only present if extended length messages are to be used. The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details						
RESPONSE MESSAGE								
Message Header	m A	Returned to the Host unchanged.						
Response Code	2 A	Value 'RP'.						
Error Code	2 A	'00': No error '10': Key register parity error '11': ZPK parity error '68': Command disabled or a standard error code.						
Response MAC residue	8 H	The Response MAC residue (generated during the calculation of the Response MAC), encrypted under the LMK.						
Response MAC	8 H	The generated MAC to be sent to the terminal.						
Terminal Key Register	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The new Terminal Key Register, to replace the current one. For a Variant LMK, the 'Terminal Key Register' will be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 9 if the setting has the value "Y". For a Key Block LMK, the 'Terminal Key Register' will comply with the following:						
		<table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'73'</td> <td>'D', 'T'</td> <td>'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'73'	'D', 'T'	'N'
Key Usage	Algorithm	Mode of Use						
'73'	'D', 'T'	'N'						
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.						
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.						

Transaction Response with Auth Para from Card Issuer (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate the MAC on a Response message to a terminal, update the Terminal Key Register and return the encrypted value and the encrypted Response MAC Residue to the Host.

Notes: This command code should be used where the Transaction Key Scheme has been set to Australian in the security setting "*Transaction key scheme: Racal, Australian or None?*", but it is also required to process commands for the Racal Transaction Key Scheme.

In this environment, the HO commands acts exactly like the RO command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RO Host command described in this manual, except that:

Command Code = HO

Response Code = HP

If Transaction Key Scheme has been set to Racal, then the RO Host command (as described in this manual) must be used. (With this setting, the HO command code is as described in the AS2805 section of this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command	Use the Hx variant of the command
You want to process Australian Transaction Key commands	Use the Hx variant of the command	Use the Rx variant of the command

For further details, see the *payShield 10K Host Programmer's manual*.

The command is used to respond to requests from terminals at the acquirer Host.

Generate Auth Para and Transaction Response (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate the MAC on a Response message to a terminal, update the Terminal Key Register and return the encrypted value and the encrypted Response MAC Residue to the Host.

Notes: This command is only available if Transaction Key Scheme has been set to Racal in the security setting "*Transaction key scheme: Racal, Australian or None?*". If Transaction Key Scheme has been set to Australian, then the HQ Host command can be used, which provides exactly the same functionality as the RQ Host command described below. For further details, see the *payShield 10K Host Programmer's manual*.

The command used to respond to requests from terminals at the acquirer Host.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'RQ'.						
Terminal Key Register	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The Terminal Key Register, used to generate the MAC.</p> <p>For a Variant LMK, the 'Terminal Key Register' must be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 9 if the setting has the value "Y".</p> <p>For a Key Block LMK, the 'Terminal Key Register' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'P0', '73'</td><td>'D', 'T'</td><td>'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '73'	'D', 'T'	'N'
Key Usage	Algorithm	Mode of Use						
'P0', '73'	'D', 'T'	'N'						
Fields A & B	16 H	The A & B fields, from the magnetic stripe, as defined in the Racal Security Scheme.						
Auth Para data block	16 H	The data block used to generate Auth Para.						
Request MAC residue	8 H	The MAC residue from the corresponding transaction Request message, encrypted under the LMK.						
Message length	2 H	Value '00' to 'A0' (decimal 160) indicating the length of the next field. This field should be set to '00' and the next field omitted if extended length messages required.						
Message text	n A	The message to be authenticated, as received from the terminal, but excluding STX, ETX and LRC. This field is omitted if extended length messages are required.						
Delimiter	1 C	Optional. Value ';'. Only present if extended length messages to be used.						
Extended Message Length	4 H	Optional. Only present if extended length messages are to be used. Defines the length of the next field. Maximum value is determined by the maximum size of the HSM input buffer.						
Extended Message Text	n A	Optional. Only present if extended length messages are to be used. The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details						
RESPONSE MESSAGE								
Message Header	m A	Returned to the Host unchanged.						
Response Code	2 A	Value 'RR'.						
Error Code	2 A	'00': No error '10': Key register parity error '68': Command disabled or a standard error code.						
Response MAC residue	8 H	The MAC residue (generated during the calculation of the Response MAC), encrypted under the LMK.						
Response MAC	8 H	The generated MAC to be sent to the terminal.						
Terminal Key Register	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	For a Variant LMK, the 'Terminal Key Register' will be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 9 if the setting has the value "Y". For a Key Block LMK, the 'Terminal Key Register' will comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'73'</td> <td>'D', 'T'</td> <td>'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'73'	'D', 'T'	'N'
Key Usage	Algorithm	Mode of Use						
'73'	'D', 'T'	'N'						
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.						
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.						

Generate Auth Para and Transaction Response (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate the MAC on a Response message to a terminal, update the Terminal Key Register and return the encrypted value and the encrypted Response MAC Residue to the Host.

Notes: This command code should be used where the Transaction Key Scheme has been set to Australian in the security setting "*Transaction key scheme: Racal, Australian or None?*", but it is also required to process commands for the Racal Transaction Key Scheme.

In this environment, the HQ commands acts exactly like the RQ command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RQ Host command described in this manual, except that:

Command Code = HQ

Response Code = HR

If Transaction Key Scheme has been set to Racal, then the RQ Host command (as described in this manual) must be used. (With this setting, the HQ command code is as described in the AS2805 section of this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command	Use the Hx variant of the command
You want to process Australian Transaction Key commands	Use the Hx variant of the command	Use the Rx variant of the command

For further details, see the *payShield 10K Host Programmer's manual*.

Confirmation (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify MAC on incoming confirmation message from the terminal.

Notes: This command is only available if Transaction Key Scheme has been set to Racal in the security setting "*Transaction key scheme: Racal, Australian or None?*". If Transaction Key Scheme has been set to Australian, then the HS Host command can be used, which provides exactly the same functionality as the RS Host command described below. For further details, see the *payShield 10K Host Programmer's manual*.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'RS'.						
Terminal Key Register	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The Terminal Key Register, used to verify the MAC.</p> <p>For a Variant LMK, the 'Terminal Key Register' must be encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 9 if the setting has the value "Y".</p> <p>For a Key Block LMK, the 'Terminal Key Register' must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '73'</td> <td>'D', 'T'</td> <td>'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '73'	'D', 'T'	'N'
Key Usage	Algorithm	Mode of Use						
'P0', '73'	'D', 'T'	'N'						
Fields A & B	16 H	The A & B fields, from the magnetic stripe, as defined in the Racal Security Scheme.						
Response MAC Residue	8 H	The MAC residue from the corresponding transaction Response message, encrypted under the LMK.						
Message length	2 H	Value '00' to 'A0' (decimal 160) indicating the length of the next field. This field should be set to '00' and the next field omitted if extended length messages required.						
Message text	n A	The message to be authenticated, as received from the terminal, but excluding STX, ETX and LRC. The last 8 characters are assumed to be the MAC. This field is omitted if extended length messages are required.						
Delimiter	1 C	Optional. Value ';'. Only present if extended length messages to be used.						
Extended Message Length	4 H	Optional. Only present if extended length messages are to be used. Defines the length of the next field. Maximum value is determined by the maximum size of the HSM input buffer.						
Extended Message Text	n A	Optional. Only present if extended length messages are to be used. The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RT'.
Error Code	2 A	'00': No error '01': MAC verification failure '10': Key register parity error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Confirmation (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify MAC on incoming confirmation message from the terminal.

Notes: This command code should be used where the Transaction Key Scheme has been set to Australian in the security setting "*Transaction key scheme: Racal, Australian or None?*", but it is also required to process commands for the Racal Transaction Key Scheme.
In this environment, the HS commands acts exactly like the RS command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RS Host command described in this manual, except that:

Command Code = HS

Response Code = HT

If Transaction Key Scheme has been set to Racal, then the RS Host command (as described in this manual) must be used. (With this setting, the HS command code is as described in the AS2805 section of this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command	Use the Hx variant of the command
You want to process Australian Transaction Key commands	Use the Hx variant of the command	Use the Rx variant of the command

For further details, see the *payShield 10K Host Programmer's manual*.

5.6 DUKPT (X9.24) Transaction Processing Commands

The payShield 10K provides the following host commands to support DUKPT operations:

Function	Command	Page
Translate a PIN from BDK to BDK or ZPK Encryption (3DES & AES DUKPT)	G0 (G1)	398
Verify a PIN Using the IBM Offset Method (3DES & AES DUKPT)	GO (GP)	402
Verify a PIN Using the ABA PVV Method (3DES & AES DUKPT)	GQ (GR)	406
Verify a PIN Using the Diebold Method (3DES & AES DUKPT)	GS (GT)	410
Verify a PIN Using the Encrypted PIN Method (3DES & AES DUKPT)	GU (GV)	413
Generate/Verify a MAC (3DES & AES DUKPT)	GW (GX)	416

The above commands are used to acquire transactions from terminals that support the DUKPT key management scheme (as defined in X9.24). In the DUKPT scheme, both the terminal and the HSM derive a transaction key from the BDK and transaction data. Variants are then applied to the transaction key to produce working keys for PIN verification, data authentication purposes.

Note: This section only describes DUKPT for PIN encryption and data authentication. For DUKPT commands supporting data encryption (including the BDK-3), please refer to [Message Encryption Commands](#)

The latest revision of the DUKPT standard (X9.24-3:2017) defines two different methods for producing data authentication keys:

- The *bidirectional* method uses a single key to authenticate terminal-to-host data and host-to-terminal data. A BDK-1 supports the bidirectional method.
- The *unidirectional* method uses two keys: one key to authenticate terminal-to-host data, and another key to authenticate host-to-terminal data. A BDK-2 and BDK-4 support this method.

When acquiring transactions (i.e. receiving 'request' transaction data from a terminal, and (optionally) transmitting 'response' transaction data to the terminal):

- Use a BDK of type BDK-1 when *bidirectional* terminal-to-acquirer keys are required;
- Use a BDK of type BDK-2 when *unidirectional* terminal-to-acquirer keys are required.

For Payment Service Providers (PSPs) that emulate the function of a terminal (i.e. by transmitting 'request' transaction data to an acquirer, and (optionally) receiving 'response' transaction data from an acquirer):

- When *bidirectional* keys are required, the PSP and the acquirer should use the same BDK, of type BDK-1.
- When *unidirectional* keys are required, the PSP should use a BDK of type BDK-4, while the acquirer should use the same BDK, but of type BDK-2.

(Note that a BDK-3 uses the 'PIN encryption' variant to derive the data encryption key, and therefore can only be used to perform data encryption operations. A BDK-3 cannot be used to perform PIN or MAC related operations.)

Use BDK-5 to derive the appropriate PIN encryption key using the Italian Standard Derivation Method SPE-DEF-041-112. BDK-5 is equivalent to BDK-1 in all aspects apart from derivation of the IPEK / IKEY which uses the Italian Standard Key Derivation Method.

The differences between these four BDK types are summarised in the table below.

BDKs used with PIN encryption & MACing Commands

3DES DUKPT Key Variants

The table below lists the different Variant values that are applied during the derivation of the data encryption keys from a 3DES BDK:

BDK Type		Description								
BDK-1	For a Variant LMK, the 3DES BDK is encrypted under LMK 28-29.	<p>Variants are applied to the derived transaction key as follows:</p> <table border="1"> <thead> <tr> <th>Key function</th><th>Variant</th></tr> </thead> <tbody> <tr> <td>PIN encryption</td><td>00 00 00 00 00 00 00 FF</td></tr> <tr> <td>Verifying "request" MACs</td><td>00 00 00 00 00 00 FF 00</td></tr> <tr> <td>Generating "response" MACs</td><td>00 00 00 00 00 00 FF 00</td></tr> </tbody> </table> <p>Note that this method will produce <i>bidirectional</i> MAC keys.</p>	Key function	Variant	PIN encryption	00 00 00 00 00 00 00 FF	Verifying "request" MACs	00 00 00 00 00 00 FF 00	Generating "response" MACs	00 00 00 00 00 00 FF 00
Key function	Variant									
PIN encryption	00 00 00 00 00 00 00 FF									
Verifying "request" MACs	00 00 00 00 00 00 FF 00									
Generating "response" MACs	00 00 00 00 00 00 FF 00									
For a Key Block LMK, the 3DES BDK must have Key Usage = 'B0'.										
BDK-2	For a Variant LMK, the 3DES BDK is encrypted under LMK 28-29 variant 6.	<p>Variants are applied to the derived transaction key as follows:</p> <table border="1"> <thead> <tr> <th>Key function</th><th>Variant</th></tr> </thead> <tbody> <tr> <td>PIN encryption</td><td>00 00 00 00 00 00 00 FF</td></tr> <tr> <td>Verifying "request" MACs</td><td>00 00 00 00 00 00 FF 00</td></tr> <tr> <td>Generating "response" MACs</td><td>00 00 00 00 FF 00 00 00</td></tr> </tbody> </table> <p>Note that this method will produce <i>unidirectional</i> MAC keys.</p>	Key function	Variant	PIN encryption	00 00 00 00 00 00 00 FF	Verifying "request" MACs	00 00 00 00 00 00 FF 00	Generating "response" MACs	00 00 00 00 FF 00 00 00
Key function	Variant									
PIN encryption	00 00 00 00 00 00 00 FF									
Verifying "request" MACs	00 00 00 00 00 00 FF 00									
Generating "response" MACs	00 00 00 00 FF 00 00 00									
For a Key Block LMK, the 3DES BDK must have Key Usage = '41'.										
BDK-4	For a Variant LMK, the 3DES BDK is encrypted under LMK 28-29 variant 9.	<p>Variants are applied to the derived transaction key as follows:</p> <table border="1"> <thead> <tr> <th>Key function</th><th>Variant</th></tr> </thead> <tbody> <tr> <td>PIN encryption</td><td>00 00 00 00 00 00 00 FF</td></tr> <tr> <td>Generating "request" MACs</td><td>00 00 00 00 00 00 FF 00</td></tr> <tr> <td>Verifying "response" MACs</td><td>00 00 00 00 FF 00 00 00</td></tr> </tbody> </table> <p>Note that this method will produce <i>unidirectional</i> MAC keys.</p>	Key function	Variant	PIN encryption	00 00 00 00 00 00 00 FF	Generating "request" MACs	00 00 00 00 00 00 FF 00	Verifying "response" MACs	00 00 00 00 FF 00 00 00
Key function	Variant									
PIN encryption	00 00 00 00 00 00 00 FF									
Generating "request" MACs	00 00 00 00 00 00 FF 00									
Verifying "response" MACs	00 00 00 00 FF 00 00 00									
For a Key Block LMK, the 3DES BDK must have Key Usage = '43'.										
BDK-5	This key is not supported for a Variant LMK.	<p>This BDK is used for the Italian Standard Key Derivation Method only. The initial key is generated using Host Command A0.</p>								
	For a Key Block LMK, the 3DES BDK must have Key Usage = '44'.	<p>BDK-5 is equivalent to BDK-1 in all aspects apart from derivation of the IPEK / IKEY (which uses the Italian Standard Key Derivation Method).</p>								

AES DUKPT Key Usage Indicator

The table below lists the different Key Usage Indicator values that are applied during the derivation of the authentication & PIN encryption keys from an AES BDK:

BDK Type		Description								
BDK-1	For an AES Key Block LMK, the AES BDK must have Key Usage = 'B0'.	<p>The following Key Usage Indicator values are used in the derivation of the authentication & PIN encryption key:</p> <table border="1"> <thead> <tr> <th>Key function</th><th>Key Usage Indicator</th></tr> </thead> <tbody> <tr> <td>PIN encryption</td><td>0x1000</td></tr> <tr> <td>Verifying "request" MACs</td><td>0x2002</td></tr> <tr> <td>Generating "response" MACs</td><td>0x2002</td></tr> </tbody> </table> <p>Note that this method will produce <i>bidirectional</i> encryption keys.</p>	Key function	Key Usage Indicator	PIN encryption	0x1000	Verifying "request" MACs	0x2002	Generating "response" MACs	0x2002
Key function	Key Usage Indicator									
PIN encryption	0x1000									
Verifying "request" MACs	0x2002									
Generating "response" MACs	0x2002									
BDK-2	For an AES Key Block LMK, the AES BDK must have Key Usage = '41'.	<p>The following Key Usage Indicator values are used in the derivation of the authentication & PIN encryption key:</p> <table border="1"> <thead> <tr> <th>Key function</th><th>Key Usage Indicator</th></tr> </thead> <tbody> <tr> <td>PIN encryption</td><td>0x1000</td></tr> <tr> <td>Verifying "request" MACs</td><td>0x2000</td></tr> <tr> <td>Generating "response" MACs</td><td>0x2001</td></tr> </tbody> </table> <p>Note that this method will produce <i>unidirectional</i> encryption keys.</p>	Key function	Key Usage Indicator	PIN encryption	0x1000	Verifying "request" MACs	0x2000	Generating "response" MACs	0x2001
Key function	Key Usage Indicator									
PIN encryption	0x1000									
Verifying "request" MACs	0x2000									
Generating "response" MACs	0x2001									
BDK-4	For an AES Key Block LMK, the AES BDK must have Key Usage = '43'.	<p>The following Key Usage Indicator values are used in the derivation of the authentication & PIN encryption key:</p> <table border="1"> <thead> <tr> <th>Key function</th><th>Key Usage Indicator</th></tr> </thead> <tbody> <tr> <td>PIN encryption</td><td>0x1000</td></tr> <tr> <td>Generating "request" MACs</td><td>0x2000</td></tr> <tr> <td>Verifying "response" MACs</td><td>0x2001</td></tr> </tbody> </table> <p>Note that this method will produce <i>unidirectional</i> encryption keys.</p>	Key function	Key Usage Indicator	PIN encryption	0x1000	Generating "request" MACs	0x2000	Verifying "response" MACs	0x2001
Key function	Key Usage Indicator									
PIN encryption	0x1000									
Generating "request" MACs	0x2000									
Verifying "response" MACs	0x2001									

Further information about DUKPT and its implementation on the payShield 10K can be found in the *payShield 10K Host Programmer's manual*.

Translate a PIN from BDK to BDK or ZPK Encryption (3DES & AES DUKPT)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Translate a PIN from encryption under the DUKPT key to encryption under an interchange key (ZPK) or a (different) DUKPT key for transmission to another node. Note that translation to BDK encryption is only permitted if the security setting "*Enable PIN translation to BDK encryption*" is "YES".

This command supports the translation of PIN blocks built using a Token instead of the real PAN. This functionality is only supported if the security setting "*Enable use of Tokens in PIN Translation*" is "YES".

For a list of PIN block formats permitted for use in this command, please refer to the *payShield 10K Host Programmer's Manual*.

Notes: The PIN block format may also be changed, but refer to the table below for restrictions.

The ANSI X9.24-1:2009 method for DUKPT key derivation is used when a 3DES BDK is supplied.

The ANSI X9.24-3:2017 method for DUKPT key derivation is used when an AES BDK is supplied.

When supplied with a BDK-5, this command will derive the appropriate PIN encryption key using the Italian Standard Derivation Method SPE-DEF-041-112.

The Source Key may be a BDK-1, BDK-2 or BDK-5.

The Destination Key may be a BDK-1, BDK-2 or BDK-4.

3DES PIN encryption keys cannot be used with PIN block format code 48.

AES PIN encryption keys can only be used with PIN block format code 48.

Field	Length & Type	Details									
COMMAND MESSAGE											
Message Header	m A	Subsequently returned to the Host unchanged.									
Command Code	2 A	Value 'G0' (G-zero).									
Source Key Flag	1 A	For a Variant LMK only. Value '~' (X'7E). Optional; if present, this flag indicates that the supplied BDK is a BDK-2.									
Source Key	32 H or 'U' + 32 H or 'S' + n A	The key used to decrypt the source PIN block. Three types of BDK are supported: BDK-1, BDK-2 and BDK-5. For a Variant LMK: If the 'Source Key Flag' is not present, this key must be a BDK-1, encrypted under LMK pair 28-29. If the 'Source Key Flag' is present, this key must be a BDK-2, encrypted under LMK pair 28-29 variant 6. For a Key Block LMK: This key must be a BDK-1, BDK-2 or BDK-5, and comply with the following:									
		<table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'B0', '41'</td> <td>T', 'A'</td> <td>'X', 'N'</td> </tr> <tr> <td>'44'</td> <td>T'</td> <td>'X', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'B0', '41'	T', 'A'	'X', 'N'	'44'	T'	'X', 'N'
Key Usage	Algorithm	Mode of Use									
'B0', '41'	T', 'A'	'X', 'N'									
'44'	T'	'X', 'N'									
Destination Key Flag	1 A	For a Variant LMK only. Value '*' (X'2A). Optional; if present, this flag indicates that the destination key is a BDK-1.									

Field	Length & Type	Details									
COMMAND MESSAGE											
Destination Key		<p>Value '~' (X'7E). Optional; if present, this flag indicates that the destination key is a BDK-2.</p> <p>Value '!' (X'21). Optional; if present, this flag indicates that the destination key is a BDK-4.</p>									
	16 H or 'U' + 32 H or 'T' + 48 H	<p>The key used to re-encrypt the destination PIN block.</p> <p>Four types of keys are supported: ZPK, BDK-1 and BDK-2 or BDK-4.</p> <p>For a Variant LMK:</p> <p>If 'Destination Key Flag' is not present, then this key must be a ZPK, encrypted under LMK 06-07.</p> <p>If 'Destination Key Flag' is '*', then this key must be a BDK-1, encrypted under LMK 28-29.</p> <p>If 'Destination Key Flag' is '~', then this key must be a BDK-2, encrypted under LMK 28-29/6.</p> <p>If 'Destination Key Flag' is '!', then this key must be a BDK-4, encrypted under LMK 28-29/9.</p>									
	or 'S' + n A	<p>For a Key Block LMK:</p> <p>This key must be either a ZPK or BDK-1, BDK-2 or BDK-4, and comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'P0', '72'</td><td>'D', 'T', 'A'</td><td>'B', 'E', 'N'</td></tr> <tr> <td>'B0', '41', '43'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'P0', '72'	'D', 'T', 'A'	'B', 'E', 'N'	'B0', '41', '43'	'T', 'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use									
'P0', '72'	'D', 'T', 'A'	'B', 'E', 'N'									
'B0', '41', '43'	'T', 'A'	'X', 'N'									
Source KSN Descriptor	3 H	<p>The descriptor for the Source KSN (Key Serial Number - in the next field). For further information see the <i>payShield 10K Host Programmer's manual</i>.</p> <p>If 'Source Key' is an AES BDK-1 or BDK-2, this field is ignored and should be set to '000'</p> <p>1st digit: Source BDK Identifier Length ('0' – 'F')</p> <p>2nd digit: Reserved. Should be '0'.</p> <p>3rd digit: Device Identifier Length ('0' – 'F')</p>									
Source Key Serial Number	12 - 20 H or 24 H	<p>The KSN supplied by the PIN pad. For further information, see the <i>payShield 10K Host Programmer's manual</i>.</p> <p>If the Source Key is 3DES this field will be 12 to 20 Hex digits</p> <p>If the Source Key is an AES BDK-1 or BDK-2 this field will be 24 Hex digits.</p> <p>The KSN supplied by the PIN pad. For further information see the <i>payShield 10K Host Programmer's manual</i>.</p>									
Destination KSN Descriptor	3 H	<p>Only present if the 'Destination Key' is a BDK</p> <p>If 'Destination Key' is an AES BDK-1 or BDK-4, this field is ignored and should be set to '000'</p> <p>The descriptor for the 'Destination KSN' (in the next field).</p> <p>1st digit: Destination BDK Identifier Length ('0' – 'F')</p> <p>2nd digit: Reserved. Should be '0'.</p> <p>3rd digit: Device Identifier Length ('0' – 'F')</p>									
Destination KSN	12 - 20 H or 24 H	<p>The Destination Key Serial Number, supplied by the host (emulating a DUKPT terminal).</p> <p>If the 'Destination Key' is a 3DES BDK-1, BDK-2 or BDK-4, this field will be 12 – 20 Hex digits.</p> <p>If the 'Destinatin Key' is an AES BDK-1 or BDK-4, this field will be 24 digits.</p>									
Source PIN Block	16 H or 32 H	<p>The Source PIN Block, encrypted using the Source Key, supplied by the POS PIN terminal.</p> <p>When using a DES Source Key, this field will be 16 H.</p> <p>When using an AES Source Key, this field will be 32 H.</p>									
Source PIN Block Format Code	2 N	<p>The format code for the 'Source PIN Block'. The format code for any currently enabled and permitted PIN block format may be specified.</p>									
Destination PIN Block Format Code	2 N	<p>The format code for the 'Destination PIN Block'. The format code for any currently enabled and permitted PIN block format may be specified, unless prohibited by one or more of the following security settings:</p> <ul style="list-style-type: none"> • "Restrict PIN block usage for PCI compliance" • "Enable PIN Block Format 34 as output format for PIN translations to ZPK" 									

Field	Length & Type	Details
COMMAND MESSAGE		
The following fields are required when the Source PIN Block and the Destination PIN Block use the same PAN.		
Primary Account Number (PAN)	n N or 18 H or 12 N	<p>The PAN that was used to form the Source PIN Block and to be used to form the Destination PIN Block.</p> <p>If 'Source PIN Block Format Code' or 'Destination PIN Block Format Code' is '48': The 12-19 digit PAN.</p> <p>If present, the delimiter below must also be present.</p> <p>If 'Source PIN Block Format Code' or 'Destination PIN Block Format Code' is '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left.</p> <p>For all other values of 'Source PIN Block Format Code' and 'Destination PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.</p>
Delimiter	1 A	<p>Value ';'. Only present if 'Source PIN Block Format Code' = '48' or 'Destination PIN Block Format Code' = '48'.</p>
The following fields are required when the Source PIN Block was formed using a token PAN (instead of the real PAN), and the Destination PIN Block needs to be formed using the real PAN.		
Source PAN	n N or 18 H or 12 N	<p>The PAN that was used to form the Source PIN Block.</p> <p>If 'Source PIN Block Format Code' is '48': The 12-19 digit Source PAN.</p> <p>If present, the delimiter below must also be present.</p> <p>If 'Source PIN Block Format Code' is '04': The 18 digit Source PAN excluding the check digit. If the Source PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left.</p> <p>For all other values of 'Source PIN Block Format Code': The 12 right-most digits of the Source PAN, excluding the check digit.</p>
Delimiter	1 A	<p>Value ';'. Only present if 'Source PIN Block Format Code' = '48'.</p>
Destination PAN Delimiter	1 A	<p>Value ';'. Always required.</p>
Destination PAN	n N or 18 H or 12 N	<p>The PAN to be used to form the Destination PIN Block.</p> <p>If 'Destination PIN Block Format Code' is '48': The 12-19 digit Destination PAN.</p> <p>If present, the delimiter below must also be present.</p> <p>If 'Destination PIN Block Format Code' is '04': The 18 digit Destination PAN excluding the check digit. If the Destination PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left.</p> <p>For all other values of 'Destination PIN Block Format Code': The 12 right-most digits of the Destination PAN, excluding the check digit.</p>
Delimiter	1 A	<p>Value ';'. Only present if 'Destination PIN Block Format Code' is '48'.</p>
Delimiter	1 A	<p>Value '%'. Optional; if present, the following field must also be present.</p>
LMK Identifier	2 N	<p>LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.</p>
End Message Delimiter	1 C	<p>Must be present if a message trailer is present. Value X'19.</p>
Message Trailer	n A	<p>Optional. Maximum length 32 characters.</p>

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'G1'.
Error Code	2 A	'00': No error '10': BDK parity error '11': Interchange key parity error '17': PIN translation disabled '27': BDK not double or triple length '68': Command disabled '69': PIN Block format has been disabled '88': Warning: PIN Block contains a zero length PIN or a standard error code.
PIN Length	2 N	Length of the translated PIN. Note: If the security setting "Return PIN length in PIN translation response" is "NO", this field will be set to "00".
Destination PIN Block	16 H or 32 H	The PIN block encrypted under the Destination Key and formatted according to the Destination PIN Block Format Code. When using a DES Destination Key, this field will be 16 H. When using an AES Destination Key, this field will be 32 H.
Destination PIN block format code	2 N	Returned to the Host unchanged.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a PIN Using the IBM Offset Method (3DES & AES DUKPT)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a PIN using the IBM offset method.

This command can optionally verify a MAC using a DUKPT MAC Key

Notes: The command performs the same function as DA and EA, except the Host supplies the HSM with the information necessary to compute the current key. The PIN Block and the KSN originate from the DUKPT terminal.

The ANSI X9.24-1:2009 method for DUKPT key derivation is used when a 3DES BDK is supplied.

The ANSI X9.24-3:2017 method for DUKPT key derivation is used when an AES BDK is supplied.

When supplied with a BDK-5, this command will derive the appropriate PIN encryption key using the Italian Standard Derivation Method SPE-DEF-041-112.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues verifying the PIN using 3DES in place of DES. (Double-length PVKs are now acceptable, but the returned error code has not been changed to allow for backward compatibility with existing Host applications which are expecting Error Code 02 to be returned.)

If MAC verification is required, the HSM will derive a transaction key from the supplied BDK, and apply a variant to that transaction key to produce the MAC key. The MAC key is used to verify "request" MACs originating from the terminal.

This command supports both bidirectional and unidirectional (DUKPT) PIN keys and MAC keys.

Caution: The behavior of this command is affected by the following CS (Configure Security) console command setting:

Decimalization Table: Encrypted/Plaintext [E/P]

- When set to 'E' (the default setting), the supplied decimalization table must be encrypted (using console command ED), and will consist of 16 hexadecimal digits (for a Variant or 3DES Key Block LMK) or 'L' + 32 hexadecimal digits (for an AES Key Block LMK).
- When set to 'P', the supplied decimalization table must be plaintext, and will consist of 16 decimal digits.

The behavior of this command is affected by the following CS (Configure Security) console command setting:

Decimalization Table checks enabled? [Yes/No]

- When set to 'Yes' (the default setting), the decimalization table must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, error code 25 is returned.
- When set to 'No', the decimalization table is not checked.

Field	Length & Type	Details														
COMMAND MESSAGE																
Message Header	m A	Subsequently returned to the Host unchanged.														
Command Code	2 A	Value 'GO' (G-oh).														
Mode	1 N	Indicates the operation of the Function: '0': PIN Verify only (using a bidirectional PIN key) '1': PIN Verify and MAC Verify '2': PIN Verify only (using a unidirectional PIN key) When using a Key Block LMK: '0': PIN Verify only '1': PIN Verify and MAC Verify														
MAC Mode	1 A	Present only for Mode = '1': '1' & 'A': Verify 8 byte MAC '2' & 'B': Verify 4 byte MAC (leftmost 4 bytes) '3' & 'C': Verify 4 byte MAC (rightmost 4 bytes) '1' ... '3' are for verifying MACs using a bidirectional MAC key. 'A' ... 'C' are for verifying MACs using a unidirectional MAC key.														
MAC Method	1 N	Present only for Mode = '1': '1': X9.19 '2': CBC MAC (for an AES BDK only) '3': CMAC (for an AES BDK only)														
BDK	32 H or 'U' + 32 H or 'S' + n A	The Base Derivation Key, used to decrypt the PIN block and optionally verify the MAC. Three types of BDK are supported: BDK-1, BDK-2 and BDK-5. For a Variant LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' ... '3', this key must be a BDK-1, encrypted under LMK pair 28 29. If Mode = '2', or if Mode = '1' and MAC Mode = 'A' ... 'C', this key must be a BDK-2, encrypted under LMK pair 28-29 variant 6.														
PVK		For a Key Block LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' ... '3', this key must be a BDK-1 or BDK-5, and comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'B0'</td> <td>T', 'A'</td> <td>'X', 'N'</td> </tr> <tr> <td>'44'</td> <td>T'</td> <td>'X', 'N'</td> </tr> </table> If Mode = '2', or if Mode = '1' and MAC Mode = 'A' ... 'C', this key must be a BDK-2, and comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'41'</td> <td>T', 'A'</td> <td>'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'B0'	T', 'A'	'X', 'N'	'44'	T'	'X', 'N'	Key Usage	Algorithm	Mode of Use	'41'	T', 'A'
Key Usage	Algorithm	Mode of Use														
'B0'	T', 'A'	'X', 'N'														
'44'	T'	'X', 'N'														
Key Usage	Algorithm	Mode of Use														
'41'	T', 'A'	'X', 'N'														
KSN Descriptor	16 H or 'U' + 32 H or T' + 48 H or 'S' + n A	The PIN Verification Key, used to verify the customer PIN. For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0. For a Key Block LMK, the 'PVK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'V1'</td> <td>'D', 'T'</td> <td>'C', 'V', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'V1'	'D', 'T'	'C', 'V', 'N'								
Key Usage	Algorithm	Mode of Use														
'V1'	'D', 'T'	'C', 'V', 'N'														
Key Serial Number	3 H	The descriptor for the KSN (in the next field). For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i> . This field is ignored when using an AES BDK-1 or BDK-2 and should be set to '000'. The KSN supplied by the PIN pad. For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i> .														
PIN Block	12 - 20 H or 24 16 H or 32 H	For a 3DES BDK-1 or BDK-2, this field is 12-20 H. For an AES BDK-1 or BDK-2, this field is 24 H. Encrypted PIN block received from the POS PIN terminal. When using a DES BDK, this field will be 16 H. When using an AES BDK, this field will be 32 H.														

Field	Length & Type	Details
PIN Block Format Code	2 N	Restricted to the following: '01': ISO 9564-1 / ANSI X9.8 Format 0 '04': Plus format '05': ISO 9564-1 / ANSI X9.8 Format 1 '47': ISO 9564-1 / ANSI X9.8 Format 3 '48': ISO 9564-1 / ANSI X9.8 Format 4
Check Length	2 N	Minimum PIN Length: 4..12
Primary Account Number (PAN)	n N or 18 H or 12 N	The Primary Account Number, used to form the PIN Block. If 'PIN Block Format Code' = '48': The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present. If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.
Delimiter	1 A	Value ';'. Only present if 'PIN Block Format Code' = '48'.
Decimalization Table	16 N or 16 H or 'K' + 3 H or 'L' + 32 H	16 N when using Plaintext decimalization tables. 16 H when using Encrypted decimalization tables and a Variant LMK or 3DES Key Block LMK. 'K' + 3 H when referencing a decimalization table held in the HSM's User Storage Area. 'L' + 32 H when using Encrypted decimalization tables and an AES Key Block LMK.
PIN Validation Data	12 A or 'P' + 16 H	User-defined data consisting of hexadecimal characters and the character 'N', which indicates to the HSM where to insert the last 5 digits of the PAN; or User-defined data consisting of the ASCII character 'P' followed by 16 hexadecimal digits which will be used as input to the PIN generation algorithm.
Offset	12 H	The IBM offset value, left-justified and padded with 'F's.
MAC	8 H or 16 H	Only present for Mode = '1'. MAC to be verified. 16 H if MAC Mode = '1' or 'A'. 8 H if MAC Mode = '2', '3', 'B' or 'C'.
Message Data Length	4 N	Only present for Mode = '1'. Length of next field in bytes. Must be multiple of 8 bytes.
Message Data	n B	Only present for Mode = '1'. Data for which MAC is to be verified.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'GP'.
Error Code	2 A	'00': No error '01': PIN Verification failure '06': Invalid offset length '10': BDK parity error '11': PVK error '27': BDK not double length '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
MAC Error Code	2 N	Present only for Mode = '1'. '00': No error '01': MAC Verification failure
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a PIN Using the ABA PVV Method (3DES & AES DUKPT)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a PIN using the ABA PVV method.

This command can optionally verify a MAC using a DUKPT MAC Key.

This command supports the verification of PIN blocks built using a Token instead of the real PAN. This functionality is only supported if the security setting "*Enable use of Tokens in PIN Verification*" has the value "Y".

Notes: The command performs the same function as DC and EC, except the Host supplies the HSM with the information necessary to compute the current key. The PIN Block and the KSN originate from the DUKPT terminal.

The ANSI X9.24-1:2009 method for DUKPT key derivation is used when a 3DES BDK is supplied.

The ANSI X9.24-3:2017 method for DUKPT key derivation is used when an AES BDK is supplied.

When supplied with a BDK-5, this command will derive the appropriate PIN encryption key using the Italian Standard Derivation Method SPE-DEF-041-112.

If MAC verification is required, the HSM will derive a transaction key from the supplied BDK, and apply a variant to that transaction key to produce the MAC key. The MAC key is used to verify "request" MACs originating from the terminal. This command supports both bidirectional and unidirectional (DUKPT) MAC keys.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'GQ'.
Mode	1 N	Indicates the operation of the Function: '0': PIN Verify Only '1': PIN Verify and MAC Verify '2': PIN Verify only, using a unidirectional BDK. When using a Key Block LMK: '0': PIN Verify only '1': PIN Verify and MAC Verify
MAC Mode	1 A	Present only for Mode = '1': '1' & 'A': Verify 8 byte MAC '2' & 'B': Verify 4 byte MAC (leftmost 4 bytes) '3' & 'C': Verify 4 byte MAC (rightmost 4 bytes) '1' ... '3' are for verifying MACs using bidirectional MAC keys. 'A' ... 'C' are for verifying MACs using unidirectional MAC keys.
MAC Method	1 N	Present only for Mode = '1': '1': X9.19 '2': CBC MAC (for an AES BDK only) '3': CMAC (for an AES BDK only)
BDK		The Base Derivation Key, used to decrypt the PIN block and optionally verify the MAC. Three types of BDK are supported: BDK-1, BDK-2 and BDK-5.

Field	Length & Type	Details															
PVK	32 H or 'U' + 32 H	For a Variant LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' ... '3', this key must be a BDK-1, encrypted under LMK pair 28-29. If Mode = '2', or if Mode = '1' and MAC Mode = 'A' ... 'C', this key must be a BDK-2, encrypted under LMK pair 28-29 variant 6.															
	or 'S' + n A	For a Key Block LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' ... '3', this key must be a BDK-1 or BDK-5, and comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'B0'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> <tr> <td>'44'</td><td>'T'</td><td>'X', 'N'</td></tr> </tbody> </table> If Mode = '2', or if Mode = '1' and MAC Mode = 'A' ... 'C', this key must be a BDK-2, and comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'41'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'B0'	'T', 'A'	'X', 'N'	'44'	'T'	'X', 'N'	Key Usage	Algorithm	Mode of Use	'41'	'T', 'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use															
'B0'	'T', 'A'	'X', 'N'															
'44'	'T'	'X', 'N'															
Key Usage	Algorithm	Mode of Use															
'41'	'T', 'A'	'X', 'N'															
KSN Descriptor	32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0. For a Key Block LMK, the 'PVK' must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'V2'</td><td>'T'</td><td>'C', 'V', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'V2'	'T'	'C', 'V', 'N'									
Key Usage	Algorithm	Mode of Use															
'V2'	'T'	'C', 'V', 'N'															
Key Serial Number	12 - 20 H or 24 H	The descriptor for the KSN (in the next field). For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i> . This field is ignored when using an AES BDK-1 or BDK-2 and should be set to '000'. The KSN supplied by the PIN pad. For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i> .															
PIN Block	16 H or 32 H	For a 3DES BDK-1 or BDK-2, this field is 12-20 H. For an AES BDK-1 or BDK-2, this field is 24 H.															
PIN Block Format Code	2 N	The encrypted PIN block received from the POS PIN terminal. When using a DES BDK, this field will be 16 H. When using an AES BDK, this field will be 32 H. Restricted to the following: '01': ISO 9564-1 / ANSI X9.8 Format 0 '04': Plus format '05': ISO 9564-1 / ANSI X9.8 Format 1 '47': ISO 9564-1 / ANSI X9.8 Format 3 '48': ISO 9564-1 / ANSI X9.8 Format 4															

payShield 10K Core Host Commands

Field	Length & Type	Details
Primary Account Number (PAN) or Token	n N	If 'PIN Block' uses a token instead of the actual PAN, this field will contain the token number. Otherwise, it will contain the PAN.
	or 18 H	If 'PIN Block Format Code' = '48': The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present.
	or 12 N	If 'PIN Block Format Code' = '04': The 18 digit PAN/Token excluding the check digit. If the PAN/Token is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN/Token, excluding the check digit.
Delimiter	1 A	Value ';'. Only present if 'PIN Block Format Code' = '48'.
The following 2 or 3 fields are required when the PIN Block was formed using a Token (instead of the real PAN), and the PIN Verification Value (PVV) needs to be formed using the real PAN.		
Verification PAN Delimiter	1 A	Value ';'. Optional; if present, the following field must also be present. Only allowed if the security setting "Enable use of Tokens in PIN Verification" is set to "Y".
Verification PAN	n N	Only present if 'Verification PAN Delimiter' is present.
	or 12 N	If 'PIN Block Format Code' = '48': The 12-19 digit Verification PAN, including the check digit. If present, the delimiter below must also be present.
	or 12 N	For all other values of 'PIN Block Format Code': The 12 right-most digits of the Verification PAN, excluding the check digit.
Delimiter	1 A	Value ';'. Only present if 'PIN Block Format Code' = '48'.
PVKI	1 N	PIN Verification Key Index.
PVV	4 N	The PIN Verification Value from the card or database.
MAC	8 H or 16 H	Only present for Mode = '1'. MAC to be verified. 16 H if MAC Mode = '1' or 'A'. 8 H if MAC Mode = '2', '3', 'B' or 'C'.
	4 N	Only present for Mode = '1'. Length of next field in bytes. Must be multiple of 8 bytes.
Message Data Length	n B	Only present for Mode = '1'. Data for which MAC is to be verified.
Message Data	n B	Only present for Mode = '1'. Data for which MAC is to be verified.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'GR'.
Error Code	2 A	'00': No error '01': PIN Verification failure '10': BDK parity error '11': PVK error '17': PIN token validation disabled '27': BDK not double or triple length '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
MAC Error Code	2 N	Present only for Mode = '1': '00': No error '01': MAC Verification failure
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a PIN Using the Diebold Method (3DES & AES DUKPT)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a PIN using the Diebold method.

This command can optionally verify a MAC using a DUKPT MAC Key

Notes: The command performs the same function as CG and EG, except the Host supplies the HSM with the information necessary to compute the current key. The PIN Block and the KSN originate from the DUKPT terminal.

The ANSI X9.24-1:2009 method for DUKPT key derivation is used when a 3DES BDK is supplied..

The ANSI X9.24-3:2017 method for DUKPT key derivation is used when an AES BDK is supplied.

When supplied with a BDK-5, this command will derive the appropriate PIN encryption key using the Italian Standard Derivation Method SPE-DEF-041-112.

If MAC verification is required, the HSM will derive a transaction key from the supplied BDK, and apply a variant to that transaction key to produce the MAC key. The MAC key is used to verify "request" MACs originating from the terminal. This command supports both bidirectional and unidirectional (DUKPT) MAC keys.

The Diebold table must be stored in user storage before using this command.

If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", the Diebold table is encrypted using LMK pair 14-15 variant 0.

If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y", the Diebold table is encrypted using LMK pair 36-37 variant 6.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'GS'.
Mode	1 N	Indicates the operation of the Function: '0': PIN Verify Only '1': PIN Verify and MAC Verify '2': PIN Verify only (using a unidirectional PIN key) When using a Key Block LMK: '0': PIN Verify only '1': PIN Verify and MAC Verify
MAC Mode	1 A	Present only for Mode = '1': '1' & 'A': Verify 8 byte MAC '2' & 'B': Verify 4 byte MAC (leftmost 4 bytes) '3' & 'C': Verify 4 byte MAC (rightmost 4 bytes) '1' ... '3' are for verifying MACs using bidirectional MAC keys. 'A' ... 'C' are for verifying MACs using unidirectional MAC keys.
MAC Method	1 N	Present only for Mode = '1'. '1': ANSI X9.19 '2': CBC MAC (for an AES BDK only) '3': CMAC (for an AES BDK only)

Field	Length & Type	Details															
BDK	32 H or 'U' + 32 H	The Base Derivation Key, used to decrypt the PIN block and optionally verify the MAC. Three types of BDK are supported: BDK-1, BDK-2 and BDK-5. For a Variant LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' ... '3', this key must be a BDK-1, encrypted under LMK pair 28 29. If Mode = '2', or if Mode = '1' and MAC Mode = 'A' ... 'C', this key must be a BDK-2, encrypted under LMK pair 28-29 variant 6.															
	or 'S' + n A	For a Key Block LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' ... '3', this key must be a BDK-1 or BDK-5, and comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'B0'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> <tr> <td>'44'</td><td>'T'</td><td>'X', 'N'</td></tr> </tbody> </table> If Mode = '2', or if Mode = '1' and MAC Mode = 'A' ... 'C', this key must be a BDK-2, and comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'41'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'B0'	'T', 'A'	'X', 'N'	'44'	'T'	'X', 'N'	Key Usage	Algorithm	Mode of Use	'41'	'T', 'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use															
'B0'	'T', 'A'	'X', 'N'															
'44'	'T'	'X', 'N'															
Key Usage	Algorithm	Mode of Use															
'41'	'T', 'A'	'X', 'N'															
Index Flag	1 A	Value 'K'.															
Base Index	3 H	The index pointing to the start of the Diebold table in user storage.															
Diebold Algorithm Number	2 H	The algorithm number required by the Diebold method.															
KSN Descriptor	3 H	The descriptor for the KSN (in the next field). For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i> . This field is ignored when using an AES BDK-1 or BDK-2 and should be set to '000'.															
Key Serial Number	12 - 20 H or 24 H	The KSN supplied by the PIN pad. For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i> . For a 3DES BDK-1 or BDK-2, this field is 12-20 H. For an AES BDK-1 or BDK-2, this field is 24 H.															
PIN Block	16 H or 32 H	The encrypted PIN block received from the POS PIN terminal. When using a DES BDK, this field will be 16 H. When using an AES BDK, this field will be 32 H.															
PIN Block Format Code	2 N	Restricted to the following: '01': ISO 9564-1 / ANSI X9.8 Format 0 '04': Plus format '05': ISO 9564-1 / ANSI X9.8 Format 1 '47': ISO 9564-1 / ANSI X9.8 Format 3 '48': ISO 9564-1 / ANSI X9.8 Format 4															
Primary Account Number (PAN)	n N	The Primary Account Number, used to form the PIN Block. If 'PIN Block Format Code' = '48': The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present. If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.															
Delimiter	1 A	Value ':'. Only present if 'PIN Block Format Code' = '48'.															
PIN Validation Data	16 H	User-defined data consisting of hexadecimal characters and the character 'N', which indicates to the HSM where to insert the last 5 digits of the PAN. The data must be right-justified and padded with 'F's.															
Offset	4 N	The Diebold offset value.															
MAC	8 H or 16 H	Only present for Mode = '1'. MAC to be verified. 16 H if MAC Mode = '1' or 'A'. 8 H if MAC Mode = '2', '3', 'B' or 'C'.															
Message Data Length	4 N	Only present for Mode = '1'. Length of next field in bytes. Must be multiple of 8 bytes															
Message Data	n B	Only present for Mode = '1'. Data for which MAC is to be verified															

payShield 10K Core Host Commands

Field	Length & Type	Details
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'GT'.
Error Code	2 A	'00': No error '01': PIN Verification failure '10': BDK parity error '27': BDK not double or triple length '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
MAC Error Code	2 N	Present only for Mode = '1': '00': No error '01': MAC Verification failure
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a PIN Using the Encrypted PIN Method (3DES & AES DUKPT)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a PIN using the Encrypted PIN method.

This command can optionally verify a MAC using a DUKPT MAC Key

Notes: The command performs the same function as BC and BE, except the Host supplies the HSM with the information necessary to compute the current key. The PIN Block and the KSN originate from the DUKPT terminal.

The ANSI X9.24-1:2009 method for DUKPT key derivation is used when a 3DES BDK is supplied.

The ANSI X9.24-3:2017 method for DUKPT key derivation is used when an AES BDK is supplied.

When supplied with a BDK-5, this command will derive the appropriate PIN encryption key using the Italian Standard Derivation Method SPE-DEF-041-112.

If MAC verification is required, the HSM will derive a transaction key from the supplied BDK, and apply a variant to that transaction key to produce the MAC key. The MAC key may be used to verify "request" MACs originating from the terminal. This command supports both bidirectional and unidirectional (DUKPT) MAC keys.

3DES PIN encryption keys cannot be used with PIN block format code 48.

AES PIN encryption keys can only be used with PIN block format code 48.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'GU'.
Mode	1 N	Indicates the operation of the Function: '0': PIN Verify only '1': PIN Verify and MAC Verify '2': PIN Verify only (using a unidirectional PIN key) When using a Key Block LMK: '0': PIN Verify only '1': PIN Verify and MAC Verify
MAC Mode	1 A	Present only for Mode = '1': '1' & 'A': Verify 8 byte MAC '2' & 'B': Verify 4 byte MAC (leftmost 4 bytes) '3' & 'C': Verify 4 byte MAC (rightmost 4 bytes) '1' ... '3' are for verifying MACs using bidirectional MAC keys. 'A' ... 'C' are for verifying MACs using unidirectional MAC keys.
MAC Method	1 N	Present only for Mode = '1'. '1': ANSI X9.19 '2': CBC MAC (for an AES BDK only) '3': CMAC (for an AES BDK only)
BDK	32 H or 'U' + 32 H	The Base Derivation Key, used to decrypt the PIN block and optionally verify the MAC. Three types of BDK are supported: BDK-1, BDK-2 and BDK-5. For a Variant LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' ... '3', this key must be a BDK-1, encrypted under LMK pair 28 29.

Field	Length & Type	Details															
	or 'S' + n A	If Mode = '2', or if Mode = '1' and MAC Mode = 'A' ... 'C', this key must be a BDK-2, encrypted under LMK pair 28-29 variant 6. For a Key Block LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' ... '3', this key must be a BDK-1 or BDK-5, and comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'B0'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> <tr> <td>'44'</td><td>'T'</td><td>'X', 'N'</td></tr> </tbody> </table> If Mode = '2', or if Mode = '1' and MAC Mode = 'A' ... 'C', this key must be a BDK-2, and comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'41'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'B0'	'T', 'A'	'X', 'N'	'44'	'T'	'X', 'N'	Key Usage	Algorithm	Mode of Use	'41'	'T', 'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use															
'B0'	'T', 'A'	'X', 'N'															
'44'	'T'	'X', 'N'															
Key Usage	Algorithm	Mode of Use															
'41'	'T', 'A'	'X', 'N'															
KSN Descriptor	3 H	The descriptor for the KSN (in the next field). For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i> .															
Key Serial Number	12 - 20 H or 24 H	The KSN supplied by the PIN pad. For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i> . For a 3DES BDK-1 or BDK-2, this field is 12-20 H. For an AES BDK-1 or BDK-2, this field is 24 H.															
PIN Block	16 H or 32 H	The encrypted PIN block received from the POS PIN terminal. When using a DES BDK, this field will be 16 H. When using an AES BDK, this field will be 32 H.															
PIN Block Format Code	2 N	Restricted to the following: '01': ISO 9564-1 / ANSI X9.8 Format 0 '04': Plus format '05': ISO 9564-1 / ANSI X9.8 Format 1 '47': ISO 9564-1 / ANSI X9.8 Format 3 '48': ISO 9564-1 / ANSI X9.8 Format 4															

For a 3DES Variant or 3DES Key Block LMK, the following field must be present:

Primary Account Number (PAN)	18 H or 12 N	The PAN, used to form the PIN Block. If 'PIN Block Format Code' = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of 'PIN Block Format Code': The 12 right-most digits of the PAN, excluding the check digit.
------------------------------	--------------------	--

For an AES Key Block LMK, the following two fields must be present:

Primary Account Number (PAN)	n N	The PAN, used to form the PIN Block.
Delimiter	1 A	The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present. Value ':'.
PIN	L N or L H or 'M' + 32 H	The PIN from the host database, encrypted under the LMK. When using a 3DES Variant or Key Block LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Key Block LMK, this field must consist of a 'M' followed by 32 hex digits.
MAC	8 H or 16 H	Only present for Mode = '1'. The MAC to be verified: 16 H if MAC Mode = '1' or 'A'. 8 H if MAC Mode = '2', '3', 'B' or 'C'.
Message Data Length	4 N	Only present for Mode = '1'. Length of next field in bytes. Must be multiple of 8 bytes.
Message Data	n B	Only present for Mode = '1'. Data for which MAC is to be verified.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'GV'.
Error Code	2 A	'00': No error '01': PIN Verification failure '10': BDK parity error '11': PVK error '27': BDK not double or triple length '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
MAC Error Code	2 N	Present only for Mode = '1': '00': No error '01': MAC Verification failure
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate/Verify a MAC (3DES & AES DUKPT)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate or Verify a MAC on Message Data using a MAC Key derived according to the DUKPT method.

Notes: The ANSI X9.24-1:2009 method for DUKPT key derivation is used when a 3DES BDK is supplied.

The ANSI X9.24-3:2017 method for DUKPT key derivation is used when an AES BDK is supplied.

As part of this command, the HSM will derive a transaction key from the supplied BDK, and apply a variant to it in order to produce the MAC key. The variant will vary depending on the type of BDK being used, and whether the operation involves MAC generation or MAC verification.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'GW'.
MAC Mode	1 A	<p>Indicates the mode of operation:</p> <p>'1', 'A', 'G': Verify 8/16 byte MAC '2', 'B', 'H': Verify 4 byte MAC (4 leftmost bytes of MAC) '3', 'C', 'I': Verify 4 byte MAC (4 rightmost bytes of MAC) '4', 'D', 'J': Generate 8/16 byte MAC '5', 'E', 'K': Generate 4 byte MAC (4 leftmost bytes of MAC) '6', 'F', 'L': Generate 4 byte MAC (4 rightmost bytes of MAC)</p> <p>Use '1' ... '6' when using BDK-1 (bidirectional MAC keys). Use 'A' ... 'C' when using BDK-2 (unidirectional 'request' MAC keys). Use 'D' ... 'F' when using BDK-2 (unidirectional 'response' MAC keys). Use 'G' ... 'I' when using BDK-4 (unidirectional 'response' MAC keys). Use 'J' ... 'L' when using BDK-4 (unidirectional 'request' MAC keys).</p>
MAC Method	1 N	<p>Indicates the MAC algorithm:</p> <p>'1': ANSI X9.19 – 8 byte MAC '2': AS2805.4.1 (2001) – 8 byte MAC '3': CBC MAC (for an AES BDK only) – 8 byte MAC '4': CMAC (for an AES BDK only) – 8 byte MAC '5': CMAC (for an AES BDK only) – 16 byte MAC</p>

Field	Length & Type	Details																		
COMMAND MESSAGE																				
BDK	32 H or 'U' + 32 H	<p>The Base Derivation Key, used to derive the MAC key. Two types of BDK are supported: BDK-1, BDK-2 & BDK-4.</p> <p>For a Variant LMK: If MAC Mode = '1' ... '6', this key must be a BDK-1, encrypted under LMK pair 28-29. If MAC Mode = 'A' ... 'F', this key must be a BDK-2, encrypted under LMK pair 28-29 variant 6. If MAC Mode = 'G' ... 'L', this key must be a BDK-4, encrypted under LMK pair 28-29 variant 9.</p>																		
	or 'S' + n A	<p>For a Key Block LMK: For MAC Mode = '1' ... '6', this key must be a BDK-1, and comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'B0'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> </table> <p>For MAC Mode = 'A' ... 'F', this key must be a BDK-2, and comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'41'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> </table> <p>For MAC Mode = 'G' ... 'L', this key must be a BDK-4, and comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'43'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'B0'	'T', 'A'	'X', 'N'	Key Usage	Algorithm	Mode of Use	'41'	'T', 'A'	'X', 'N'	Key Usage	Algorithm	Mode of Use	'43'	'T', 'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use																		
'B0'	'T', 'A'	'X', 'N'																		
Key Usage	Algorithm	Mode of Use																		
'41'	'T', 'A'	'X', 'N'																		
Key Usage	Algorithm	Mode of Use																		
'43'	'T', 'A'	'X', 'N'																		
KSN Descriptor	3 H	<p>The descriptor for the KSN (in the next field). For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i>.</p> <p>This field is ignored when using an AES BDK-1, BDK-2 or BDK-4 and should be set to '000'.</p>																		
Key Serial Number	12 – 20 H or 24 H	<p>The KSN supplied by the PIN Pad. For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i>.</p> <p>For a 3DES BDK-1, BDK-2 or BDK-4, this field is 12-20 H. For an AES BDK-1, BDK-2 or BDK-4, this field is 24 H.</p>																		
MAC	8 H or 16 H or 32 H	<p>Only present for MAC Mode = '1', '2', '3', 'A', 'B', 'C', 'G', 'H' or 'I'. MAC to be verified: 32 H if MAC Mode = '1', 'A' or 'G' and MAC Method = '5'. 16 H if MAC Mode = '1', 'A' or 'G' and MAC Method = '1', '2', '3' or '4'. 8 H if MAC Mode = '2', '3', 'B', 'C', 'H' or 'I'.</p>																		
Message Data Length	4 N	<p>Length of next field in bytes. If MAC Method = 1, 2 or 3, this value must be a multiple of 8 bytes.</p>																		
Message Data	n B	Data for which MAC is to be generated/verified.																		
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.																		
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.																		
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.																		
Message Trailer	n A	Optional. Maximum length 32 characters.																		

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'GX'.
Error Code	2 A	'00': No error '01': MAC Verification Failure '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
MAC	8 H or 16 H or 32 H	Only present if MAC Mode is '4', '5', '6', 'D', 'E', 'F', 'J', 'K' or 'L'. The MAC generated on the Message Data: 32 H if MAC Mode is '4', 'D' or 'J' and MAC Method = '5'. 16 H if MAC Mode is '4', 'D', or 'J' and MAC Method = '1', '2', '3' or '4'. 8 H if MAC Mode is '5', '6', 'E', 'F', 'K' or 'L'.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

6 Data Protection Commands

6.1 Message Integrity Commands

The Message Authentication Code (MAC) can be computed to verify that a message transferred by a telecommunications network has not been altered. This method involves submitting sensitive elements of a message to DES with a secret key.

The originator appends the MAC to the message. The recipient uses the same elements and secret key to compute the MAC and compares it with the one sent by the originator. If the two agree, the message is accepted as valid.

The user chooses several parameters:

- Which fields to use in the MAC computation, the order of the fields, their format, and any editing criteria.
- Character coding (for example, whether or not data is represented in ASCII or EBCDIC).
- DES key management: although not part of DES, secure key storage and transmission are vital to the integrity of the MAC.

HSM transactions assume:

- The Host computer is responsible for all data editing. The HSM is supplied with a variable-length data field for MAC computation, and except for zero filling of the last 64-bit block, uses all supplied data in the order provided.
- All MACs are computed on ASCII data (EBCDIC data is converted to ASCII before computation).

The payShield 10K provides commands to generate, verify and translate a MAC.

Because the HSM has no flow control, the application programmer is responsible for ensuring that the input buffer is not exceeded. The HSM input buffer is 32K bytes per connection in length. The length of the input buffer limits the amount of data over which a MAC can be calculated in a single call to the HSM.

When the HSM is in EBCDIC mode (using the CH (Configure Host) console command), the HSM calculates a MAC by converting any text characters to ASCII. The HSM performs no other editing of the data.

The payShield 10K provides the following host commands to support generic MAC operations:

Function	Command	Page
Generate MAC	M6 (M7)	420
Verify MAC	M8 (M9)	423
Verify and Translate MAC	MY (MZ)	426
Generate an RSA/ECC Signature	EW (EX)	430
Validate an RSA/ECC Signature	EY (EZ)	433
Hash a Block of Data	GM (GN)	435

Note: Other (legacy) MAC commands exist – see the payShield 10K Legacy Commands manual.

Generate MAC

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate a MAC on a message using a TAK or ZAK.

This command supports the use of a variety of MAC algorithms and padding modes, as described in the command message below.

Notes: The message to be MAC'd by this command may be presented to the HSM in different formats, as indicated by the Input Format Flag field.

Note: When Input Format Flag = 2, the input message goes through a conversion process (from EBCDIC to ASCII) when the HSM is configured as using EBCDIC.

When using Thales Key Blocks, the key block's Key Usage field will determine which MAC algorithms & padding methods are permitted:

Key Usage	Algorithm	Permitted MAC algorithms	Permitted MAC padding methods
'M1'	'D', 'T'	ISO 9797 MAC algorithm 1	One of: <ul style="list-style-type: none"> • No padding. • ISO 9797 Padding method 1 • ISO 9797 Padding method 2 • ISO 9797 Padding method 3
'M3'	'T'	ISO 9797 MAC algorithm 3	
'M5'	'A'	CBC MAC	
'M6'	'A'	CMAC	AES CMAC padding.

The maximum value for the Message Length field will be dependent on the format of the message, but the maximum length of the overall command is 32K bytes.

When a MAC is required to be generated on a multi-block message using MAC Algorithm '3' (ISO 9797 MAC algorithm 3, equivalent to ANSI X9.19), then the intermediate IV will be encrypted under a key derived from the MAC key.

When generating a MAC using multiple message blocks (i.e. Mode Flag = '1', '2' or '3'), there is a minimum length to the separate message blocks:

- For multi-block MACs using 3DES: each supplied message block must be at least 24 bytes (binary/text) or 48 hex characters.
- For multi-block MACs using AES: each supplied message block must be at least 48 bytes (binary/text) or 96 hex characters.

Field	Length & Type	Details										
COMMAND MESSAGE												
Message Header	m A	Subsequently returned to the Host unchanged.										
Command Code	2 A	Value 'M6'.										
Mode Flag	1 N	'0': Only block of a single-block message '1': First block of a multi-block message '2': Middle block of a multi-block message '3': Final block of a multi-block message.										
Input Format Flag	1 N	'0': Binary '1': Hex-Encoded Binary '2': Text.										
MAC Size	1 N	'0': MAC size of 8 hex digits '1': MAC size of 16 hex digits '2': MAC size of 32 hex digits (only valid for MAC Algorithm '6' CMAC) '3' ... '9': Reserved for future use.										
MAC Algorithm	1 N	'1': ISO 9797 MAC algorithm 1 (= ANSI X9.9 when used with a single-length key) (DES only) '3': ISO 9797 MAC algorithm 3 (= ANSI X9.19 when used with a double-length key) (DES only) '5': CBC-MAC (AES only) '6': CMAC (AES only) '0', '2', '4', '7' ... '9': Reserved for future use.										
Padding Method	1 N	For MAC Algorithm values '1', '3' & '5': '0': No padding. (Overall message length must be multiple of 8 bytes for MAC Algorithm 1 & 3; and must be a multiple of 16 bytes for MAC Algorithm 5.) '1': ISO 9797 Padding method 1 (i.e. pad with 0x00). '2': ISO 9797 Padding method 2 (i.e. add 0x80 and pad with 0x00). '3': ISO 9797 Padding method 3 (i.e. prepend message with length, pad with 0x00). Note that if Padding Method = '3', then Mode Flag must be set to '0'. For MAC Algorithm = '6': '4': AES CMAC Padding. '5' ... '9': Reserved for future use.										
Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be used. The following key types are permitted: '003': TAK (encrypted under LMK pair 16-17) '008': ZAK (encrypted under LMK pair 26-27)										
Key	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	For a Key Block LMK: This field is ignored; should be set to 'FFF'. The Message Authentication Key, used in conjunction with the IV, if appropriate, to generate the MAC.										
		For a Variant LMK, the 'Key' is either a TAK or ZAK, as specified above.										
IV	16 H or 32 H	For a Key Block LMK, the 'Key' must comply with one of the following:										
		<table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'M1'</td><td>'D', 'T'</td><td>'C', 'G', 'N'</td></tr> <tr> <td>'M3'</td><td>'T'</td><td>'C', 'G', 'N'</td></tr> <tr> <td>'M5', 'M6'</td><td>'A'</td><td>'C', 'G', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'M1'	'D', 'T'	'C', 'G', 'N'	'M3'	'T'	'C', 'G', 'N'	'M5', 'M6'
Key Usage	Algorithm	Mode of Use										
'M1'	'D', 'T'	'C', 'G', 'N'										
'M3'	'T'	'C', 'G', 'N'										
'M5', 'M6'	'A'	'C', 'G', 'N'										
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes.										
Message	n B or n H	The message to be MAC'd. The length & type of the field will depend on the value of the Mode Flag & Input Format Flag: Input Format Flag = '0' (Binary); If Mode Flag = '1' or '2', then n = multiple of 8 when using a DES key, or a multiple of 16 when using an AES key. Input Format Flag = '1' (Hex-Encoded Binary); If Mode Flag = '1' or '2', then n = multiple of 16 when using a DES key, or a multiple of 32 when using an AES key.										

Field	Length & Type	Details
	n A	Input Format Flag = '2' (Text); If Mode Flag = '1' or '2', then n = multiple of 8 when using a DES key, or a multiple of 16 when using an AES key.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'M7'.
Error Code	2 A	'00': No error '02': Invalid Mode Flag field '03': Invalid Input Format Flag field '04': Invalid MAC Algorithm field '05': Invalid Key Type field '06': Invalid Message Length field '09': Invalid Padding Method field '10': MAC Key Parity Error '68': Command disabled or a standard error code.
IV	16 H or 32 H	The intermediate IV. This IV should be supplied as input when MACing the next block in the series of blocks. If using a DES/3DES key, the IV will be a 16 H field. If using an AES key, the IV will be a 32 H field. Only present if Mode Flag = '1' or '2'.
MAC	8 H or 16 H or 32 H	The calculated MAC. The length of this field is determined by the input 'MAC Size' field. Only present if Mode Flag = '0' or '3'.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify MAC

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a MAC on a message using a TAK or ZAK.

This command supports the use of a variety of MAC algorithms and padding modes, as described in the command message below.

Notes: The message to be MAC'd by this command may be presented to the HSM in different formats, as indicated by the Input Format Flag field.

When Input Format Flag = 2, the input message goes through a conversion process (from EBCDIC to ASCII) when the HSM is configured as using EBCDIC.

When using Thales Key Blocks, the key block's Key Usage field will determine which MAC algorithms & padding methods are permitted:

Key Usage	Algorithm	Permitted MAC algorithms	Permitted MAC padding methods
'M1'	'D', 'T'	ISO 9797 MAC algorithm 1	One of: • No padding. • ISO 9797 Padding method 1 • ISO 9797 Padding method 2 • ISO 9797 Padding method 3
'M3'	'T'	ISO 9797 MAC algorithm 3	
'M5'	'A'	CBC MAC	
'M6'	'A'	CMAC	AES CMAC padding.

The maximum value for the Message Length field will be dependent on the format of the message, but the maximum length of the overall command is 32K bytes.

When a MAC is required to be validated on a multi-block message using MAC Algorithm '3' (ISO 9797 MAC algorithm 3, equivalent to ANSI X9.19), then the intermediate IV will be encrypted under a key derived from the MAC key.

When verifying a MAC using multiple message blocks (i.e. Mode Flag = '1', '2' or '3'), there is a minimum length to the separate message blocks:

- For multi-block MACs using 3DES: each supplied message block must be at least 24 bytes (binary/text) or 48 hex characters.
- For multi-block MACs using AES: each supplied message block must be at least 48 bytes (binary/text) or 96 hex characters.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'M8'.
Mode Flag	1 N	'0': Only block of a single-block message '1': First block of a multi-block message '2': Middle block of a multi-block message '3': Final block of a multi-block message.
Input Format Flag	1 N	'0': Binary '1': Hex-Encoded Binary '2': Text.
MAC Size	1 N	'0': MAC size of 8 hex digits '1': MAC size of 16 hex digits '2': MAC size of 32 hex digits (only valid for MAC Algorithm '6' CMAC) '3' ... '9': Reserved for future use.
MAC Algorithm	1 N	'1': ISO 9797 MAC algorithm 1 (= ANSI X9.9 when used with a single-length key) (DES only) '3': ISO 9797 MAC algorithm 3 (= ANSI X9.19 when used with a double-length key) (DES only) '5': CBC-MAC (AES only) '6': CMAC (AES only) '0', '2', '4', '7' ... '9': Reserved for future use.
Padding Method	1 N	For MAC Algorithm values '1', '3' & '5': '0': No padding. (Overall message length must be multiple of 8 bytes for MAC Algorithm 1 & 3; and must be a multiple of 16 bytes for MAC Algorithm 5.) '1': ISO 9797 Padding method 1 (i.e. pad with 0x00). '2': ISO 9797 Padding method 2 (i.e. add 0x80 and pad with 0x00). '3': ISO 9797 Padding method 3 (i.e. prepend message with length, pad with 0x00). Note that if Padding Method = '3', then Mode Flag must be set to '0'. For MAC Algorithm = '6': '4': AES CMAC Padding. '5' ... '9': Reserved for future use.
Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be used. The following key types are permitted: '003': TAK (encrypted under LMK pair 16-17) '008': ZAK (encrypted under LMK pair 26-27)
Key	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	For a Key Block LMK: This field is ignored; should be set to 'FFF'. The Message Authentication Key, used in conjunction with the IV, if appropriate, to verify the MAC. For a Variant LMK, the 'Key' is either a TAK or ZAK, as specified above.
IV	16 H or 32 H	The intermediate IV. When verifying the middle or final blocks of a series of blocks, this value should be the IV returned from MACing the previous block. If using a DES/3DES key, the IV will be a 16 H field. If using an AES key, the IV will be a 32 H field. Only present if Mode Flag = '2' or '3'.
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes.
Message	n B or n H	The message upon which the MAC is to be verified. The length & type of the field will depend on the value of the Mode Flag & Input Format Flag: Input Format Flag = '0' (Binary); If Mode Flag = '1' or '2', then n = multiple of 8 when using a DES key, or a multiple of 16 when using an AES key. Input Format Flag = '1' (Hex-Encoded Binary); If Mode Flag = '1' or '2', then n = multiple of 16 when using a DES key, or a multiple of 32 when using an AES key.

payShield 10K Core Host Commands

Field	Length & Type	Details
MAC	n A 8 H or 16 H or 32 H	<p>Input Format Flag = '2' (Text); If Mode Flag = '1' or '2', then n = multiple of 8 when using a DES key, or a multiple of 16 when using an AES key.</p> <p>The MAC to be verified. The length of this field is determined by the input 'MAC Size' field. Only present if Mode Flag = '0' or '3'.</p>
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'M9'.
Error Code	2 A	<p>'00': No error '01': MAC verification failed '02': Invalid Mode Flag field '03': Invalid Input Format Flag field '04': Invalid MAC Algorithm field '05': Invalid Key Type field '06': Invalid Message Length field '09': Invalid Padding Method field '10': MAC Key Parity Error '68': Command disabled or a standard error code.</p>
IV	16 H or 32 H	<p>The intermediate IV. This IV should be supplied as input when MACing the next block in the series of blocks. If using a DES/3DES key, the IV will be a 16 H field. If using an AES key, the IV will be a 32 H field. Only present if Mode Flag = '1' or '2'.</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify and Translate MAC

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify a MAC on a message using a TAK or ZAK and, if successful, generate a MAC on the same message using a different TAK or ZAK.

This command supports the use of a variety of MAC algorithms and padding modes, as described in the command message below.

Notes: The message with which the MAC is to be verified and translated may be presented to the HSM in different formats, as indicated by the Input Format Flag field.

When Input Format Flag = 2, the input message goes through a conversion process (from EBCDIC to ASCII) when the HSM is configured as using EBCDIC.

When using Thales Key Blocks, the key block's Key Usage field will determine which MAC algorithms & padding methods are permitted:

Key Usage	Algorithm	Permitted MAC algorithms	Permitted MAC padding methods
'M1'	'D', 'T'	ISO 9797 MAC algorithm 1	
'M3'	'T'	ISO 9797 MAC algorithm 3	For ISO 9797 MAC algorithms 1 and 3 and AES CBC MAC, one of: •No padding. •ISO 9797 Padding method 1 •ISO 9797 Padding method 2 •ISO 9797 Padding method 3
'M5'	'A'	CBC MAC	
'M6'	'A'	CMAC	
'B0'	'T'	One of: •ISO 9797 MAC algorithm 1 •ISO 9797 MAC algorithm 3	
'41'	'T'		
'43'	'T'		For AES CMAC: •AES CMAC padding.
'B0'	'A'	One of: •CBC MAC •CMAC	
'41'	'A'		
'43'	'A'		

If the source key is a BDK (key usage = 'B0', '41' or '43'), then the X9.24-3:2017 DUKPT method will be used to determine the MAC verification key. Both bidirectional and unidirectional MAC keys are supported, and the data will be assumed to be "request" data.

The maximum value for the Message Length field will be dependent on the format of the message, but the maximum length of the overall command is 32K bytes.

When a MAC is required to be validated or generated on a multi-block message using MAC Algorithm '3' (ISO 9797 MAC algorithm 3, equivalent to ANSI X9.19), then the intermediate IV will be encrypted under a key derived from the MAC key.

When generating or verifying a MAC using multiple message blocks (i.e. Mode Flag = '1', '2' or '3'), there is a minimum length to the individual message blocks:

- For multi-block MACs using 3DES: each supplied message block must be at least 24 bytes (binary/text) or 48 hex characters.
- For multi-block MACs using AES: each supplied message block must be at least 48 bytes (binary/text) or 96 hex characters.

Field	Length & Type	Details												
COMMAND MESSAGE														
Message Header	m A	Subsequently returned to the Host unchanged.												
Command Code	2 A	Value 'MY'.												
Mode Flag	1 N	'0': Only block of a single-block message '1': First block of a multi-block message '2': Middle block of a multi-block message '3': Final block of a multi-block message.												
Input Format Flag	1 N	'0': Binary '1': Hex-Encoded Binary '2': Text.												
Source MAC Size	1 N	'0': MAC size of 8 hex digits '1': MAC size of 16 hex digits '2' ... '9': Reserved for future use.												
Source MAC Algorithm	1 N	'1': ISO 9797 MAC algorithm 1 (= ANSI X9.9 when used with a single-length key) (DES only) '3': ISO 9797 MAC algorithm 3 (= ANSI X9.19 when used with a double-length key) (DES only) '5': CBC-MAC (AES only) '6': CMAC (AES only) '0', '2', '4', '7' ... '9': Reserved for future use.												
Source Padding Method	1 N	For Source MAC Algorithm values '1', '3' & '5': '0': No padding. (Overall message length must be multiple of 8 bytes for MAC Algorithm 1 & 3; and must be a multiple of 16 bytes for MAC Algorithm 5.) '1': ISO 9797 Padding method 1 (i.e. pad with 0x00). '2': ISO 9797 Padding method 2 (i.e. add 0x80 and pad with 0x00). '3': ISO 9797 Padding method 3 (i.e. prepend message with length, pad with 0x00). Note that if Source Padding Method = '3', then Mode Flag must be set to '0'. For Source MAC Algorithm = '6': '4': AES CMAC Padding. '5' ... '9': Reserved for future use.												
Source Key Type	3 H	For a Variant LMK: Indicates the key type of the Source Key to be used. The following key types are permitted: '003': TAK (encrypted under LMK pair 16-17) '008': ZAK (encrypted under LMK pair 26-27) For a Key Block LMK: This field is ignored; should be set to 'FFF'.												
Source Key	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The Source Message Authentication Key, used in conjunction with the Source IV, if appropriate, to verify the supplied MAC. For a Variant LMK, the 'Source Key' is either a TAK or ZAK, as specified above.												
		For a Key Block LMK, the 'Source Key' must comply with one of the following: <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'M1'</td> <td>'D', 'T'</td> <td>'C', 'V', 'N'</td> </tr> <tr> <td>'M3'</td> <td>'T'</td> <td>'C', 'V', 'N'</td> </tr> <tr> <td>'M5', 'M6'</td> <td>'A'</td> <td>'C', 'V', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'M1'	'D', 'T'	'C', 'V', 'N'	'M3'	'T'	'C', 'V', 'N'	'M5', 'M6'	'A'	'C', 'V', 'N'
Key Usage	Algorithm	Mode of Use												
'M1'	'D', 'T'	'C', 'V', 'N'												
'M3'	'T'	'C', 'V', 'N'												
'M5', 'M6'	'A'	'C', 'V', 'N'												

Field	Length & Type	Details														
		'B0', '41', '43'	'T', 'A'	'X', 'N'												
Source KSN Descriptor	3 H	The descriptor for the KSN (in the next field). See the Host Programmer manual for further information. Only present if the Source Key is a BDK. If Source Key is an AES BDK-1 or BDK-2, this field is ignored and should be set to '000'.														
Source Key Serial Number	12 – 20 H or 24 H	The KSN supplied by the PIN pad. See the Host Programmer manual for further information. Only present if the Source Key is a BDK. If the Source Key is a 3DES BDK-1, BDK-2 or BDK-4, this field will be 12 to 20 Hex digits If the Source Key is an AES BDK-1, BDK-2 or BDK-4, this field will be 24 Hex digits														
Destination MAC Size	1 N	'0': MAC size of 8 hex digits '1': MAC size of 16 hex digits '2' ... '9': Reserved for future use.														
Destination MAC Algorithm	1 N	'1': ISO 9797 MAC algorithm 1 (= ANSI X9.9 when used with a single-length key) (DES only) '3': ISO 9797 MAC algorithm 3 (= ANSI X9.19 when used with a double-length key) (DES only) '5': CBC-MAC (AES only) '6': CMAC (AES only) '0', '2', '4', '7' ... '9': Reserved for future use.														
Destination Padding Method	1 N	For Destination MAC Algorithm values '1', '3' & '5': '0': No padding. (Overall message length must be multiple of 8 bytes for MAC Algorithm 1 & 3; and must be a multiple of 16 bytes for MAC Algorithm 5.) '1': ISO 9797 Padding method 1 (i.e. pad with 0x00). '2': ISO 9797 Padding method 2 (i.e. add 0x80 and pad with 0x00). '3': ISO 9797 Padding method 3 (i.e. prepend message with length, pad with 0x00). Note that if Destination Padding Method = '3', then Mode Flag must be set to '0'. For Destination MAC Algorithm = '6': '4': AES CMAC Padding. '5' ... '9': Reserved for future use.														
Destination Key Type	3 H	For a Variant LMK: Indicates the key type of the Destination Key to be used. The following key types are permitted: '003': TAK (encrypted under LMK pair 16-17) '008': ZAK (encrypted under LMK pair 26-27) For a Key Block LMK: This field is ignored; should be set to 'FFF'.														
Destination Key	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The Destination Message Authentication Key, used in conjunction with the Destination IV, if appropriate, to generate the new MAC. For a Variant LMK, the 'Destination Key' is either a TAK or ZAK, as specified above. For a Key Block LMK, the 'Destination Key' must comply with one of the following:	<table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'M1'</td><td>'D', 'T'</td><td>'C', 'G', 'N'</td></tr> <tr> <td>'M3'</td><td>'T'</td><td>'C', 'G', 'N'</td></tr> <tr> <td>'M5', 'M6'</td><td>'A'</td><td>'C', 'G', 'N'</td></tr> </tbody> </table>		Key Usage	Algorithm	Mode of Use	'M1'	'D', 'T'	'C', 'G', 'N'	'M3'	'T'	'C', 'G', 'N'	'M5', 'M6'	'A'	'C', 'G', 'N'
Key Usage	Algorithm	Mode of Use														
'M1'	'D', 'T'	'C', 'G', 'N'														
'M3'	'T'	'C', 'G', 'N'														
'M5', 'M6'	'A'	'C', 'G', 'N'														
Source IV	16 H or 32 H	The intermediate IV, calculated using the Source Key. This IV should be supplied as input when MACing the next block in the series of blocks. If using a DES/3DES Source Key, the Source IV will be a 16 H field. If using an AES Source key, the Source IV will be a 32 H field. Only present if Mode Flag = '2' or '3'.														
Destination IV	16 H or 32 H	The intermediate IV, calculated using the Destination Key. This IV should be supplied as input when translating the MAC on the next block in the series of blocks. If using a DES/3DES Destination Key, the Destination IV will be a 16 H field. If using an AES Destination Key, the Destination IV will be a 32 H field. Only present if Mode Flag = '2' or '3'.														
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes.														

Field	Length & Type	Details
Message	n B or n H or n A	The message upon which the MAC is to be verified and regenerated. The length & type of the field will depend on the value of the Mode Flag & Input Format Flag: Input Format Flag = '0' (Binary); If Mode Flag = '1' or '2', then n = multiple of 8 when using a DES key, or a multiple of 16 when using an AES key. Input Format Flag = '1' (Hex-Encoded Binary); If Mode Flag = '1' or '2', then n = multiple of 16 when using a DES key, or a multiple of 32 when using an AES key. Input Format Flag = '2' (Text); If Mode Flag = '1' or '2', then n = multiple of 8 when using a DES key, or a multiple of 16 when using an AES key.
	8 H or 16 H	The MAC to be verified using the Source Key. The length of this field is determined by the input 'Source MAC Size' field. Only present if Mode Flag = 0 or 3.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'MZ'.
Error Code	2 A	'00': No error '01': MAC verification failure '02': Invalid Mode Flag field '03': Invalid Input Format Flag field '04': Invalid Source MAC Algorithm field '05': Invalid Source Key Type field '06': Invalid Message Length field '07': Invalid Destination MAC Algorithm field '08': Invalid Destination Key Type field '09': Invalid Source Padding Method field '10': Source MAC Key Parity Error '11': Destination MAC Key Parity Error '34': Invalid Destination Padding Method field '68': Command disabled or a standard error code.
Source IV	16 H or 32 H	The intermediate IV, calculated using Source Key. If using a DES/3DES Source Key, the Source IV will be a 16 H field. If using an AES Source Key, the Source IV will be a 32 H field. Only present if Mode Flag = '1' or '2'.
Destination IV	16 H or 32 H	The intermediate IV, calculated using Destination Key. If using a DES/3DES Destination Key, the Destination IV will be a 16 H field. If using an AES Destination Key, the Destination IV will be a 32 H field. Only present if Mode Flag = '1' or '2'.
Destination MAC	8 H or 16 H	The MAC generated using the Destination Key. The length of this field is determined by the input 'Destination MAC Size' field. Only present if Mode Flag = '0' or '3'.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate an RSA/ECC Signature

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate a signature on a message using a private key, schemes supported: RSA & ECDSA.

Note: For information about support for the RSA algorithm, see the *payShield 10K Host Programmer's manual*.

Hash Identifier	Algorithm	Minimum RSA private key length	ECC private key curve
'01'	SHA-1	368 bits	-
'02'	MD5	360 bits	-
'03'	ISO 10118-2	320 bits	-
'04'	No Hash	320 bits	-
'05'	SHA-224	464 bits	-
'06'	SHA-256	496 bits	P-256
'07'	SHA-384	624 bits	P-384
'08'	SHA-512	752 bits	P-521

Additional note regarding use of "No Hash": If "Hash Identifier" = 04 (No hash), then the supplied "Message Data" field must consist of the ASN.1 DER encoding of the message digest, as described by PKCS#1.

For example, the following two scenarios will produce identical results:

Scenario 1: "Hash Identifier" = 06 (SHA-256) and "Message Data" = "raw data"

Scenario 2: "Hash Identifier" = 04 (No hash) and "Message Data" = ASN.1 DER(SHA-256(raw data)).

Sample ASN.1 DER Schema is as follows (refer to PKCS#1 for hash identifier values):

```
digestInfo ::= SEQUENCE {
    digestAlgorithm   SEQUENCE {
        algorithm      <hash identifier>
        parameters     NULL
    }
    digest          OCTET STRING
}
```

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'EW'.
Hash Identifier	2 N	Identifier of the hash algorithm used to hash the message: '01': SHA-1 '02': MD5 '03': ISO 10118-2 '04': No Hash '05': SHA-224

Field	Length & Type	Details												
Signature Identifier	2 N	'06': SHA-256 '07': SHA-384 '08': SHA-512 Identifier of the signature algorithm used to sign the message: '01': RSA '02': ECDSA												
Pad Mode Identifier	2 N	Only present if the Signature Identifier is '01': Identifier of the padding mode used in signature generation. '01': PKCS#1 v1.5 method (EMSA-PKCS1-v1_5) '04': PKCS#1 v2.2 method RSASSA-PSS (except Hash Identifier = '04') Note for Pad Mode Identifier = '04': <ul style="list-style-type: none">• the MGF hash function will use the hash algorithm defined by Hash Identifier;• the salt length will be the same length as the hash value.												
Signature Output Format	1 N	Only present if Signature Identifier is '02': '0': Plain format (simple concatenation of r, s) '1': ANSI X9.62 ASN.1 encoded (SEQUENCE {r INTEGER, s INTEGER})												
Data Length	4 N	Length (in bytes) of the message data to be signed.												
Message Data	n B	Data to be signed.												
Delimiter	1 A	Value ';'. Used to indicate the end of the message data field.												
Private Key Flag	2 N	Flag to indicate location of the private key to decrypt the encrypted key; '00' ... '20': index of stored private key '99': use private key provided with command.												
Private Key Length	4 N or 4 H	Optional. Must be present if the Private key flag = '99'. For a Variant LMK: Length (in bytes) of the next field. For a Key Block LMK: This field is ignored, and should be set to 'FFFF'.												
Private Key	n B or 'S' + n B	Optional. Must be present if the Private key flag = '99'. The Private Key, used to generate the signature. For a Variant LMK, the 'Private Key' is encrypted under LMK pair 34-35. For a Key Block LMK, the 'Private Key' must comply with the following: If Signature Identifier is '01' (RSA): <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'03', '06'</td> <td>'R'</td> <td>'S', 'B', 'N'</td> </tr> </table> If Signature Identifier is '02' (ECDSA): <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'03'</td> <td>'E'</td> <td>'S', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'03', '06'	'R'	'S', 'B', 'N'	Key Usage	Algorithm	Mode of Use	'03'	'E'	'S', 'N'
Key Usage	Algorithm	Mode of Use												
'03', '06'	'R'	'S', 'B', 'N'												
Key Usage	Algorithm	Mode of Use												
'03'	'E'	'S', 'N'												
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.												
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.												
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.												
Message Trailer	n A	Optional. Maximum length 32 characters.												

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'EX'.
Error Code	2 A	<p>'00': No error '03': Invalid private key type '04': Invalid private key flag '05': Invalid hash identifier '06': Invalid signature identifier '07': Invalid pad mode identifier '47': Algorithm not licensed '68': Command disabled '74': Invalid digest info syntax (no-hash mode only) '76': Hash length error '78': Private key length error '80': Message length error 'D2': Invalid Curve Reference value 'DB': Private key is greater than the order of curve 'DC': Invalid Signature Output Format value or a standard error code.</p>
Signature length	4 N	Length (in bytes) of the signature.
Signature	n B	Calculated signature.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Validate an RSA/ECC Signature

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Validate a signature on a message using a public key, schemes supported: RSA & ECDSA.

Note: For information about support for the RSA algorithm, see the *payShield 10K Host Programmer's manual*.

Hash Identifier	Algorithm	Minimum RSA private key length	ECC private key curve
'01'	SHA-1	368 bits	n/a
'02'	MD5	360 bits	n/a
'03'	ISO 10118-2	320 bits	n/a
'04'	No Hash	320 bits	n/a
'05'	SHA-224	464 bits	n/a
'06'	SHA-256	496 bits	P-256
'07'	SHA-384	624 bits	P-384
'08'	SHA-512	752 bits	P-521

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'EY'.
Hash Identifier	2 N	Identifier of the hash algorithm used to hash the message: '01': SHA-1 '02': MD5 '03': ISO 10118-2 '04': No Hash '05': SHA-224 '06': SHA-256 '07': SHA-384 '08': SHA-512
Signature Identifier	2 N	Identifier of the signature algorithm used to sign the message: '01': RSA '02': ECDSA
Pad Mode Identifier	2 N	If Signature Identifier is '01', the following field will be present Identifier of the pad mode used in signature generation. '01': PKCS#1 v1.5 method (EMSA-PKCS1-v1_5) '04': PKCS#1 v2.2 method RSASSA-PSS Note for Pad Mode Identifier = '04': <ul style="list-style-type: none"> • the MGF hash function will use the hash algorithm defined by Hash Identifier; • the salt length will be the same length as the hash value.
Signature Format	1 N	Only present if Signature Identifier is '02': '0': Plain format (simple concatenation of r, s) '1': ANSI X9.62 ASN.1 encoded (SEQUENCE {r INTEGER, s INTEGER})
Signature Length	4 N	Signature length (in bytes).
Signature	n B	Signature to be verified.
Delimiter	1 A	Value ';'.
		Used to indicate the end of the signature field.

payShield 10K Core Host Commands

Field	Length & Type	Details																		
Data Length	4 N	Length (in bytes) of the message data to be validated.																		
Message data	n B	Data to be validated.																		
Delimiter	1 A	Value ':'. Used to indicate the end of the message data field.																		
The following section applies only when using a Variant LMK.																				
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.																		
Public Key	n B	The Public Key used to validate the signature; DER encoded in ASN.1 format (sequence of modulus, exponent).																		
Authentication Data	n B	Optional. Additional data included in the MAC calculation (must not include ';' or '~').																		
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present.																		
The following section applies only when using a Key Block LMK.																				
Public Key	'S' + n B	<p>The Public Key used to validate the signature; must be in key block format, and comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'02'</td> <td>'R'</td> <td>'V', 'B', 'N'</td> </tr> </table> <p>If Signature Identifier is '01' (RSA):</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'02'</td> <td>'E'</td> <td>'V', 'N'</td> </tr> </table> <p>If Signature Identifier is '02' (ECDSA):</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'02'</td> <td>'E'</td> <td>'V', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'02'	'R'	'V', 'B', 'N'	Key Usage	Algorithm	Mode of Use	'02'	'E'	'V', 'N'	Key Usage	Algorithm	Mode of Use	'02'	'E'	'V', 'N'
Key Usage	Algorithm	Mode of Use																		
'02'	'R'	'V', 'B', 'N'																		
Key Usage	Algorithm	Mode of Use																		
'02'	'E'	'V', 'N'																		
Key Usage	Algorithm	Mode of Use																		
'02'	'E'	'V', 'N'																		
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.																		
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.																		
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.																		
Message Trailer	n A	Optional. Maximum length 32 characters.																		

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'EZ'.
Error Code	2 A	<p>'00': No error '01': MAC verification failure '02': Signature verification failure '04': Public key does not conform to encoding rules '05': Invalid hash identifier '06': Invalid signature identifier '07': Invalid pad mode identifier '47': Algorithm not licensed '68': Command disabled '74': Invalid digest info syntax (no-hash mode only) '76': Public key length error '77': Clear data block error '79': Hash algorithm object identifier error '80': Message length error 'D2': Unsupported curve reference value 'DA': Invalid Public Key block 'DB': Signature (r,s) values are greater than the order of the curve 'DC': Invalid Signature Format value or a standard error code.</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Hash a Block of Data

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Hash a block of data.

Notes: For information about support for the RSA algorithm, see the *payShield 10K Host Programmer's manual*.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'GM'.
Hash identifier	2 N	Identifier of the hash algorithm used to hash the data: '01': SHA-1 '02': MD5 '03': ISO 10118-2 '05': SHA-224 '06': SHA-256 '07': SHA-384 '08': SHA-512
Data length	5 N	The length of the following field, in bytes. Maximum: 32000 bytes.
Message data	n B	Data to be hashed.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'GN'.
Error Code	2 A	'00': No error '05': Invalid hash identifier '68': Command disabled or a standard error code.
Hash value	n B	Hash result (length depends on the algorithm used).
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

6.2 Message Encryption Commands

The payShield 10K provides the following host commands to support message encryption operations:

Function	Command	Page
<i>Encrypt Data Block</i>	M0 (M1)	439
<i>Decrypt Data Block</i>	M2 (M3)	446
<i>Translate Data Block</i>	M4 (M5)	452

The above commands provide general purpose encryption and decryption functionality, and are aimed at protecting data in transit (e.g. live transaction data) and data at rest (e.g. data stored in a database). These commands support four types of encryption keys:

- *Terminal Encryption Keys* (TEKs), which are shared between a terminal and a host system (e.g. a PIN-pad/ATM and an acquirer), and are used for encryption of data in transit.
- *Zone Encryption Keys* (ZEKs), which are shared between cryptographic zones (e.g. an acquirer and a switch), and are therefore used for encryption of data in transit.
- *Data Encryption Keys* (DEKs), which only exist within a single cryptographic zone (e.g. an acquirer) for protection of data at rest.
- *DUKPT Base Derivation Keys* (BDKs), which are used to drive DUKPT-compliant terminals, and may be used to encrypt live transaction "request" (i.e. terminal-to-host) messages or "response" (i.e. host-to-terminal) messages. In the DUKPT scheme, both the terminal and the HSM derive a transaction key from the BDK and transaction data. Variants are then applied to the transaction key to produce data encryption keys.

The current DUKPT standard (X9.24-3) defines two different methods for producing data encryption keys:

- The *bidirectional* method uses a single key to protect terminal-to-host and host-to-terminal messages. A BDK-1 and BDK-3 support the bidirectional method.
- The *unidirectional* method uses two independent keys: one key to protect terminal-to-host messages, and a different key to protect host-to-terminal messages. A BDK-2 and BDK-4 support the unidirectional method.

When acquiring transactions (i.e. receiving 'request' transaction data from a terminal, and (optionally) transmitting 'response' transaction data to the terminal):

- Use a BDK of type BDK-1 when *bidirectional* terminal-to-acquirer keys are required;
- Use a BDK of type BDK-2 when *unidirectional* terminal-to-acquirer keys are required.

For Payment Service Providers (PSPs) that emulate the function of a terminal (i.e. by transmitting 'request' transaction data to an acquirer, and (optionally) receiving 'response' transaction data from an acquirer):

- When *bidirectional* keys are required, the PSP and the acquirer should use the same BDK, of type BDK-1.
- When *unidirectional* keys are required, the PSP should use a BDK of type BDK-4, while the acquirer should use the same BDK, but of type BDK-2.

(Note that a BDK-3 uses the 'PIN encryption' variant to derive the data encryption key, and therefore can only be used to perform data encryption operations. A BDK-3 cannot be used to perform PIN or MAC related operations.)

Use BDK-5 to derive the appropriate PIN encryption key using the Italian Standard Derivation Method SPE-DEF-041-112. BDK-5 is equivalent to BDK-1 in all aspects apart from derivation of the IPEK / IKEY which uses the Italian Standard Key Derivation Method.

The differences between the five types of BDKs are summarised in the table below.

Further information about DUKPT and its implementation on the payShield 10K can be found in the *payShield 10K Host Programmer's manual*.

BDKs used with Message Encryption Commands

3DES DUKPT Key Variants

The table below lists the different Variant values that are applied during the derivation of the data encryption keys from a 3DES BDK:

BDK Type		Description						
BDK-1	For a Variant LMK, the 3DES BDK is encrypted under LMK 28-29.	<p>Variants are applied to the derived transaction key as follows:</p> <table border="1"> <thead> <tr> <th>Key function</th><th>Variant</th></tr> </thead> <tbody> <tr> <td>Encrypt/Decrypt "request" data</td><td>00 00 00 00 00 FF 00 00</td></tr> <tr> <td>Encrypt/Decrypt "response" data</td><td>00 00 00 00 00 FF 00 00</td></tr> </tbody> </table> <p>Note that this method will produce <i>bidirectional</i> encryption keys.</p>	Key function	Variant	Encrypt/Decrypt "request" data	00 00 00 00 00 FF 00 00	Encrypt/Decrypt "response" data	00 00 00 00 00 FF 00 00
Key function	Variant							
Encrypt/Decrypt "request" data	00 00 00 00 00 FF 00 00							
Encrypt/Decrypt "response" data	00 00 00 00 00 FF 00 00							
For a Key Block LMK, the 3DES BDK must have Key Usage = 'B0'.								
BDK-2	For a Variant LMK, the 3DES BDK is encrypted under LMK 28-29 variant 6.	<p>Variants are applied to the derived transaction key as follows:</p> <table border="1"> <thead> <tr> <th>Key function</th><th>Variant</th></tr> </thead> <tbody> <tr> <td>Decrypt "request" data</td><td>00 00 00 00 00 FF 00 00</td></tr> <tr> <td>Encrypt "response" data</td><td>00 00 00 FF 00 00 00 00</td></tr> </tbody> </table> <p>Note that this method will produce <i>unidirectional</i> encryption keys.</p>	Key function	Variant	Decrypt "request" data	00 00 00 00 00 FF 00 00	Encrypt "response" data	00 00 00 FF 00 00 00 00
Key function	Variant							
Decrypt "request" data	00 00 00 00 00 FF 00 00							
Encrypt "response" data	00 00 00 FF 00 00 00 00							
For a Key Block LMK, the 3DES BDK must have Key Usage = '41'.								
BDK-3	For a Variant LMK, the 3DES BDK is encrypted under LMK 28-29 variant 8.	<p>Variants are applied to the derived transaction key as follows:</p> <table border="1"> <thead> <tr> <th>Key function</th><th>Variant</th></tr> </thead> <tbody> <tr> <td>Encrypt/Decrypt "request" data</td><td>00 00 00 00 00 00 00 FF</td></tr> <tr> <td>Encrypt/Decrypt "response" data</td><td>00 00 00 00 00 00 00 FF</td></tr> </tbody> </table> <p>Note that this method will produce <i>bidirectional</i> encryption keys.</p>	Key function	Variant	Encrypt/Decrypt "request" data	00 00 00 00 00 00 00 FF	Encrypt/Decrypt "response" data	00 00 00 00 00 00 00 FF
Key function	Variant							
Encrypt/Decrypt "request" data	00 00 00 00 00 00 00 FF							
Encrypt/Decrypt "response" data	00 00 00 00 00 00 00 FF							
For a Key Block LMK, the 3DES BDK must have Key Usage = '42'.								
BDK-4	For a Variant LMK, the 3DES BDK is encrypted under LMK 28-29 variant 9.	<p>Variants are applied to the derived transaction key as follows:</p> <table border="1"> <thead> <tr> <th>Key function</th><th>Variant</th></tr> </thead> <tbody> <tr> <td>Encrypt "request" data</td><td>00 00 00 00 00 FF 00 00</td></tr> <tr> <td>Decrypt "response" data</td><td>00 00 00 FF 00 00 00 00</td></tr> </tbody> </table> <p>Note that this method will produce <i>unidirectional</i> encryption keys.</p>	Key function	Variant	Encrypt "request" data	00 00 00 00 00 FF 00 00	Decrypt "response" data	00 00 00 FF 00 00 00 00
Key function	Variant							
Encrypt "request" data	00 00 00 00 00 FF 00 00							
Decrypt "response" data	00 00 00 FF 00 00 00 00							
For a Key Block LMK, the 3DES BDK must have Key Usage = '43'.								
BDK-5	This key is not supported for a Variant LMK.	<p>This BDK is used for the Italian Standard Key Derivation Method only. The initial key is generated using Host Command A0.</p>						
	For a Key Block LMK, the 3DES BDK must have Key Usage = '44'.	<p>BDK-5 is equivalent to BDK-1 in all aspects apart from derivation of the IPEK / IKEY (which uses the Italian Standard Key Derivation Method).</p>						

AES DUKPT Key Usage Indicator

The table below lists the different Key Usage Indicator values that are applied during the derivation of the data encryption keys from an AES BDK:

BDK Type	Description						
BDK-1 For an AES Key Block LMK, the AES BDK must have Key Usage = 'B0'.	<p>The following Key Usage Indicator values are used in the derivation of the encryption key:</p> <table border="1" data-bbox="557 406 1271 518"> <thead> <tr> <th data-bbox="557 406 954 440">Key function</th><th data-bbox="954 406 1271 440">Key Usage Indicator</th></tr> </thead> <tbody> <tr> <td data-bbox="557 440 954 473">Encrypt/Decrypt "request" data</td><td data-bbox="954 440 1271 473">0x3002</td></tr> <tr> <td data-bbox="557 473 954 507">Encrypt/Decrypt "response" data</td><td data-bbox="954 473 1271 507">0x3002</td></tr> </tbody> </table> <p>Note that this method will produce <i>bidirectional</i> encryption keys.</p>	Key function	Key Usage Indicator	Encrypt/Decrypt "request" data	0x3002	Encrypt/Decrypt "response" data	0x3002
Key function	Key Usage Indicator						
Encrypt/Decrypt "request" data	0x3002						
Encrypt/Decrypt "response" data	0x3002						
BDK-2 For an AES Key Block LMK, the AES BDK must have Key Usage = '41'.	<p>The following Key Usage Indicator values are used in the derivation of the encryption key:</p> <table border="1" data-bbox="557 631 1271 743"> <thead> <tr> <th data-bbox="557 631 954 664">Key function</th><th data-bbox="954 631 1271 664">Key Usage Indicator</th></tr> </thead> <tbody> <tr> <td data-bbox="557 664 954 698">Decrypt "request" data</td><td data-bbox="954 664 1271 698">0x3000</td></tr> <tr> <td data-bbox="557 698 954 732">Encrypt "response" data</td><td data-bbox="954 698 1271 732">0x3001</td></tr> </tbody> </table> <p>Note that this method will produce <i>unidirectional</i> encryption keys.</p>	Key function	Key Usage Indicator	Decrypt "request" data	0x3000	Encrypt "response" data	0x3001
Key function	Key Usage Indicator						
Decrypt "request" data	0x3000						
Encrypt "response" data	0x3001						
BDK-4 For an AES Key Block LMK, the AES BDK must have Key Usage = '43'.	<p>The following Key Usage Indicator values are used in the derivation of the encryption key:</p> <table border="1" data-bbox="557 855 1271 968"> <thead> <tr> <th data-bbox="557 855 954 889">Key function</th><th data-bbox="954 855 1271 889">Key Usage Indicator</th></tr> </thead> <tbody> <tr> <td data-bbox="557 889 954 923">Encrypt "request" data</td><td data-bbox="954 889 1271 923">0x3000</td></tr> <tr> <td data-bbox="557 923 954 956">Decrypt "response" data</td><td data-bbox="954 923 1271 956">0x3001</td></tr> </tbody> </table> <p>Note that this method will produce <i>unidirectional</i> encryption keys.</p>	Key function	Key Usage Indicator	Encrypt "request" data	0x3000	Decrypt "response" data	0x3001
Key function	Key Usage Indicator						
Encrypt "request" data	0x3000						
Decrypt "response" data	0x3001						

Encrypt Data Block

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Encrypt a block of data.

Notes (general): The encryption key may be a BDK. This command supports a BDK-1, BDK-2, BDK-3 and BDK-4. If a BDK is supplied, then the DUKPT method (as defined in X9.24-3:2017) of key derivation will be used to determine the encryption key:

- If used with a BDK-1 or BDK-3, the data to be encrypted may be "request" or "response" data (the derived encrypted key will be the same in each case).
- If used with a BDK-2, the data to be encrypted is assumed to be "response" data.
- If used with a BDK-4, the data to be encrypted is assumed to be "request" data.

For further information on the use of BDKs with message encryption commands, please refer to the table on page 437.

If a ZEK or TEK is supplied as the encryption key, the contents of the plaintext message must comply with the CS "ZEK/TEK encryption" setting. This imposes certain restrictions on the contents of the message.

There are no restrictions on the contents of the message when a DEK or BDK is used.

Encryption using CTR mode requires the use of an AES key with Key Usage = 25.

The data to be encrypted by this command may be presented to the HSM in different formats, as indicated by the Input Format Flag field.

When Input Format Flag = '2', the input message goes through a conversion process (from EBCDIC to ASCII) when the HSM processes an EBCDIC formatted message.

The HSM does not apply any padding to the messages. The input message must be a multiple of the block size for binary or text messages, or a multiple of 2x block size for hex-encoded messages. When using a DES/3DES key, the block size is 8. When using an AES key, the block size is 16.

Notes (specific to FF1 mode): The use of this functionality is controlled via optional license PS10-LIC-FF1.
In order to use FF1, the Key must be an AES key encrypted under an AES Key Block LMK, and the Key must have an Algorithm either 'A' or '1'.
If Algorithm = 'A', the Key can be used to perform regular AES encryption (e.g. ECB, CBC, etc.) as well as FF1 encryption (as per the Mode Of Use).
If Algorithm = '1', the Key can only be used to perform FF1 encryption (as per the Mode Of Use) and cannot be used to perform normal AES encryption (e.g. ECB, CBC, etc.).

Notes (specific to Visa modes): This command optionally supports the encryption of data using the Visa Standard Encryption or Visa FPE modes, using a 3DES key. The use of this functionality is controlled via optional license PS10-LIC-VDSP.

Customers using PS10-LIC-VDSP must have and maintain a valid, binding and enforceable service agreement with Visa that gives them the right to use the Visa Data Secure Platform (DSP) technology, including Visa's Format Preserving Encryption (FPE) technology.

If Visa Standard Encryption or Visa FPE modes are specified, then this command supports the encryption of multiple data blocks in a single call. Each data block to be encrypted is supplied in a sequence of the following fields:

- Block Type – indicates the type of data being encrypted;
 - Primary Account Number (PAN)
 - Cardholder Name
 - Track 1 Discretionary Data
 - Track 2 Discretionary Data
- Block Length – containing the length of the following field
- Data Block – contains the data to be encrypted

For Visa FPE, the following notes apply:

- PAN and Track 2 Discretionary Data fields are always 'nibble' (4-bit) format – e.g. a PAN of "12345678" would be represented using the 4 bytes 0x12, 0x34, 0x56, 0x78.
- Whenever an odd-length PAN or Track 2 Discretionary Data field is used, the field will be padded, on the right, in the command and response messages with an additional 'F' character, to make it consist of an even number of characters. This padding is only part of the parameter in the message and not part of the VFPE process.
- Cardholder Name & Track 1 Discretionary Data fields are always in 'text' format, which means that the HSM will automatically translate to/from ASCII/EBCDIC as required. This means that a message encrypted by a system using EBCDEC can be decrypted on a system using ASCII, and vice versa.

This command will only support the use of VFPE when used in conjunction with DUKPT key management (i.e. 112/168-bit 3DES BDK).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'M0'.
Mode Flag	2 N	<p>Describes the encryption mode:</p> <p>'00': ECB '01': CBC (requires an IV) '02': CFB8 (requires an IV) '03': CFB64 (requires an IV) '04': Visa Standard Encryption (requires PS10-LIC-VDSP) '05': OFB (requires an IV) '06': CTR (requires an IV) '11': FF1 (NIST approved FPE) (requires PS10-LIC-FF1) '13': Visa Format Preserving Encryption (requires PS10-LIC-VDSP)</p>
If Mode Flag = '11' (FF1), the following FOUR fields apply:		
FPE Radix Flag	1 A	<p>Optional – Only present if Mode Flag = '11'. This flag selects a pre-specified Radix value, or alternatively, indicates that a user-specified value is to be used. 'A': FPE Radix Value = 10 'U': User defined value specified in the next field Note: If this field is 'U', then the FPE Radix Value field must be present; otherwise, the FPE Radix Value field must be omitted. <i>Note: The Message field must consist of values in the range 0...FPE Radix Value – 1.</i></p>
FPE Radix Value	5 N	<p>Optional – Only present if FPE Radix Flag = 'U'. Specifies the radix (base) of the FPE character set. The FPE Radix Value must be in the range:</p> <ul style="list-style-type: none"> • 00002...00256 (Mode Flag = '11') <p><i>Note: The Message field must consist of values in the range 0...FPE Radix Value – 1.</i></p>

Field	Length & Type	Details															
FPE Tweak Length	4 H	Only present if Mode Flag = '11'. The length of the following field.															
FPE Tweak	n B	Only present if Mode Flag = '11'. Specifies the tweak value.															
Input Format Flag	1 N	Describes the format of the input message: '0': Binary '1': Hex-Encoded Binary '2': Text. This field is omitted when Mode Flag = '04' or '13'.															
Output Format Flag	1 N	Describes the format of the output message: '0': Binary '1': Hex-Encoded Binary. This field is omitted when Mode Flag = '13'.															
Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be used. The following key types are permitted: '009': BDK-1 (encrypted under LMK pair 28-29) '609': BDK-2 (encrypted under LMK pair 28-29/6) '809': BDK-3 (encrypted under LMK pair 28-29/8) '909': BDK-4 (encrypted under LMK pair 28-29/9) Note that the above key types will require the optional fields KSN Descriptor, Key Serial Number to be supplied. '00A': ZEK (encrypted under LMK pair 30-31) '00B': DEK (encrypted under LMK pair 32-33) '30B': TEK (encrypted under LMK pair 32-33/3) For a Key Block LMK: This field is ignored; should be set to 'FFF'.															
Key	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The encryption Key, used in conjunction with the IV, if appropriate, to encrypt the supplied Message. Note: If Mode Flag = '13' (Visa FPE), then this field must specify a BDK (not a ZEK, DEK or TEK). For a Variant LMK, the 'Key' is a BDK, ZEK, DEK or TEK, as specified above. For a Key Block LMK, the 'Key' must comply with one of the following: <table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'B0', '41', '43'</td> <td>'T', 'A'</td> <td>'X', 'N'</td> </tr> <tr> <td>'42'</td> <td>'T'</td> <td>'X', 'N'</td> </tr> <tr> <td>'D0', '21', '22', '23'</td> <td>'D', 'T', 'A', '1'</td> <td>'B', 'E', 'N'</td> </tr> <tr> <td>'25'</td> <td>'A'</td> <td>'B', 'E', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'B0', '41', '43'	'T', 'A'	'X', 'N'	'42'	'T'	'X', 'N'	'D0', '21', '22', '23'	'D', 'T', 'A', '1'	'B', 'E', 'N'	'25'	'A'	'B', 'E', 'N'
Key Usage	Algorithm	Mode of Use															
'B0', '41', '43'	'T', 'A'	'X', 'N'															
'42'	'T'	'X', 'N'															
'D0', '21', '22', '23'	'D', 'T', 'A', '1'	'B', 'E', 'N'															
'25'	'A'	'B', 'E', 'N'															
KSN Descriptor	3 H	The descriptor for the KSN (in the next field). For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i> . This field is ignored when using an AES BDK-1, BDK-2 or BDK-4 and should be set to '000'. Only present if Key Type is a BDK.															
Key Serial Number	12 - 20 H Or 24 H	The KSN supplied by the PIN pad, including the transaction counter. For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i> . Only present if Key Type is a BDK. For a 3DES BDK-1, BDK-2, BDK-3 or BDK-4, this field is 12-20 H. For an AES BDK-1, BDK-2 or BDK-4, this field is 24 H.															
IV	16 H or 32 H	The input IV, used in conjunction with the encryption Key. When encrypting the first of a series of blocks, this initial IV should be set by the caller – a typical initial IV is {00 00 00 00 00 00 00 00}. For subsequent blocks, this value should be the IV returned from encrypting the previous block. If using a DES/3DES Key, the IV will be a 16 H field. If using an AES Key, the IV will be a 32 H field. Only present if the Mode Flag is '01', '02', '03', '05' or '06'.															
Counter Offset	3 N	The offset in bits from the LSB of the IV for the start of the counter. Only present if the Mode Flag is '06' (CTR Mode).															

Field	Length & Type	Details
Counter Length	3 N	The length of the counter in bits. Minimum value 8 bits. Only present if the Mode Flag is '06' (CTR Mode).
OFB Mode Flag	1 N	Flag to indicate the mode of the OFB operation: '1': OFB8 '8': OFB64 Only present if Mode Flag = '05' (OFB Mode).
If Mode Flag ≠ '04' or '13', the following TWO fields must be present:		
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes. Note: When using FF1, the Message length must comply with NIST SP800-38G: <ul style="list-style-type: none">• Radix in the range 2...2¹⁶• radix^{minlen} ≥ 100• 2 ≤ minlen ≤ maxlen ≤ 2³²
Message	n B or n H or n A	The message to be encrypted. The length & type of the field will depend on the value of the Input Format Flag: Input Format Flag = '0' (Binary); If Mode Flag ≠ '06' (CTR mode): n = a multiple of 8 when using a DES/3DES key, or a multiple of 16 when using an AES key. Input Format Flag = '1' (Hex-Encoded Binary); If Mode Flag ≠ '06' (CTR mode): n = a multiple of 16 when using a DES/3DES key, or a multiple of 32 when using an AES key. Input Format Flag = '2' (Text); If Mode Flag ≠ '06' (CTR mode): n = a multiple of 8 when using a DES/3DES key, or a multiple of 16 when using an AES key. Note: When using FF1, the Message must consist of a string of bytes each having a value less than the FF1 Radix Value. The type of the message will depend on the value of the Input Format Flag field
If Mode Flag = '04' or '13', the following fields are present:		
Block Count	2 N	Indicates the number of Data Blocks to be encrypted in this command. Value: '01' ... '04'. Each Data Block is of a certain Block Type, as defined here: <ul style="list-style-type: none">• Primary Account Number (PAN)• Cardholder Name• Track 1 Discretionary Data• Track 2 Discretionary Data This command supports the encryption of up to 4 Data Blocks within a single call, but each Block Type must be unique – e.g. it is not permitted to encrypt two 'Cardholder Name' blocks in a single call to this command. Note: If Mode Flag = '13', the Data Blocks fields must be supplied in the order given above.
If Mode Flag = '04' or '13', the following THREE fields are repeated 'Block Count' times.		
Block Type	1 A	Indicates the type of data being encrypted. 'A': Primary Account Number (PAN) 'B': Cardholder Name 'C': Track 1 Discretionary Data 'D': Track 2 Discretionary Data
Block Length Data Block	4 H	The length of the following field, in bytes.
	n B	The data to be encrypted. The format of this field will depend on the value of the Block Type field: If Block Type = 'A' (BCD – Binary Coded Decimal) If Block Type = 'B' (Text – ASCII or EBCDIC) If Block Type = 'C' (Text – ASCII or EBCDIC) If Block Type = 'D' (4-bit BASE15 chars)
	n A	
	n B	
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'M1'.
Error Code	2 A	<p>'00': No error '02': Invalid Mode Flag field or Block Type field '03': Invalid Input Format Flag field '04': Invalid Output Format Flag field '05': Invalid Key Type field '06': Invalid Message/Data Block Length field '09': Character not in FPE Character Set '10': Encryption Key Parity Error '21': VFPE Process S Counter Overflow '35': Illegal Message Format '53': Invalid Block Count field '67': Command not licensed '68': Command disabled '80': Data Block not within expected length for Type 'D1': Mode Flag requires AES Key Block LMK 'D2': Mode Flag requires AES key or a standard error code.</p>
IV	16 H or 32 H	<p>The output IV. When encrypting a series of blocks, this IV should be supplied as input when encrypting the next block. If using a DES/3DES Key, the IV will be a 16 H field. If using an AES Key, the IV will be a 32 H field. Only present if the Mode Flag is '01', '02', '03' or '05'.</p>
If Mode Flag ≠ '04' or '13', the following TWO fields will be present:		
Message Length	4 H	The length of the following field, in bytes.
Encrypted Message	n B or n H	<p>The encrypted message. The length & type of the field will depend on the value of the Output Format Flag: Output Format Flag = '0' (Binary); If Mode Flag ≠ '06' (CTR mode): n = a multiple of 8 when using a DES/3DES key, or a multiple of 16 when using an AES key. Output Format Flag = '1' (Hex-Encoded Binary); If Mode Flag ≠ '06' (CTR mode): n = a multiple of 16 when using a DES/3DES key, or a multiple of 32 when using an AES key.</p>
If Mode Flag = '04' or '13', the following fields will be present:		
Block Count	2 N	Indicates the number of Encrypted Blocks in the following fields.
If Mode Flag = '04', the following THREE fields are repeated 'Block Count' times.		
Block Type	1 A	<p>Indicates the type of data that was encrypted. 'A': Primary Account Number (PAN) 'B': Cardholder Name 'C': Track 1 Discretionary Data 'D': Track 2 Discretionary Data</p>
Block Length	4 H	The length of the following field, in bytes.
Encrypted Block	n B n H	<p>The encrypted data. The format of this field will depend on the value of the Output Format Flag field: If Output Format Flag = '0' (Binary). If Output Format Flag = '1' (Hex-Encoded Binary).</p>

If Mode Flag = '13', the following THREE fields are repeated 'Block Count' times.		
Block Type	1 A	Indicates the type of data that was encrypted. 'A': Primary Account Number (PAN) 'B': Cardholder Name 'C': Track 1 Discretionary Data 'D': Track 2 Discretionary Data
Block Length	4 H	The length of the following field, in bytes.
Encrypted Block	n B	The encrypted data. The format of the block will depend on the value of the Block Type field.
	n A	If Block Type = 'A' (BCD – Binary Coded Decimal)
	n A	If Block Type = 'B' (Text – ASCII or EBCDIC)
	n B	If Block Type = 'C' (Text – ASCII or EBCDIC)
	n B	If Block Type = 'D' (4-bit BASE15 chars)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Decrypt Data Block

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Decrypt a block of data.

Notes (general): The decryption key may be a BDK. This command supports a BDK-1, BDK-2, BDK-3 and BDK-4. If a BDK is supplied, then the DUKPT method (as defined in X9.24-3:2017) of key derivation will be used to determine the decryption key:

- If used with a BDK-1 or BDK-3, the data to be decrypted may be "request" or "response" data (the derived key will be the same in each case).
- If used with a BDK-2, the data to be decrypted is assumed to be "request" data.
- If used with a BDK-4, the data to be decrypted is assumed to be "response" data.

For further information on the use of BDKs with message encryption commands, please refer to the table on page 437.

If a ZEK or TEK is supplied as the encryption key, the contents of the plaintext message must comply with the CS "ZEK/TEK encryption" setting. This imposes certain restrictions on the contents of the message.

There are no restrictions on the contents of the message when a DEK or BDK is used.

Decryption using CTR mode requires the use of an AES key with Key Usage = 25.

The data to be decrypted by this command may be presented to the HSM in different formats, as indicated by the Input Format Flag field.

The decrypted data block may be returned to the host in different formats, as indicated by the Output Format Flag field.

When Output Format Flag = '2', the output message goes through a conversion process (from ASCII to EBCDIC) when the HSM processes an EBCDIC formatted message.

The HSM does not apply any padding to the messages. For non-FPE modes, the input message must be a multiple of the block size for binary messages, or a multiple of 2x block size for hex-encoded messages. When using a DES/3DES key, the block size is 8. When using an AES key, the block size is 16.

Notes (specific to Ingenico BPS):	This command optionally supports the decryption of data using the Ingenico BPS Format Preserving Encryption (FPE) method, using a 3DES key. When using the Ingenico BPS method to decrypt transaction fields, all the BPS-encrypted fields must be supplied (concatenated in the order in which they were encrypted) in one call to this command. The output block will contain a concatenated string of the decrypted fields. Additionally, the encrypted transaction fields must be supplied to the HSM as a string of bytes of values in the range 0 ... BPS-Radix-1. For example, for a BPS-encrypted Primary Account Number (PAN) with a BPS-Radix of 10, the Encrypted Message field will consist of bytes with values 0x00 ... 0x09 representing the digits '0' ... '9'. The output Decrypted Message field will also consist of bytes with values 0x00 ... 0x09 representing the digits '0' ... '9'.
Notes (specific to FF1 mode):	The use of this functionality is controlled via optional license PS10-LIC-FF1. In order to use FF1, the Key must be an AES key encrypted under an AES Key Block LMK, and the Key must have an Algorithm either 'A' or '1'.

If Algorithm = 'A', the Key can be used to perform regular AES decryption (e.g. ECB, CBC, etc.) as well as FF1 decryption (as per the Mode Of Use).

If Algorithm = '1', the Key can only be used to perform FF1 decryption (as per the Mode Of Use) and cannot be used to perform normal AES decryption (e.g. ECB, CBC, etc.).

Notes (specific to Visa modes):

This command optionally supports the decryption of data using the Visa Standard Encryption or Visa FPE modes, using a 3DES key. The use of this functionality is controlled via optional license PS10-LIC-VDSP.

Customers using PS10-LIC-VDSP must have and maintain a valid, binding and enforceable service agreement with Visa that gives them the right to use the Visa Data Secure Platform (DSP) technology, including Visa's Format Preserving Encryption (FPE) technology.

If Visa Standard Encryption or Visa FPE modes are specified, then this command supports the decryption of multiple data blocks in a single call. Each data block to be decrypted is supplied in a sequence of the following fields:

- Block Type – indicates the type of data being encrypted;
 - Primary Account Number (PAN)
 - Cardholder Name
 - Track 1 Discretionary Data
 - Track 2 Discretionary Data
- Block Length – containing the length of the following field
- Encrypted Block – contains the data to be decrypted

For Visa FPE, the following notes apply:

- PAN and Track 2 Discretionary Data fields are always 'nibble' (4-bit) format – e.g. a PAN of "12345678" would be represented using the 4 bytes 0x12, 0x34, 0x56, 0x78.
- Whenever an odd-length PAN or Track 2 Discretionary Data field is used, the field will be padded, on the right, in the command and response messages with an additional 'F' character, to make it consist of an even number of characters. This padding is only part of the parameter in the message and not part of the VFPE process.
- Cardholder Name & Track 1 Discretionary Data fields are always in 'text' format, which means that the HSM will automatically translate to/from ASCII/EBCDIC as required. This means that a message encrypted by a system using EBCDEC can be decrypted on a system using ASCII, and vice versa.

This command will only support the use of VFPE when used in conjunction with DUKPT key management (i.e. 112/168-bit 3DES BDK).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'M2'.
Mode Flag	2 N	<p>Describes the decryption mode:</p> <ul style="list-style-type: none"> '00': ECB '01': CBC (requires an IV) '02': CFB8 (requires an IV) '03': CFB64 (requires an IV) '04': Visa Standard Encryption (requires PS10-LIC-VDSP) '05': OFB (requires an IV) '06': CTR (requires an IV) '10': BPS (Ingenico FPE) '11': FF1 (NIST approved FPE) (requires PS10-LIC-FF1) '13': Visa Format Preserving Encryption (requires PS10-LIC-VDSP)
If Mode Flag = '10' (BPS) or '11' (FF1), the following FOUR fields apply:		
FPE Radix Flag	1 A	<p>Optional – Only present if Mode Flag = '10' or '11'.</p> <p>This flag selects a pre-specified Radix value, or alternatively, indicates that a user-specified value is to be used.</p> <ul style="list-style-type: none"> 'A': FPE Radix Value = 10 'U': User defined value specified in the next field <p><i>Note: If this field is 'U', then the FPE Radix Value field must be present; otherwise, the FPE Radix Value field must be omitted.</i></p> <p><i>Note: The Encrypted Message field must consist of values in the range 0....FPE Radix Value – 1.</i></p>
FPE Radix Value	3 N or 5 N	<p>Optional – Only present if FPE Radix Flag = 'U'</p> <p>Specifies the Radix of the FPE character set.</p> <p>Must be in the range 002...256 (Mode Flag = '10').</p> <p>Must be in the range 00002...00256 (Mode Flag = '11').</p> <p><i>Note: The Encrypted Message field must consist of values in the range 0....FPE Radix Value – 1.</i></p> <p>If Mode Flag = '10', length of FPE Radix Value is 3 N. If Mode Flag = '11', length of FPE Radix Value is 5 N.</p>
FPE Tweak Length	4 H	<p>Only present if Mode Flag = '11'.</p> <p>The length of the following field.</p>
FPE Tweak	8 B or n B	<p>Only present if Mode Flag = '10' or '11'.</p> <p>Specifies the tweak value:</p> <p>If Mode Flag = '10', length of FPE Tweak is 8 B. If Mode Flag = '11', length of FPE Tweak is n B (defined in the preceding field).</p>
Input Format Flag	1 N	<p>Describes the format of the input message:</p> <ul style="list-style-type: none"> '0': Binary '1': Hex-Encoded Binary <p>This field is omitted when Mode Flag = '13'.</p>
Output Format Flag	1 N	<p>Describes the format of the output message:</p> <ul style="list-style-type: none"> '0': Binary '1': Hex-Encoded Binary '2': Text <p>This field is omitted when Mode Flag = '04' or '13'.</p>
Key Type	3 H	<p>For a Variant LMK:</p> <p>Indicates the key type of the key to be used. The following key types are permitted:</p> <ul style="list-style-type: none"> '009': BDK-1 (encrypted under LMK pair 28-29) '609': BDK-2 (encrypted under LMK pair 28-29/6) '809': BDK-3 (encrypted under LMK pair 28-29/8) '909': BDK-4 (encrypted under LMK pair 28-29/9) <p>Note that the above key types will require the optional fields KSN Descriptor, Key Serial Number to be supplied.</p> <ul style="list-style-type: none"> '00A': ZEK (encrypted under LMK pair 30-31) '00B': DEK (encrypted under LMK pair 32-33) '30B': TEK (encrypted under LMK pair 32-33/3). <p>For a Key Block LMK:</p> <p>This field is ignored; should be set to 'FFF'.</p>

Field	Length & Type	Details															
Key	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The decryption Key, used in conjunction with the IV, if appropriate, to decrypt the supplied Message. Note: If Mode Flag = '13' (Visa FPE), then this field must specify a BDK (not a ZEK, DEK or TEK). For a Variant LMK, the 'Key' is a BDK, ZEK, DEK or TEK, as specified above. For a Key Block LMK, the 'Key' must comply with one of the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'B0', '41', '43'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> <tr> <td>'42'</td><td>'T'</td><td>'X', 'N'</td></tr> <tr> <td>'D0', '21', '22', '23'</td><td>'D', 'T', 'A', '1'</td><td>'B', 'D', 'N'</td></tr> <tr> <td>'25'</td><td>'A'</td><td>'B', 'D', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'B0', '41', '43'	'T', 'A'	'X', 'N'	'42'	'T'	'X', 'N'	'D0', '21', '22', '23'	'D', 'T', 'A', '1'	'B', 'D', 'N'	'25'	'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use															
'B0', '41', '43'	'T', 'A'	'X', 'N'															
'42'	'T'	'X', 'N'															
'D0', '21', '22', '23'	'D', 'T', 'A', '1'	'B', 'D', 'N'															
'25'	'A'	'B', 'D', 'N'															
KSN Descriptor	3 H	The descriptor for the KSN (in the next field). For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i> . Only present if Key Type is a BDK. This field is ignored when using an AES BDK-1, BDK-2 or BDK-4 and should be set to '000'.															
Key Serial Number	12 - 20 H or 24 H	The KSN supplied by the PIN pad. For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i> . Only present if Key Type is a BDK. For a 3DES BDK-1, BDK-2, BDK-3 or BDK-4, this field is 12-20 H. For an AES BDK-1, BDK-2 or BDK-4, this field is 24 H.															
IV	16 H or 32 H	The input IV, to be used in conjunction with the decryption Key. When decrypting the first of a series of blocks, this initial IV should match the initial IV used to encrypt the original message. For subsequent blocks, this value should be the IV returned from decrypting the previous block. If using a DES/3DES Key, the IV will be a 16 H field. If using an AES Key, the IV will be a 32 H field. Only present if the Mode Flag is '01', '02', '03', '05' or '06'.															
Counter Offset	3 N	The offset in bits from the LSB of the IV for the start of the counter. Only present if the Mode Flag is '06' (CTR Mode).															
Counter Length	3 N	The length of the counter in bits. Minimum value 8 bits. Only present if the Mode Flag is '06' (CTR Mode).															
OFB Mode Flag	1 N	Flag to indicate the mode of the OFB operation: '1': OFB8 '8': OFB64 Only present if Mode Flag = '05' (OFB Mode).															

If Mode Flag ≠ '04' or '13', the following TWO fields must be present:

Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes. Note: When using BPS/FF1, the Message length must comply with NIST SP800-38G : <ul style="list-style-type: none"> • Radix in range 2... 2¹⁶ • radix^{minlen} >= 100 • 2 <= minlen <= maxlen <= 2³²
Encrypted Message	n B or n H	The encrypted message. Note: When using FPE, the Encrypted Message must consist of a string of bytes each having a value less than the FPE Radix Value. The type of the message will depend on the value of the Input Format Flag field: Input Format Flag = '0' (Binary); If Mode Flag ≠ '06' (CTR mode) or '10' (BPS mode): n = a multiple of 8 when using a DES/3DES key, or a multiple of 16 when using an AES key. Input Format Flag = '1' (Hex-Encoded Binary); If Mode Flag ≠ '06' (CTR mode) or '10' (BPS mode): n = a multiple of 16 when using a DES/3DES key, or a multiple of 32 when using an AES key.

If Mode Flag = '04' or '13', the following fields must be present:

Field	Length & Type	Details
Block Count	2 N	<p>Indicates the number of Encrypted Blocks to be decrypted in this command. Value: '01' ... '04'.</p> <p>Each Encrypted Block is of a certain Block Type, as defined here:</p> <ul style="list-style-type: none"> • Primary Account Number (PAN) • Cardholder Name • Track 1 Discretionary Data • Track 2 Discretionary Data <p>This command supports the decryption of up to 4 Encrypted Blocks within a single call, but each Block Type must be unique – e.g. it is not permitted to decrypt two 'Cardholder Name' blocks in a single call to this command.</p> <p>Note: If Mode Flag = '13', the Encrypted Blocks fields must be supplied in the order given above.</p>
If Mode Flag = '04', the following THREE fields must be repeated 'Block Count' times:		
Block Type	1 A	Indicates the type of data being decrypted. A: Primary Account Number (PAN) B: Cardholder Name C: Track 1 Discretionary Data D: Track 2 Discretionary Data
Block Length	4 H	The length of the following field, in bytes.
Encrypted Block	n B	The encrypted data.
	n H	The format of this field will depend on the value of the Output Format Flag field: If Output Format Flag = 0 (Binary). If Output Format Flag = 1 (Hex-Encoded Binary).
If Mode Flag = '13', the following THREE, or FOUR, fields must be repeated 'Block Count' times.		
Block Type	1 A	Indicates the type of data being decrypted. 'A': Primary Account Number (PAN) 'B': Cardholder Name 'C': Track 1 Discretionary Data 'D': Track 2 Discretionary Data
Check Digit Flag	1 N	Indicates if original unencrypted PAN had a valid check digit. '0': Check Digit valid '1': Check Digit invalid Only present if Block Type = 'A'.
Block Length	4 H	The length of the following field, in bytes.
Encrypted Block	n B	The encrypted data. The format of the block will depend on the value of the Block Type field.
	n A	If Block Type = 'A' (BCD – Binary Coded Decimal)
	n A	If Block Type = 'B' (Text – ASCII or EBCDIC)
	n A	If Block Type = 'C' (Text – ASCII or EBCDIC)
	n B	If Block Type = 'D' (4-bit BASE15 chars)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'M3'.
Error Code	2 A	'00': No error '02': Invalid Mode Flag, Block Type or Check Digit Flag field '03': Invalid Input Format Flag field '04': Invalid Output Format Flag field '05': Invalid Key Type field '06': Invalid Message/Block Length field '09': Invalid Visa Standard Encryption block '10': Decryption Key Parity Error '21': VFPE Process S Counter Overflow '35': Illegal Message Format '53': Invalid Block Count field '67': Command not licensed '68': Command disabled 'D1': Mode Flag requires AES Key Block LMK 'D2': Mode Flag requires AES key or a standard error code.
IV	16 H or 32 H	The output IV. When decrypting a series of blocks, this IV should be supplied as input when encrypting the next block. If using a DES/3DES Key, the IV will be a 16 H field. If using an AES Key, the IV will be a 32 H field. Only present if the Mode Flag is '01', '02', '03', '05' or '06'.
If Mode Flag ≠ '04' or '13', the following TWO fields will be present:		
Message Length	4 H	The length of the following field, in bytes.
Decrypted Message	n B or n H or n A	The decrypted message. The type of the message will depend on the value of the Output Format Flag field. Output Format Flag = '0' (Binary); If Mode Flag ≠ '06' (CTR mode) or '10' (BPS mode): n = a multiple of 8 when using a DES/3DES key, or a multiple of 16 when using an AES key. Output Format Flag = '1' (Hex-Encoded Binary); If Mode Flag ≠ '06' (CTR mode) or '10' (BPS mode): n = a multiple of 16 when using a DES/3DES key, or a multiple of 32 when using an AES key. Output Format Flag = '2' (Text); If Mode Flag ≠ '06' (CTR mode) or '10' (BPS mode): n = a multiple of 8 when using a DES/3DES key, or a multiple of 16 when using an AES key.
If Mode Flag = '04' or '13', the following field will be present:		
Block Count	2 N	Indicates the number of Decrypted Blocks in the following fields.
If Mode Flag = '04' or '13', the following fields will be repeated 'Block Count' times:		
Block Type	1 A	Indicates the type of data that was decrypted. 'A': Primary Account Number (PAN) 'B': Cardholder Name 'C': Track 1 Discretionary Data 'D': Track 2 Discretionary Data
Block Length	4 H	The length of the following field, in bytes.
Decrypted Block	n B	A decrypted data block. The format of the block will depend on the value of the Block Type field. If Block Type = 'A' (BCD – Binary Coded Decimal)
	n A	If Block Type = 'B' (Text – ASCII or EBCDIC)
	n A	If Block Type = 'C' (Text – ASCII or EBCDIC)
	n B	If Block Type = 'D' (4-bit BASE15 chars)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate Data Block

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Translate a block of data from encryption under one key, to encryption under another key.

Notes (general): The data to be translated by this command may be presented to the HSM in different formats, as indicated by the Input Format Flag field.
The translated data block may be returned to the host in different formats, as indicated by the Output Format Flag field.
If a ZEK or TEK is supplied as either encryption or decryption key, the contents of the plaintext message must comply with the CS "ZEK/TEK encryption" setting. This imposes certain restrictions on the contents of the message.
The source key and/or the destination key may be a BDK. This command supports a BDK-1, BDK-2 and BDK-3.
If the source key is a BDK, then the DUKPT (as defined X9.24-3:2017) method will be used to determine the decryption key. Both bidirectional and unidirectional decryption keys are supported, and the data will be assumed to be "request" data.
If the destination key is a BDK, then the DUKPT method will be used to determine the encryption key. Both bidirectional and unidirectional encryption keys are supported, and the data will be assumed to be "response" data.
For further information on the use of BDKs with message encryption commands, please refer to the table on page 430.

Notes (specific to FF1 mode): The use of this functionality is controlled via optional license PS10-LIC-FF1.
In order to use FF1, the Key must be an AES key encrypted under an AES Key Block LMK, and the Key must have an Algorithm either 'A' or '1'.
If Algorithm = 'A', the Key can be used to perform regular AES encryption/decryption (e.g. ECB, CBC, etc.) as well as FF1 encryption/decryption (as per the Mode Of Use).
If Algorithm = '1', the Key can only be used to perform FF1 encryption/decryption (as per the Mode Of Use) and cannot be used to perform normal AES encryption/decryption (e.g. ECB, CBC, etc.).

Notes (specific to Visa modes): This command optionally supports the translation of data using the Visa Standard Encryption or Visa FPE modes, using a 3DES key. The use of this functionality is controlled via optional license PS10-LIC-VDSP.
Customers using PS10-LIC-VDSP must have and maintain a valid, binding and enforceable service agreement with Visa that gives them the right to use the Visa Data Secure Platform (DSP) technology, including Visa's Format Preserving Encryption (FPE) technology.

If Visa Standard Encryption or Visa FPE modes are specified, then this command supports the translation of multiple data blocks in a single call. Each data block to be translated is supplied in a sequence of the following fields:

- Block Type – indicates the type of data being encrypted;
 - Primary Account Number (PAN)
 - Cardholder Name
 - Track 1 Discretionary Data
 - Track 2 Discretionary Data

- Block Length – containing the length of the following field
- Encrypted Block – contains the data to be decrypted

For Visa FPE, the following notes apply:

- PAN and Track 2 Discretionary Data fields are always 'nibble' (4-bit) format – e.g. a PAN of "12345678" would be represented using the 4 bytes 0x12, 0x34, 0x56, 0x78.
- Whenever an odd-length PAN or Track 2 Discretionary Data field is used, the field will be padded, on the right, in the command and response messages with an additional 'F' character, to make it consist of an even number of characters. This padding is only part of the parameter in the message and not part of the VFPE process.
- Cardholder Name & Track 1 Discretionary Data fields are always in 'text' format, which means that the HSM will automatically translate to/from ASCII/EBCDIC as required. This means that a message encrypted by a system using EBCDEC can be decrypted on a system using ASCII, and vice versa.

This command will only support the use of VFPE when used in conjunction with DUKPT key management (i.e. 112/168-bit 3DES BDK).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'M4'.
Source Mode Flag	2 N	<p>'00': ECB '01': CBC (requires IV) '02': CFB8 (requires IV) '03': CFB64 (requires IV) '04': Visa Standard Encryption (requires PS10-LIC-VDSP) '11': FF1 (NIST approved FPE) (requires PS10-LIC-FF1) '13': Visa Format Preserving Encryption (requires PS10-LIC-VDSP)</p>
Destination Mode Flag	2 N	<p>'00': ECB '01': CBC (requires IV) '02': CFB8 (requires IV) '03': CFB64 (requires IV) '04': Visa Standard Encryption (requires PS10-LIC-VDSP) '11': FF1 (NIST approved FPE) (requires PS10-LIC-FF1)</p>
If Source Mode Flag = '11' (FF1), the following fields apply:		
Source FPE Radix Flag	1 A	<p>Optional – Only present if Source Mode Flag = '11'. This flag selects a pre-specified Radix value, or alternatively, indicates that a user-specified value is to be used. 'A': Source FPE Radix Value = 10 'U': User defined value specified in the next field</p> <p><i>Note: If this field is 'U', then the Source FPE Radix Value field must be present; otherwise, the Source FPE Radix Value field must be omitted.</i></p> <p><i>Note: The Encrypted Message field must consist of values in the range 0...Source FPE Radix Value – 1.</i></p>
Source FPE Radix Value	5 N	<p>Optional – Only present if Source FPE Radix Flag = 'U'. Specifies the radix (base) of the source FPE character set. The Source FPE Radix Value must be in the range: • 00002...00256</p> <p><i>Note: The Encrypted Message field must consist of values in the range 0...Source FPE Radix Value – 1.</i></p>
Source FPE Tweak Length	4 H	Only present if Source Mode Flag = '11'. The length of the following field.
Source FPE Tweak	n B	Only present if Source Mode Flag = '11'. Specifies the tweak value.
If Destination Mode Flag = '11' (FF1), the following fields apply:		
Destination FPE Radix Flag	1 A	<p>Optional – Only present if Destination Mode Flag = '11'. This flag selects a pre-specified Radix value, or alternatively, indicates that a user-specified value is to be used. 'A': Destination FPE Radix Value = 10 'U': User defined value specified in the next field</p> <p><i>Note: If this field is 'U', then the Destination FPE Radix Value field must be present; otherwise, the Destination FPE Radix Value field must be omitted.</i></p> <p><i>Note: The Translated Message field will consist of values in the range 0... Destination FPE Radix Value – 1.</i></p>
Destination FPE Radix Value	5 N	<p>Optional – Only present if Destination FPE Radix Flag = 'U'. Specifies the radix (base) of the destination FPE character set. The Destination FPE Radix Value must be in the range: • 00002...00256</p> <p><i>Note: The Translated Message field will consist of values in the range 0... Destination FPE Radix Value – 1.</i></p>
Destination FPE Tweak Length	4 H	Only present if Destination Mode Flag = '11'. The length of the following field.
Destination FPE Tweak	n B	Only present if Destination Mode Flag = '11'. Specifies the tweak value.
Input Format Flag	1 N	<p>'0': Binary '1': Hex-Encoded Binary.</p> <p>This field is omitted when Source Mode Flag = '13'.</p>
Output Format Flag	1 N	<p>'0': Binary '1': Hex-Encoded Binary.</p>
Source Key Type	3 H	For a Variant LMK:

Field	Length & Type	Details															
Source Key	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>Indicates the source (decryption) key type of the key to be used. The following key types are permitted:</p> <ul style="list-style-type: none"> '009': BDK-1 (encrypted under LMK pair 28-29) '609': BDK-2 (encrypted under LMK pair 28-29/6) '809': BDK-3 (encrypted under LMK pair 28-29/8) '00A': ZEK (encrypted under LMK pair 30-31) '00B': DEK (encrypted under LMK pair 32-33) '30B': TEK (encrypted under LMK pair 32-33/3). <p>For a Key Block LMK:</p> <p>This field is ignored; should be set to 'FFF'.</p> <p>The Source (decryption) Key, used in conjunction with the IV, if appropriate, to decrypt the supplied Message.</p> <p>Note: If Mode Flag = '13' (Visa FPE), then this field must specify a BDK (not a ZEK, DEK or TEK).</p> <p>For a Variant LMK, the 'Source Key' is a BDK, ZEK, DEK or TEK, as specified above.</p> <p>For a Key Block LMK, the 'Source Key' must comply with one of the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'B0', '41'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> <tr> <td>'42'</td><td>'T'</td><td>'X', 'N'</td></tr> <tr> <td>'D0', '21', '22', '23'</td><td>'D', 'T', 'A'</td><td>'B', 'D', 'N'</td></tr> <tr> <td>'D0', '21', '22', '23'</td><td>'A', '1'</td><td>'B', 'D', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'B0', '41'	'T', 'A'	'X', 'N'	'42'	'T'	'X', 'N'	'D0', '21', '22', '23'	'D', 'T', 'A'	'B', 'D', 'N'	'D0', '21', '22', '23'	'A', '1'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use															
'B0', '41'	'T', 'A'	'X', 'N'															
'42'	'T'	'X', 'N'															
'D0', '21', '22', '23'	'D', 'T', 'A'	'B', 'D', 'N'															
'D0', '21', '22', '23'	'A', '1'	'B', 'D', 'N'															
Source KSN Descriptor	3 H	<p>The descriptor for the KSN (in the next field). For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i>.</p> <p>If Source Key is an AES BDK-1 or BDK-2, this field is ignored and should be set to '000'.</p> <p>Only present if Source Key Type is a BDK.</p>															
Source Key Serial Number	12 - 20 H or 24 H	<p>The KSN supplied by the PIN pad. For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i>.</p> <p>Only present if Source Key Type is a BDK.</p>															
Destination Key Type	3 H	<p>If the Source Key is an AES BDK-1 or BDK-2, this field will be 24 Hex digits</p> <p>For a Variant LMK:</p> <p>Indicates the destination (encryption) key type of the key to be used. The following key types are permitted:</p> <ul style="list-style-type: none"> '009': BDK-1 (encrypted under LMK pair 28-29) '609': BDK-2 (encrypted under LMK pair 28-29/6) '809': BDK-3 (encrypted under LMK pair 28-29/8) '00A': ZEK (encrypted under LMK pair 30-31) '00B': DEK (encrypted under LMK pair 32-33) '30B': TEK (encrypted under LMK pair 32-33/3) <p>For a Key Block LMK:</p> <p>This field is ignored; should be set to 'FFF'.</p>															
Destination Key	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	<p>The Destination (encryption) Key, used in conjunction with the IV, if appropriate, to re-encrypt the decrypted Message.</p> <p>For a Variant LMK, the 'Destination Key' is a BDK, ZEK, DEK or TEK, as specified above.</p> <p>For a Key Block LMK, the 'Destination Key' must comply with one of the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'B0', '41'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> <tr> <td>'42'</td><td>'T'</td><td>'X', 'N'</td></tr> <tr> <td>'D0', '21', '22', '23'</td><td>'D', 'T', 'A'</td><td>'B', 'E', 'N'</td></tr> <tr> <td>'D0', '21', '22', '23'</td><td>'A', '1'</td><td>'B', 'E', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'B0', '41'	'T', 'A'	'X', 'N'	'42'	'T'	'X', 'N'	'D0', '21', '22', '23'	'D', 'T', 'A'	'B', 'E', 'N'	'D0', '21', '22', '23'	'A', '1'	'B', 'E', 'N'
Key Usage	Algorithm	Mode of Use															
'B0', '41'	'T', 'A'	'X', 'N'															
'42'	'T'	'X', 'N'															
'D0', '21', '22', '23'	'D', 'T', 'A'	'B', 'E', 'N'															
'D0', '21', '22', '23'	'A', '1'	'B', 'E', 'N'															
Destination KSN Descriptor	3 H	<p>The descriptor for the KSN (in the next field). For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i>.</p> <p>Only present if Destination Key Type is a BDK.</p> <p>If Destination Key is an AES BDK-1 or BDK-2, this field is ignored and should be set to '000'.</p>															

Field	Length & Type	Details
Destination Key Serial Number	12 - 20 H or 24 H	The KSN supplied by the PIN pad. For further information on DUKPT, see the <i>payShield 10K Host Programmer's manual</i> . Only present if Destination Key Type is a BDK. If the Destination Key is an AES BDK-1 or BDK-2 this field will be 24 Hex digits
Source IV	16 H or 32 H	The source IV, to be used in conjunction with Source Key. When translating the first of a series of blocks, the initial Source IV should match the initial IV used to encrypt the original message. For subsequent blocks, this value should be the Source IV returned from translating the previous block. If using a DES/3DES Source Key, the Source IV will be a 16 H field. If using an AES Source Key, the Source IV will be a 32 H field. Only present if the Source Mode Flag is '01', '02' or '03'.
Destination IV	16 H or 32 H	The input IV, to be used in conjunction with Destination Key. When translating the first of a series of blocks, the initial Destination IV should be set by the caller – a typical value is {00 00 00 00 00 00 00 00}. For subsequent blocks, this value should be the Destination IV returned from translating the previous block. If using a DES/3DES Destination Key, the Destination IV will be a 16 H field. If using an AES Destination Key, the Destination IV will be a 32 H field. Only present if the Destination Mode Flag is '01', '02' or '03'.

If Source Mode Flag ≠ '04' or '13', the following TWO fields must be present:

Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes. Note: When using FF1, the Message length must comply with NIST SP800-38G : <ul style="list-style-type: none">• Radix in the range 2 ... 2¹⁶• radix^{minlen} >= 100• 2 <= minlen <= maxlen <= 2³²
Encrypted Message	n B	The message to be translated. The length & type of the field will depend on the value of the Input Format Flag: Input Format Flag = '0' (Binary); n = multiple of 8 when using a DES/3DES key, or a multiple of 16 when using an AES key.
	n H	Note: When using FF1, the Encrypted Message must consist of a string of bytes each having a value less than the Source FF1 Radix Value.

If Source Mode Flag = '04' or '13', the following fields must be present:

Block Count	2 N	Indicates the number of Encrypted Blocks to be decrypted in this command. Value: '01' ... '04'. Each Encrypted Block is of a certain Block Type, as defined here: <ul style="list-style-type: none">• Primary Account Number (PAN)• Cardholder Name• Track 1 Discretionary Data• Track 2 Discretionary Data This command supports the decryption of up to 4 Encrypted Blocks within a single call, but each Block Type must be unique – e.g. it is not permitted to decrypt two 'Cardholder Name' blocks in a single call to this command. Note: If Mode Flag = '13', the Encrypted Blocks fields must be supplied in the order given above.
-------------	-----	---

If Source Mode Flag = '04' or '13', the following fields must be present:

Block Count	2 N	Indicates the number of Encrypted Blocks to be translated in this command. Value: '01' ... '04'. Each Encrypted Block is of a certain Block Type, as defined here: <ul style="list-style-type: none">• Primary Account Number (PAN)• Cardholder Name• Track 1 Discretionary Data• Track 2 Discretionary Data This command supports the translation of up to 4 Encrypted Blocks within a single call, but each Block Type must be unique – e.g. it is not permitted to translate two 'Cardholder Name' blocks in a single call to this command. Note: If Mode Flag = '13', the Encrypted Blocks fields must be supplied in the order given above.
-------------	-----	---

If Source Mode Flag = '04', the following THREE fields must be repeated 'Block Count' times:

Field	Length & Type	Details
Block Type	1 A	Indicates the type of data being translated. 'A': Primary Account Number (PAN) 'B': Cardholder Name 'C': Track 1 Discretionary Data 'D': Track 2 Discretionary Data Note: The Encrypted Block field will be validated after being decrypted.
Block Length	4 H	The length of the following field, in bytes.
Encrypted Block	n B n H	The encrypted data. The format of this field will depend on the value of the Output Format Flag field: If Output Format Flag = '0' (Binary). If Output Format Flag = '1' (Hex-Encoded Binary).
If Mode Flag = '13', the following THREE, or FOUR, fields must be repeated 'Block Count' times.		
Block Type	1 A	Indicates the type of data being translated. 'A': Primary Account Number (PAN) 'B': Cardholder Name 'C': Track 1 Discretionary Data 'D': Track 2 Discretionary Data Note: The Encrypted Block field will be validated after being decrypted.
Check Digit Flag	1 N	Indicates if original unencrypted PAN had a valid check digit. '0': Check Digit valid '1': Check Digit invalid Only present if Block Type = 'A'.
Block Length	4 H	The length of the following field, in bytes.
Encrypted Block	n B n A n A n B	The encrypted data. The format of the block will depend on the value of the Block Type field. If Block Type = 'A' (BCD – Binary Coded Decimal) If Block Type = 'B' (Text – ASCII or EBCDIC) If Block Type = 'C' (Text – ASCII or EBCDIC) If Block Type = 'D' (4-bit BASE15 chars)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'M5'.
Error Code	2 A	'00': No error '02': Invalid Source Mode Flag field or Radix Flag/Value field '03': Invalid Input Format Flag field '04': Invalid Output Format Flag field '05': Invalid Key Type field '06': Actual Message Length is too Short '07': Invalid Destination Mode Flag Field '08': Invalid destination Key Type Field '10': Decryption Key Parity Error '11': Encryption Key Parity Error '15': Actual Message Length is too Long '35': Illegal Message Format '67': Command not licensed '68': Command disabled or a standard error code.
Source IV	16 H or 32 H	The output IV, calculated using the Source Key. When translating a series of blocks, this Source IV should be supplied as input when encrypting the next block. If using a DES/3DES Source Key, the Source IV will be a 16 H field. If using an AES Source Key, the Source IV will be a 32 H field. Only present if the Source Mode Flag is '01', '02' or '03'.
Destination IV	16 H or 32 H	The output IV, calculated using Destination Key. When translating a series of blocks, this Destination IV should be supplied as input when encrypting the next block. If using a DES/3DES Destination Key, the Destination IV will be a 16 H field. If using an AES Destination Key, the Destination IV will be a 32 H field. Only present if the Destination Mode Flag is '01', '02' or '03'.
If Destination Mode Flag ≠ '04', the following TWO fields will be present:		
Message Length	4 H	The length of the following field, in bytes.
Translated Message	n B	The translated message. The length & type of the field will depend on the value of the Output Format Flag: Output Format Flag = '0' (Binary); n = multiple of 8 when using a DES/3DES key, or a multiple of 16 when using an AES key.
	n H	Output Format Flag = '1' (Hex-Encoded Binary); n = multiple of 16 when using a DES key, or a multiple of 32 when using an AES/3DES key. Note: When using FF1, the Translated Message will consist of a string of bytes each having a value less than the Destination FPE Radix Value.
If Destination Mode Flag = '04', the following field will be present:		
Block Count	2 N	Indicates the number of Translated Blocks in the following fields.
If Destination Mode Flag = '04', the following THREE fields are repeated 'Block Count' times.		
Block Type	1 A	Indicates the type of data that was translated. 'A': Primary Account Number (PAN) 'B': Cardholder Name 'C': Track 1 Discretionary Data 'D': Track 2 Discretionary Data
Block Length	4 H	The length of the following field, in bytes.
Translated Block	n B	The translated data. The format of this field will depend on the value of the Output Format Flag field: If Output Format Flag = '0' (Binary). If Output Format Flag = '1' (Hex-Encoded Binary).
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

7 User Authentication Commands

7.1 HMAC Commands

The payShield 10K provides the following host commands to support generic HMAC operations:

Function	Command	Page
<i>Generate an HMAC Secret Key</i>	L0 (L1)	460
<i>Generate an HMAC on a Block of Data</i>	LQ (LR)	463
<i>Verify an HMAC on a Block of Data</i>	LS (LT)	465
<i>Import an HMAC key under a ZMK</i>	LU (LV)	467
<i>Export an HMAC key under a ZMK</i>	LW (LX)	471
<i>Translate a HMAC Key from Old LMK to New LMK</i>	LY (LZ)	474

Generate an HMAC Secret Key

Variant LMK	Key Block LMK
Available in package(s): Premium	
Variant LMK	Authorization: Determined by KTT(G) Activity: generate.hmac.host
Key Block LMK	Authorization: Not required

Function: Generate an HMAC Secret Key.

Notes: This function generates a private key for use in a Keyed-Hash Message Authentication Code (HMAC).

FIPS 198 states that there is little value in choosing a key longer in length than the length of the hash algorithm output (20 bytes in the case of SHA-1). However, this limitation will not be enforced by this command, so the maximum length of a key generated by this command is limited only by the size of the HSM's message buffers.

The HMAC Key may only be used as input to HMAC functions; it is not available for use with any other HSM functions.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'L0' (L zero).
Hash Identifier	2 N	For a Variant LMK: Identifier of the Hash Algorithm: '01': SHA-1 '05': SHA-224 '06': SHA-256 '07': SHA-384 '08': SHA-512.
	or 2 H	For a Key Block LMK: This field is ignored; should be set to 'FF'.
HMAC Key Usage	2 N	For a Variant LMK: '01': HMAC Generation '02': HMAC Verification '03': HMAC Generation and Verification.
	or 2 H	For a Key Block LMK: This field is ignored; should be set to 'FF'.
HMAC Key Length	4 N	The number of bytes in the HMAC Key. Must satisfy ($L/2 \leq$ key length), where L is the size of the hash function output (so L = 20 in the case of SHA-1). See Note above.
HMAC Key Format	2 N	Defines the format of the stored key. For a Variant LMK: '00': Thales HMAC Key format. For a Key Block LMK: '04': Thales HMAC Key Block format.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.

payShield 10K Core Host Commands

Field	Length & Type	Details
COMMAND MESSAGE		
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
The following section applies only when generating a key block.		
Delimiter	1 A	Value '#'. Required when generating a key block. If present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the key block header (bytes 5-6); must be present if the above Delimiter is present; permitted values: '61' – SHA-1 '62' – SHA-224 '63' – SHA-256 '64' – SHA-384 '65' – SHA-512
Algorithm	2 A	Algorithm field; the first character will be included in the algorithm field in the key block header (byte 7); must be present if the above Delimiter is present; permitted values: 'H0' – HMAC
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in the <i>payShield 10K Host Programmer's manual</i> .
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'L1'.
Error Code	2 A	'00': No error '04': Key length error '05': Invalid Hash Identifier '06': Invalid Key Usage '07': Invalid Key Format '67': Command not licensed '68': Command disabled or a standard error code.
HMAC Key Length	4 N or 4 H	For a Variant LMK: Length (in bytes) of the next field. For a Key Block LMK: This field is reserved, and set to 'FFFF'.
HMAC Key	n B or n A	The new HMAC Key. Note: the key is <i>not</i> prefixed with a key scheme character. For a Variant LMK, the 'HMAC Key' is encrypted under the LMK pair 34-35 variant 1. For a Key Block LMK, the 'HMAC Key' is encrypted under the LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate an HMAC on a Block of Data

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Generate an HMAC on a Block of Data.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'LQ'.						
Hash Identifier	2 N or 2 H	For a Variant LMK: Identifier of the Hash Algorithm: '01': SHA-1 '05': SHA-224 '06': SHA-256 '07': SHA-384 '08': SHA-512. For a Key Block LMK: This field is ignored; should be set to 'FF'.						
HMAC Length	4 N	Length (t) in bytes of the output HMAC. Must satisfy $(L/2 \leq t \leq L)$, where L is the size of the hash function output (so L = 20 in the case of SHA-1), unless the Minimum HMAC Length has been configured otherwise using the console CS (Configure Security) command						
HMAC Key Format	2 N	Defines the format of the stored key. For a Variant LMK: '00': Thales HMAC Key format. For a Key Block LMK: '04': Thales HMAC Key Block format.						
HMAC Key Length	4 N or 4 H	For a Variant LMK: Length (in bytes) of the next field. For a Key Block LMK: This field is ignored; should be set to 'FFFF'.						
HMAC Key	n B or n A	The HMAC Key, used to calculate the HMAC. Note: the key is <i>not</i> prefixed with a key scheme character. For a Variant LMK, the 'HMAC Key' is encrypted under the LMK pair 34-35 variant 1. For a Key Block LMK, the 'HMAC Key' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'61' – '65'</td> <td>'H'</td> <td>'C', 'G', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'61' – '65'	'H'	'C', 'G', 'N'
Key Usage	Algorithm	Mode of Use						
'61' – '65'	'H'	'C', 'G', 'N'						
Delimiter	1 A	Value ';'. Only required when using a Variant LMK.						
Data Length	5 N	Length of message to be authenticated						
Message Data	n B	Data to be authenticated						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'LR'.
Error Code	2 A	'00': No error '04': HMAC Length error '05': Invalid Hash Identifier '06': Invalid Key Usage '07': Invalid Key Format '08': HMAC Key error '67': Command not licensed '68': Command disabled or a standard error code.
HMAC Length	4 N	Length (t) in bytes of output HMAC, as defined in command message.
HMAC	n B	HMAC (length as defined in the previous field).
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify an HMAC on a Block of Data

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Verify an HMAC on a Block of Data.

Notes:

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'LS'.						
Hash Identifier	2 N	For a Variant LMK: Identifier of the Hash Algorithm: '01': SHA-1 '05': SHA-224 '06': SHA-256 '07': SHA-384 '08': SHA-512.						
	or 2 H	For a Key Block LMK: This field is ignored; should be set to 'FF'.						
HMAC Length	4 N	Length (t) in bytes of the HMAC to be verified Must satisfy ($L/2 \leq t \leq L$), where L is the size of the hash function output (so L = 20 in the case of SHA-1), unless the Minimum HMAC Length has been configured otherwise using the console CS (Configure Security) command.						
HMAC	n B	HMAC to be verified (length as defined in the previous field).						
HMAC Key Format	2 N	Defines the format of the stored key. For a Variant LMK: '00': Thales HMAC Key format. For a Key Block LMK: '04': Thales HMAC Key Block format.						
HMAC Key Length	4 N	For a Variant LMK: Length (in bytes) of the next field.						
	or 4 H	For a Key Block LMK: This field is ignored; should be set to 'FFFF'.						
HMAC Key	n B	The HMAC Key, used to verify the supplied HMAC. Note: the key is <i>not</i> prefixed with a key scheme character.						
	or n A	For a Variant LMK, the 'HMAC Key' is encrypted under the LMK pair 34-35 variant 1. For a Key Block LMK, the 'HMAC Key' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'61' – '65'</td> <td>'H'</td> <td>'C', 'V', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'61' – '65'	'H'	'C', 'V', 'N'
Key Usage	Algorithm	Mode of Use						
'61' – '65'	'H'	'C', 'V', 'N'						
Delimiter	1 A	Value ';'. Only required when using a Variant LMK.						
Data Length	5 N	Length of message to be authenticated.						
Message Data	n B	Data to be authenticated.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'LT'.
Error Code	2 A	'00': No error '01': HMAC verification failure '04': HMAC Length error '05': Invalid Hash Identifier '06': Invalid Key Usage '07': Invalid Key Format '08': HMAC Key error '67': Command not licensed '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Import an HMAC key under a ZMK

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Variant LMK	Authorization: Determined by KTT(I) Activity: import.10C.host
Key Block LMK	Authorization: If import from non-KB Activity: import.10C.host

Function: Import an HMAC under a Zone Master Key (ZMK).

Notes:

Transport Format	ZMK algorithm	Notes
01 (PKCS#11 ECB)	3DES	Requires security setting " <i>Enable PKCS#11 import and export for HMAC keys</i> " to be set to "Yes".
02 (PKCS#11 CBC)	3DES	The encrypted HMAC key must be a multiple of 8 bytes.
03 (X9.17)	3DES	Requires security setting " <i>Enable ANSI X9.17 import and export for HMAC keys</i> " to be set to "Yes". The encrypted HMAC key must contain no padding, and be a multiple of 8 bytes.
04 (Thales Key Block)	3DES	Requires use of a Key Block LMK.
05 (TR-31 Key Block)	AES	Requires use of an AES Key Block LMK. The TR-31 key block optional header must include the 'HM' optional block, specifying the Hash Algorithm

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'LU'.
ZMK		The Zone Master Key, used to decrypt the 'HMAC key (ZMK)'.

Field	Length & Type	Details								
COMMAND MESSAGE										
	32 H or 'U' + 32 H or 'T' + 48 H	For a Variant LMK, the 'ZMK' is encrypted under the LMK pair 04-05.								
	or 'S' + n A	For a Key Block LMK, the 'ZMK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'K0', '52'</td> <td>'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'K0', '52'	'T', 'A'	'B', 'D', 'N'		
Key Usage	Algorithm	Mode of Use								
'K0', '52'	'T', 'A'	'B', 'D', 'N'								
The following 3 fields apply if Transport Format = '00', '01', '02' or '03' (All non-Key Block formats):										
HMAC Key (ZMK) Length	4 N	This field specifies the length (in bytes) of the next field.								
HMAC Key (ZMK)	n B	The HMAC Key to be imported, encrypted under the ZMK. Note: the key is <i>not</i> prefixed with a key scheme character.								
Delimiter	1 A	Value ':'.								
The following 2 fields apply if Transport Format = '04' (Thales Key Block formats):										
HMAC Key (ZMK) Length	4 H	This field is reserved and must be set to 'FFFF'.								
HMAC Key (ZMK)	n A	The HMAC Key to be imported, encrypted under the ZMK. Note: the key is <i>not</i> prefixed with a key scheme character. The HMAC Key (ZMK) must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'61' – '65'</td> <td>'H'</td> <td>'C', 'G', 'V', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'61' – '65'	'H'	'C', 'G', 'V', 'N'		
Key Usage	Algorithm	Mode of Use								
'61' – '65'	'H'	'C', 'G', 'V', 'N'								
The following 2 fields apply if Transport Format = '05' (TR-31 Key Block formats):										
HMAC Key (ZMK) Length	4 H	This field is reserved and must be set to 'FFFF'.								
HMAC Key (ZMK)	'R' + n A	The HMAC Key to be imported, encrypted under the ZMK, and must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Hash Algorithm specified in 'HM' optional block</th> <th>Mode of Use</th> </tr> <tr> <td>'M7'</td> <td>'H'</td> <td>'10', '20', '21', '22', '23'</td> <td>'C', 'G', 'V', 'N'</td> </tr> </table>	Key Usage	Algorithm	Hash Algorithm specified in 'HM' optional block	Mode of Use	'M7'	'H'	'10', '20', '21', '22', '23'	'C', 'G', 'V', 'N'
Key Usage	Algorithm	Hash Algorithm specified in 'HM' optional block	Mode of Use							
'M7'	'H'	'10', '20', '21', '22', '23'	'C', 'G', 'V', 'N'							
Transport Format	2 N	Format of the HMAC Key (ZMK); see Notes above: '00': proprietary format '01': PKCS#11 ECB format '02': PKCS#11 CBC format '03': X9.17 format '04': Thales Key Block format (not permitted for variant LMK) '05': X9 TR-31:2018								
HMAC Key Format (LMK)	2 N	Defines the format of the LMK encrypted HMAC Key. For a Variant LMK: '00': Thales HMAC Key format. For a Key Block LMK: '04': Thales HMAC Key Block format.								
Hash Identifier	2 N	Only present if Transport Format = '01', '02' or '03'. Identifier of the Hash Algorithm: '01': SHA-1 '05': SHA-224 '06': SHA-256 '07': SHA-384 '08': SHA-512.								
HMAC Key Usage	2 N	Only present if Transport Format = '01', '02' or '03'. HMAC Key Usage value: '01': HMAC Generation '02': HMAC Verification '03': HMAC Generation and Verification.								

payShield 10K Core Host Commands

Field	Length & Type	Details
COMMAND MESSAGE		
HMAC Key Length	4 N	Only present if Transport Format = '01', '02' or '03'. The number of bytes of the HMAC Key. Must satisfy $L/2 \leq$ key length, where L is the size of the hash function output (so L = 20 in the case of SHA-1).
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
The following section applies only when generating a key block.		
Delimiter	1 A	Value '#'. Required when importing to Thales key block format when Transport Format ≠ '04'. If present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the key block header (bytes 5-6); must be present if the above Delimiter is present; permitted values: '61': SHA-1 '62': SHA-224 '63': SHA-256 '64': SHA-384 '65': SHA-512 Note: If importing a key from format '00', this field must be compatible with the Hash Identifier of the key being imported.
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in the <i>payShield 10K Host Programmer's manual</i> . Must be "N" or "S".
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04' to X'FF'; if value = X'04', then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'LV'.
Error Code	2 A	'00': No error '03': Invalid Transport Format '04': HMAC Key Length error '05': Invalid Hash Identifier '06': Invalid Key Usage '07': Invalid Key Format '08': HMAC Key error '10': ZMK parity error '67': Command not licensed '68': Command disabled or a standard error code.
HMAC Key Length	4 N	For a Variant LMK: Length (in bytes) of the next field.
	or 4 H	For a Key Block LMK: This field is reserved, and set to 'FFFF'.
HMAC Key (under LMK)		The imported HMAC key.

payShield 10K Core Host Commands

	n B or n A	Note: the key is <i>not</i> prefixed with a key scheme character. For a Variant LMK, the 'HMAC Key' is encrypted under the LMK pair 34-35 variant 1. For a Key Block LMK, the 'HMAC Key' is encrypted under the LMK.
End Message Delimiter Message Trailer	1 C n A	Present only if present in the command message. Value X'19. Present only if present in the command message. Maximum length 32 characters.

Export an HMAC key under a ZMK

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Variant LMK	Authorization: Determined by KTT(E) Activity: export.10C.host
Key Block LMK	Authorization: If export to non-KB Activity: export.10C.host

Function: Export an HMAC under a Zone Master Key (ZMK).

Notes:

Transport Format	ZMK algorithm	Notes
01 (PKCS#11 ECB)	3DES	Requires security setting " <i>Enable PKCS#11 import and export for HMAC keys</i> " to be set to "Yes".
02 (PKCS#11 CBC)	3DES	The encrypted HMAC key must be a multiple of 8 bytes.
03 (X9.17)	3DES	Requires security setting " <i>Enable ANSI X9.17 import and export for HMAC keys</i> " to be set to "Yes". The encrypted HMAC key must contain no padding, and be a multiple of 8 bytes.
04 (Thales Key Block)	3DES	Requires use of a Key Block LMK.
05 (TR-31 Key Block)	AES	Requires use of an AES Key Block LMK. The output TR-31 key block will include an optional block 'HM', specifying the Hash Algorithm.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'LW'.						
ZMK	32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The Zone Master Key, used to encrypt the 'HMAC Key'. For a Variant LMK, the 'ZMK' is encrypted under the LMK pair 04-05. For a Key Block LMK, the 'ZMK' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'K0', '52'</td> <td>'T', 'A'</td> <td>'B', 'E', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'K0', '52'	'T', 'A'	'B', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'K0', '52'	'T', 'A'	'B', 'E', 'N'						
HMAC Key Format (LMK)	2 N	Defines the format of the LMK encrypted HMAC Key. For a Variant LMK: '00': Thales HMAC Key format. For a Key Block LMK: '04': Thales HMAC Key Block format.						
Transport Format	2 N	Format of HMAC Key (ZMK); see Notes above '00': proprietary format '01': PKCS#11 ECB format '02': PKCS#11 CBC format '03': X9.17 format '04': Thales Key Block format (not permitted for variant LMK) '05': X9 TR-31:2018 format						
HMAC Key (LMK) Length	4 N or 4 H	For a Variant LMK: Length (in bytes) of the next field. For a Key Block LMK: This field is reserved, and should be set to 'FFFF'.						
HMAC Key (under LMK)	n B or n A	The HMAC Key to be exported. Note: the key is <i>not</i> prefixed with a key scheme character. For a Variant LMK, the 'HMAC Key' is encrypted under the LMK pair 34-35 variant 1. For a Key Block LMK, the 'HMAC Key' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'61' - '65'</td> <td>'H'</td> <td>'C', 'G', 'V', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'61' - '65'	'H'	'C', 'G', 'V', 'N'
Key Usage	Algorithm	Mode of Use						
'61' - '65'	'H'	'C', 'G', 'V', 'N'						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
The following section applies only when exporting to a key block format (e.g. TR-31 or Thales Key Block) when using a Key Block LMK.								
Delimiter	1 A	Value '&'. Optional; can only be present when the exported key is key block; if present, the following field must also be present.						
Modified Exportability	1 A	Exportability field, to be included in the key block header; only permitted value is "N"; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'LX'.
Error Code	2 A	'00': No error '03': Invalid Transport Format '07': Invalid Key Format '08': HMAC Key error '10': ZMK parity error '67': Command not licensed '68': Command disabled or a standard error code.
The following 5 fields apply when Transport Format = '00', '01', '02' or '03':		
HMAC Key (ZMK) Length	4 N	This field specifies the length (in bytes) of the next field.
HMAC Key (ZMK)	n B	The HMAC Key, encrypted under the ZMK, in the format defined by 'Transport Format'. Note: the key is <i>not</i> prefixed with a key scheme character.
Hash Identifier	2 N	Only present if Transport Format = '01', '02' or '03'. Identifier of the Hash Algorithm: '01': SHA-1 '05': SHA-224 '06': SHA-256 '07': SHA-384 '08': SHA-512.
HMAC Key Usage	2 N	Only present if Transport Format = '01', '02' or '03'. '01': HMAC Generation '02': HMAC Verification '03': HMAC Generation and Verification.
HMAC Key Length	4 N	Only present if Transport Format = '01', '02' or '03'. The number of bytes of the HMAC Key. Must satisfy $L/2 \leq$ key length, where L is the size of the hash function output (so L = 20 in the case of SHA-1).
The following 2 fields apply when Transport Format = '04' (Thales Key Block format):		
HMAC Key (ZMK) Length	4 H	This field specifies the length (in bytes) of the next field.
HMAC Key (ZMK)	n A	The HMAC Key, encrypted under the ZMK, in Thales Key Block format. Note: the key is <i>not</i> prefixed with a key scheme character.
The following 2 fields apply when Transport Format = '05' (X9 TR-31:2018 format):		
HMAC Key (ZMK) Length	4 H	This field specifies the length (in bytes) of the next field excluding 'R'.
HMAC Key (ZMK)	'R' + n A	The HMAC Key, encrypted under the ZMK, in X9 TR-31:2018 format.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate a HMAC Key from Old LMK to New LMK

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Translate an HMAC Key from encryption under an old LMK to encryption under a new LMK.

Notes: This command can also be used to change the format of the stored HMAC Key.

When translating keys to key block format, this command restricts the choice of Mode of Use to match the "HMAC Key Usage" specified at the time the HMAC key was created (e.g. using the 'L0' command).

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'LY'.						
Input HMAC Key Format	2 N	Defines the format of the Input HMAC Key (encrypted under the old LMK). For an old Variant LMK: '00': Thales HMAC Key format. For an old Key Block LMK: '04': Thales HMAC Key Block format.						
Output HMAC Key Format	2 N	Defines the format of the Output HMAC Key (encrypted under the current LMK). For a current Variant LMK: '00': Thales HMAC Key format. For a current Key Block LMK: '04': Thales HMAC Key Block format.						
HMAC Key Length	4 N or 4 H	For an old Variant LMK: Length (in bytes) of the next field. For an old Key Block LMK: This field is reserved, and set to 'FFFF'.						
HMAC Key	n B or n A	The HMAC Key to be translated, encrypted under the old LMK. Note: the key is <i>not</i> prefixed with a key scheme character. For an old Variant LMK, the 'HMAC Key' is encrypted under the old LMK pair 34-35 variant 1. For an old Key Block LMK, the 'HMAC Key' must comply with the following:						
		<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'61' - '65'</td> <td>'H'</td> <td>'C', 'G', 'V', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'61' - '65'	'H'	'C', 'G', 'V', 'N'
Key Usage	Algorithm	Mode of Use						
'61' - '65'	'H'	'C', 'G', 'V', 'N'						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						

Field	Length & Type	Details
COMMAND MESSAGE		
The following section applies only when translating from a Variant LMK to a Key Block LMK.		
Delimiter	1 A	Value '#'. Required when translating to Thales key block format. If present, the following fields must be present.
Key Usage	2 A	<p>Key Usage field, to be included in the key block header (bytes 5-6); must be present if the above Delimiter is present; permitted values:</p> <ul style="list-style-type: none"> '61' – SHA-1 '62' – SHA-224 '63' – SHA-256 '64' – SHA-384 '65' – SHA-512 <p>Note: If translating a key from format '00', this field must be compatible with the Hash Identifier of the input key.</p>
Mode of Use	1 A	Mode of Use field, to be included in the key block header; any permitted value for the key type; must be present if the above Delimiter is present. For a list of possible values, see the Mode of Use Table in the <i>payShield 10K Host Programmer's manual</i> .
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the key block header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in the <i>payShield 10K Host Programmer's manual</i> .
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
The following section applies only when translating to a Variant LMK.		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'LZ'.
Error Code	2 A	<p>'00': No error '03': Invalid Output Key Format '07': Invalid Input Key Format '08': HMAC Key error '67': Command not licensed '68': Command disabled or a standard error code.</p>
HMAC Key Length	4 N	<p>For a current Variant LMK: Length (in bytes) of the next field.</p> <p>For a current Key Block LMK: This field is reserved, and set to 'FFFF'.</p>
HMAC Key	n B or n A	<p>The translated HMAC key, encrypted under the current LMK. Note: the key is <i>not</i> prefixed with a key scheme character.</p> <p>For a current Variant LMK, the 'HMAC Key' is encrypted under the LMK pair 34-35 variant 1.</p> <p>For a current Key Block LMK, the 'HMAC Key' is encrypted under the LMK.</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

7.2 WebPIN Commands

The payShield 10K provides the following host commands to support the WebPIN product:

Function	Command	Page
<i>Generate a Random Alphanumeric PIN</i>	ZA (ZB)	477
<i>Print Alphanumeric PIN/Alphanumeric PIN and Solicitation Data</i>	ZE (ZF, ZZ)	478
<i>Translate an Alphanumeric PIN from old LMK to new LMK Encryption</i>	ZK (ZL)	480
<i>Translate Encrypted PIN to Encrypted Alphanumeric PIN</i>	ZM (ZN)	482
<i>Verify Alphanumeric PIN Block from Internet, return new encrypted PIN & Verify MAC</i>	ZU (ZV)	483

Note that other (older) WebPIN commands are available and are described in the *payShield 10K Legacy Host Commands* manual.

Generate a Random Alphanumeric PIN

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not Required	

Function: Generate a Random Alphanumeric PIN and encrypt it under LMK pair 36-37 with Variant 1.

Notes: A Random Alphanumeric PIN with character set 0 – 9, A – Z and a – z. It should not contain characters "0" (ASCII 30H), "O" (ASCII 4FH), "1" (ASCII 31H) and "l" (ASCII 49H and 6CH) to avoid confusion. No digits should occur more than 4 times.
The Alphanumeric PIN is left justified and padded with 0x20 (i.e. space character).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'ZA'.
Encrypted AN-PIN Length	1 N	Encrypted Alphanumeric PIN length '0' = 32 Hex - select this value when using the MD5 hash algorithm at the client '1' = 48 Hex - select this value when using the SHA-1 hash algorithm at the client
AN-PIN length	2 N	Length of Alphanumeric PIN to be generated. If Encrypted AN-PIN Length = '0', 06 <= AN-PIN Length <= 16 If Encrypted AN-PIN Length = '1', 06 <= AN-PIN Length <= 20
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ZB'.
Error Code	2 N	'00': No errors. '04': Invalid Encrypted AN-PIN Length. '13': LMK error; report to supervisor. '15': Error in input data. Or any standard error code
Encrypted AN-PIN	32 H or 48 H	The Alphanumeric PIN encrypted under LMK pair 36-37 with Variant 1. Length depends on Encrypted AN-PIN Length.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Print Alphanumeric PIN/Alphanumeric PIN and Solicitation Data

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Required	

Function: Print the Alphanumeric PIN/Alphanumeric PIN and solicitation data at the HSM-attached terminal.

Notes:

- The HSM must be in Authorised state.
- A printer must be attached to the HSM Auxiliary port.
- The HSM must have a print format already defined.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'ZE'.
Document Type	1 A	'A': for 1st mailer on a 2-up form. 'B': for 2nd mailer on a 2-up form. 'C': for a 1-up form.
Encrypted AN-PIN Length	1 N	Encrypted Alphanumeric PIN length '0': 32 Hex '1': 48 Hex
Encrypted AN-PIN	32 H or 48 H	The Alphanumeric PIN encrypted under LMK pair 36-37 with Variant 1.
Print Field 0	n A	The print field defined as Print Field 0 in the print format definition (must not contain a ';' character).
Delimiter	1 A	Value ':'.
Print Field 1	n A	The print field defined as Print Field 1 in the print format definition (must not contain a ';' character).
.	.	.
.	.	.
.	.	.
Last Print Field	n A	The last print field defined in the print format definition (must not contain a ';' character).
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (before printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ZF'.
Error Code	2 N	<p>'00': No errors.</p> <p>'04': Invalid Encrypted AN-PIN Length.</p> <p>'13': LMK error; report to supervisor.</p> <p>'14': Error in encrypted PIN.</p> <p>'15': Error in input data.</p> <p>'16': Printer not ready.</p> <p>'17': HSM not in authorised state.</p> <p>'18': Document definition not loaded.</p> <p>Or any standard error code</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (after printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ZZ'.
Error Code	2 N	<p>'00': No errors.</p> <p>'16': Printer not ready.</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.

Translate Encrypted PIN to Encrypted Alphanumeric PIN

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not Required	

Function: To translate encrypted PIN to encrypted Alphanumeric PIN under LMK pair 36-37 with Variant 1.

Notes: Error 50 is returned, if this command is used to convert Original Encrypted PIN (OEP) encrypted under LMK pair 36-37 with Variant 1 to PIN Format Required (PFR) with input parameter = 0.

Also note that the PIN Format Required (PFR) parameter matches the Hash Mode given in *WebPIN Appendix A - Message Formats*. (The *WebPIN Appendices* can be found in Section 14 of the *payShield 10K Legacy Host Commands* manual). A PFR value of 4 is not used in this command but is reserved for use as defined in the Appendix.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'ZM'.
Original Encrypted PIN (OEP)	1 N	Original encrypted PIN '0': PIN encrypted under LMK pair 02-03 '1': Non-hashed AN-PIN encrypted under LMK pair 36-37 with variant (generated by "ZA" command)
PIN Format Required (PFR)	1 N	PIN Format to be returned to host '0': Padding with "0x20"; used for JETCO '1': MD5 for JETCO '2': MD5 for WebPIN '3': SHA-1 for WebPIN (Note, '4' = Reserved)
Primary Account Number (PAN)	12 N	The 12 right-most digits of the PAN, excluding the check digit. (Only present when OEP = 0 "OR" PFR = 2 or 3)
Encrypted PIN	L N or L H	The PIN encrypted under LMK pair 02-03. (Only present when OEP = 0)
Encrypted AN-PIN	32 H	The AN-PIN encrypted under LMK pair 36-37 with Variant 1. (Only present when OEP = 1 "AND" PFR = 0, 1 or 2)
Encrypted AN-PIN	48 H	The AN-PIN encrypted under LMK pair 36-37 with Variant 1. (Only present when OEP = 1 "AND" PFR = 3)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ZN'.
Error Code	2 N	'00': No errors. '03': Invalid Original Encrypted PIN code. '05': Invalid PIN Format Required code. '13': LMK error; report to supervisor. '14': Error in encrypted PIN. '15': Error in input data. '50': Invalid combination. Or any standard error code
Encrypted AN-PIN	32 H	The Alphanumeric PIN encrypted under LMK pair 36-37 with Variant 1. (Only present when PIN Format Required (PFR) = 0 or 1 or 2)
Encrypted AN-PIN	48 H	The Alphanumeric PIN encrypted under LMK pair 36-37 with Variant 1. (Only present when PIN Format Required (PFR) = 3)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate an Alphanumeric PIN from old LMK to new LMK Encryption

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not Required	

Function: To translate an Alphanumeric PIN from encryption under the LMK pair held in “key change storage” to encryption under LMK pair 36-37 with Variant 1.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'ZK'.
Encrypted AN-PIN Length	1 N	Encrypted Alphanumeric PIN length '0': 32 Hex '1': 48 Hex
Encrypted AN-PIN	32 H or 48 H	The Alphanumeric PIN encrypted under the LMK pair in “key change storage”.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ZL'.
Error Code	2 N	'00': No errors. '04': Invalid Encrypted AN-PIN Length. '13': LMK error; report to supervisor. '14': Error in encrypted PIN. '15': Error in input data. Or any standard error code
Encrypted AN-PIN	32 H or 48 H	The Alphanumeric PIN encrypted under new LMK pair 36-37 with Variant 1.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify Alphanumeric PIN Block from Internet, return new encrypted PIN & Verify MAC

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not Required	

Function: To verify AN-PIN Block from Internet and optionally, return new encrypted AN-PIN and verify MAC using ANSI X9.19.

Notes: The Message is either in Alphanumeric PIN and MAC format, where only verification is carried out, or Alphanumeric Change PIN and MAC format where both verification of the old AN-PIN and return of the new AN-PIN is carried out. The Type field in these messages determines the format. The formats of these messages are defined in the the *WebPIN Appendix – Message Formats*. (The *WebPIN Appendices* can be found in Section 14 of the *payShield 10K Legacy Host Commands* manual).

The Alphanumeric PIN Block in the message is encrypted by a 128-bit session PIN key (Triple-DES: Encrypt - Decrypt - Encrypt). The Session PIN Key, the IV and also the MAC Key are derived from a Master Key which is in turn encrypted under a public key.

The TDES Electronic code book (TECB) and Cipher block chaining (TCBC) modes are supported. Both are defined in the ANSI X9.52 standard. The TCBC mode requires an Initialisation Value (IV) to be used when decrypting the Alphanumeric PIN.

The Master Key is delivered in a PKCS#1 HSM Key Block formatted as defined in the *payShield 10K Host Programmer's manual* – RSA Section. The Master Key Format is specified in *WebPIN Appendix - Master Key Format* and the Key Derivation Algorithm and Key Block Format are defined in *WebPIN Appendix - Key Derivation Algorithm and Key Block Format*. (The *WebPIN Appendices* can be found in Section 14 of the *payShield 10K Legacy Host Commands* manual.)

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'ZU'.
Encryption Identifier	2 N	Identifier of the algorithm used to encrypt the Master Key. Must be '01' for RSA. Provided for compatibility with standard HSM RSA Host commands. Refer to the <i>payShield 10K Host Programmer's manual</i> for more details.
Pad mode identifier	2 N	Identifier of the pad mode used in the encryption process. Refer to the <i>payShield 10K Host Programmer's manual</i> for more details.
Private Key Flag	2 N	Flag, indicates the location of the Private key. The number is the index of the stored private key, except '99' which means using the key supplied in the command.
Private Key length	4 N	Length (in bytes) of the next field (present only if the private key flag is '99').
Private Key	n B	Private Key encrypted using LMK pair 34-35 (present only if the private key flag is '99').
Delimiter	1 A	Delimiter indicates the end of the Private Key field. Value ':'.
Encrypted AN-PIN Length	1 N	Encrypted Alphanumeric PIN length '0': 32 Hex '1': 48 Hex
Stored Alphanumeric PIN	32 H or 48 H	The alphanumeric PIN encrypted under LMK pair 36-37 with Variant 1. (from local storage) Depends on Encrypted AN-PIN Length.
Message Length	4 N	Length of AN-PIN and MAC Message (if Message Type = "10") OR Length of A-N Change PIN and MAC Message (if Message Type = "11").
Message	n A	AN-PIN and MAC Message as received from client (if Message Type = "10") OR

payShield 10K Core Host Commands

Field	Length & Type	Details
		AN Change PIN and MAC Message as received from client (if Message Type = "11").
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ZV'.
Error Code	2 N	<p>'00': No errors. '01': PIN verification failure. '02': MAC Verification Failure. '03': Invalid private key index. '04': Invalid private key flag. '06': Invalid Encryption Identifier. '07': Invalid pad mode identifier. '08': Invalid IV. '13': LMK error; report to supervisor. '14': Error in Stored PIN from Host. '15': Error in input data. '20': Current AN-PIN Block Error. '21': Invalid user storage index. '23': Invalid Encrypted AN-PIN Length '24': PIN Length error. '50': New AN-PIN Block Error. '53': Invalid AN-PIN Block Encryption Mode. '47': DSP error; report to supervisor. '49': Private Key error; report to supervisor. '76': Key block length error. '77': Clear data block error. '78': Private Key length error. '80': Incorrect Message Length '82': Private Key field length error or missing field delimiter '83': Invalid Ver or Type in Message '84': Invalid Ver or Usage in Master Key '85': Invalid Hash Mode or invalid Hash Mode and Encrypted AN-PIN Length combination Or any standard error code </p>
New encrypted AN-PIN	32 H or 48 H	The new alphanumeric PIN encrypted under LMK pair 36-37 with Variant 1. (only present if Message Type is "11")
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

8 HSM Management Commands

8.1 User Storage Commands

The payShield 10K contains 98304 bytes of memory allocated to the storage of keys and tables, indexed from 0 to H'FFF. The CS (Configure Security) console command sets the block size for user storage locations, specifying single, double or triple length keys.

The data can be loaded and read from this storage by the Host. This facility can be used to reload the contents after a power-down, a reset, or after batch solicitation data processing.

In addition, a facility is provided to verify a Diebold table held in user storage.

The payShield 10K HSM provides the following host commands to support user storage operations:

Function	Command	Page
<i>Load Data to User Storage</i>	LA (LB)	486
<i>Read Data from User Storage</i>	LE (LF)	488
<i>Verify the Diebold Table in User Storage</i>	LC (LD)	490

Load Data to User Storage

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Load data to user storage.

Errors: Error 15 is returned if the length of the supplied data does not match the specified data length. (Relevant only where the security setting *User storage key length* has been set to variable length (Variable)).

Error 80 is returned if the length of the supplied data is too long for the specified location. (Relevant only where the security setting *User storage key length* has been set to variable length (Variable)).

Notes: See the *payShield 10K Host Programmer's manual* for a description of the User Storage capability.

Where the security setting *User storage key length* has been set to one of the Fixed Length values (Single=16 characters, Double=32 characters, or Triple=48 characters), this command can load a maximum of 32 blocks of data. If the key length is set to a larger setting than the data to be loaded the data should be padded with 'F's to fill the block.

Where the security setting *User storage key length* has been set to variable length (Variable), a single block of data can be loaded using this command.

Ensure that the location within user storage does not conflict with any Diebold table already loaded.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'LA'.
The following section applies only when User Storage key length = S, D or T		
Index Flag	1 A	Always 'K'.
Index address	3 H	The 3-digit address identifying the first location at which to store the data.
Block count	2 H	The hexadecimal count of the number of blocks of data ('00' to '20' in hex).
Block 1	16 / 32 / 48 H	The first encrypted key or other data.
Block 2	16 / 32 / 48 H	The second encrypted key or other data.
...
Last block	16 / 32 / 48 H	The last encrypted key or other data.
The following section applies only when User Storage key length = V		
Index Flag	1 A	'A' = ASCII 'B' = Binary 'H' or 'K' = Hexadecimal
Index address	3 H	The 3-digit address identifying of the location at which to store the data.
Length of data	4 N	The length of the data to be stored, in bytes. Maximum value = 1,000 for Index addresses up to 07F. Maximum value = 100 for index addresses 080 or greater.
Data	n B or n H or n C	The encrypted key or other data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'LB'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Read Data from User Storage

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Read data from user storage.

Notes: See the *payShield 10K Host Programmer's manual* for a description of the User Storage capability.

Where the security setting *User storage key length* has been set to one of the Fixed Length values (Single=16 characters, Double=32 characters, or Triple=48 characters), this command can return a maximum of 32 blocks of data.

Where the security setting *User storage key length* has been set to variable length (Variable), a single block of data can be returned using this command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'LE'.
Index Flag	1 A	Value 'K'.
Index address	3 H	The 3-digit address identifying the first (or only) location at which to read the data.
Block count	2 H	Must be present if User Storage key length is fixed, i.e. set to <u>Single</u> , <u>Double</u> , or <u>Triple</u> . The hexadecimal count of the number of blocks of data ('00' to '20' in hex). [NOTE: This item is not provided where the User Storage key length is <u>Variable</u> .]
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

payShield 10K Core Host Commands

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'LF'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
The following section applies only when User Storage key length = S, D or T		
Block 1	16 / 32 / 48 H	The first encrypted key or other data.
Block 2	16 / 32 / 48 H	The second encrypted key or other data.
...
Last block	16 / 32 / 48 H	The last encrypted key or other data.
The following section applies only when User Storage key length = V		
Index Flag	1 A	'A' = ASCII 'B' = Binary 'H' or 'K' = Hexadecimal
Length of data	4 N	Total length of data, in bytes.
Data block	n A or n B or n H	The retrieved block of data.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify the Diebold Table in User Storage

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Verify the Diebold table held in user storage.

Notes: The Diebold table must be stored in user storage before using this command.

1. If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", the Diebold table is encrypted using LMK pair 14-15 variant 0.
2. If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y", the Diebold table is encrypted using LMK pair 36-37 variant 6.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'LC'.
Index Flag	1 A	Value 'K'.
Index address	3 H	The address of the start of the Diebold table for validation.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'LD'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

8.2 Miscellaneous Commands

The payShield 10K provides the following host commands to support miscellaneous operations:

Function	Command	Page
<i>Echo Command</i>	B2 (B3)	492
<i>Cancel Authorized Activities</i>	RA (RB)	493
<i>Generate a Key Check Value</i>	BU (BV)	495
<i>Set HSM Response Delay</i>	LG (LH)	498
<i>Translate Decimalization Table from Old to New LMK</i>	LO (LP)	499
<i>Command Chaining</i>	NK (NL)	500
<i>Modify Key Block Header</i>	CS (CT)	502
<i>Generate a Random Value</i>	NO (N1)	504

Echo Command

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Echo received data back to the user.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'B2'.
Length	4 H	Length of the following field in bytes.
Data	n B	Data field to be echoed.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'B3'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
Data	n B	Data field echoed back.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Cancel Authorized Activities

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Cancel the Authorized state.

The behavior of this command depends upon the setting of the "Enable multiple authorized activities" switch of the console command Configure Security.

When multiple authorized activities are **disabled**, this command cancels the "global" Authorized State.

When multiple authorized activities are **enabled**, the Mode Flag parameter may be specified. If the Mode Flag is not present, then this command will cancel all authorized activities. If the Mode Flag is present, then this command behaves as follows:

00 : Cancel all authorized activities

01 : Cancel specified authorized activities

Notes: When canceling an Authorized Activity which includes a timeout, the original (i.e. not current) value of the timeout should be specified.

Only those authorized activities corresponding to the identified LMK are cancelled.

Cancellation of authorizations by using this command always results in an entry in the Audit Log.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RA'.
Mode flag	2 H	Optional. If not present, all Authorised Activities are cancelled. If present, the following values are valid: '00': Cancel all Authorised Activities '01': Cancel the following Authorised Activities '02' ... 'FF': Reserved for future use
Mode '00'		
No additional parameters are required		
Mode '01'		
Number of Authorised Activities	3 N	The number of activities that follow.
Authorised Activity 1	n A	ASCII encoding of an authorised activity to cancel, in the format of: <category>[.<sub-category>][.<interface>][.<timeout>]
Delimiter 1	1 A	Value ';'.
Authorised Activity 2	n A	ASCII encoding of an authorised activity to cancel, in the format of: <category>[.<sub-category>][.<interface>][.<timeout>]
Delimiter 2	1 A	Value ';'.
...
Authorised Activity N	n A	ASCII encoding of an authorised activity to cancel, in the format of: <category>[.<sub-category>][.<interface>][.<timeout>]
Delimiter N	1 A	Value ';'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.

Field	Length & Type	Details
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RB'.
Error Code	2 A	'00': No error '01': Invalid Mode Flag value '02': Multiple Authorised Activities not enabled '03': Specified activity not authorised '68': Command disabled or a standard error code.
Mode '00'		
No fields are returned		
Mode '01'		
Number of Authorised Activities	3 N	The number of authorised activities remaining after the completion of this command.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a Key Check Value

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Variant LMK	Authorization: See text Activity: generate.{keytype}.host
Key Block LMK	Authorization: Not required

Function: Generate a check value for a key encrypted under an LMK pair.

Note: This command examines Key Type Table to determine whether the key type is valid. If the key type is invalid, an error code is returned.

If a valid 2-digit Key Type code is used, then the 3-digit Key Type field should not be present.

For valid key types:

- Generation of a 6-digit key check does not require Authorization.
- Generation of a non-6-digit key check value requires Authorization. If multiple authorized activities are enabled, then as an example, the activity **generate.zpk.host** would need to be enabled in order to successfully generate a 16 digit Key Check Value of a ZPK.

Key Algorithm:	DES keys	AES keys	HMAC keys
Key Check Value Calculation Method	Use the key to perform a 3DES encryption operation on a 8-byte block consisting of all binary zeros. The key check value is the left-most 6-16 digits of the result.	Use the key to perform an AES CMAC operation on a 16-byte block consisting of all binary zeros. The key check value is the left-most 6 digits of the result.	Use the key and corresponding hash algorithm to generate an HMAC of a zero-length message. The key check value is the left-most 6 digits of the result.

When used with a Variant LMK, this command uses the security setting *Restrict Key Check Value to 6 hex chars* to determine the number of valid digits (6 or 16) to return in the *Key Check Value* field, and sets any remaining (leftmost) characters in this field to '0'.

When used with a Key Block LMK, the returned *Key Check Value* field will always contain 6 valid digits; if a 16 digit KCV is requested, the leftmost 10 digits will be set to '0'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'BU'.
2-digit Key Type Code	2 N or 2 H	For a Variant LMK: Indicates the LMK under which the key is encrypted: '00' – '9E': this field indicates a 2-digit Key Type Code (identical to the regular 3-digit Key Type Code but without the middle digit) 'FF': Use 3-digit Key Type Code, specified after Delimiter (below). For a Key Block LMK: This field is reserved, and should be set to 'FF'.
Key Length Flag	1 N or 1 H	For a Variant LMK: '0': for single-length key '1': for double-length key '2': for triple-length key. '3': for HMAC key For a Key Block LMK: This field is reserved, and should be set to 'F'.

Except when using a Variant LMK with Key Type Code = '1C' (HMAC, with Key Length Flag = 3), the fields in the following section apply:

Key	16 / 32 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	The Key for which a Key Check Value is required. For a Variant LMK, the 'Key' is encrypted under the LMK (pair/variant as defined by 'Key Type Code' above). For a Key Block LMK, the 'Key' must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>Any valid value</td><td>Any valid value</td><td>Any valid value</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	Any valid value	Any valid value	Any valid value
Key Usage	Algorithm	Mode of Use						
Any valid value	Any valid value	Any valid value						
Delimiter	1 A	Optional. Value ';'. Only present if the Key Type Code field (above) is 'FF'. If present, the following field must be present.						
3-digit Key Type Code	3 H	For a Variant LMK: This is the 3-digit Key Type Code of the key for which a Key Check Value is required. For a list of Key Type Codes, see Key Type Codes in the <i>payShield 10K Host Programmer's manual</i> . For a Key Block LMK: This field is reserved, and should be set to 'FFF'.						
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.						
Reserved	1 A	Optional. If present must be '0'.						
Reserved	1 A	Optional. If present must be '0'.						
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0': 16 digit KCV (backward compatible mode) '1': 6 digit KCV. Note: Thales Keyblocks will only generate 6-digit check values.						

For a Variant LMK with 2-digit Key Type Code = '1C' (HMAC, with Key Length Flag = 3) the fields in the following section apply. **In all other cases, these fields are not required.**

Hash Identifier	2 N	Identifier of the Hash Algorithm: '01': SHA-1 '05': SHA-224 '06': SHA-256 '07': SHA-384 '08': SHA-512.
HMAC Key Length	4 N	Length (in bytes) of the next field.
HMAC Key	n B	The HMAC Key, used to calculate the HMAC. Note: the key is not prefixed with a key scheme character.
Delimiter	1 A	Value ';'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.

payShield 10K Core Host Commands

Field	Length & Type	Details
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'BV'.
Error Code	2 A	'00': No error '04': Invalid Key Type Code '05': Invalid Key Length Flag '10': Key parity error '68': Command disabled or a standard error code.
Key Check Value	16 or 6 H	The calculated check value of the supplied key. 16 / 6 H depending on chosen Key Check Value option.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Set HSM Response Delay

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: No operation. This command is included only for backward compatibility with host applications developed against earlier Thales payment HSMs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'LG'.
Value	3 N	Value '000' to '255'.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'LH'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate Decimalization Table from Old to New LMK

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Translate an Encrypted Decimalization Table from encryption under an 'old' LMK to encryption under the 'new' LMK. The 'old' or 'new' LMK must have previously been loaded into Key Change Storage.

Notes: This command is provided to simplify the LMK conversion process for issuers or transaction processors who use a large number of decimalization tables.

The use of encrypted decimalization tables is strongly recommended. By default the HSM is configured to expect encrypted decimalization tables in PIN commands that use the IBM offset method. For backward compatibility the HSM may be configured to use plaintext decimalization tables using Configure Security.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'LO'.
Decimalization Table (old LMK)	16 H or 'L' + 32 H	16 H when using a Variant LMK or 3DES Key Block LMK. 'L' + 32 H when using an AES Key Block LMK.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'LP'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
Decimalization Table (new LMK)	16 H or 'L' + 32 H	16 H when using a Variant LMK or 3DES Key Block LMK. 'L' + 32 H when using an AES Key Block LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Command Chaining

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): As per embedded commands	
Authorization: As per embedded commands	

Function: Command Chaining allows multiple commands to be sent as a bundle.

Notes: This command allows the host to bundle up to 99 HSM commands together (called sub-commands), and send them to the HSM in one command message. The HSM will extract the sub-commands, execute them individually (as if sent independently by the host), and bundle up the responses. The HSM will then send the bundled responses back to the host in one response message.

Note: There are limits to the amount of data that the HSM can process.

- The NK command message has a limit of 32,000 bytes.
- Each sub-command has a limit of 9,999 bytes.
- The NL response message has a limit of 11,000 bytes.

If any of these limits are exceeded, the NK command will fail.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'NK'.
Message Header Flag	1 N	'0': Commands don't have message headers. '1': Commands have individual message headers.
Number of commands	2 N	'01' ... '99': Number of commands to follow.
Sub-Command #1		
Length	4 N	Size of remaining fields in this sub-command.
Message Header	m A	Only present if Message Header Flag is '1'.
Command Code	2 A	
Parameters	?	Input parameters, as appropriate to the specified command.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
Sub-Command #2		
Length	4 N	Size of remaining fields in this sub-command.
Message Header	m A	Only present if Message Header Flag is '1'.
Command Code	2 A	
Parameters	?	Input parameters, as appropriate to the specified command.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
...
Sub-Command #N		
Length	4 N	Size of remaining fields in this sub-command.
Message Header	m A	Only present if Message Header Flag is '1'.
Command Code	2 A	
Parameters	?	Input parameters, as appropriate to the specified command.

Field	Length & Type	Details
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'NL'.
Error Code	2 A	'00': No error '51': Invalid message header '52': Invalid Number of Commands field '53': Invalid Length field within sub-command '68': Command disabled or a standard error code.
Number of commands	2 N	Number of commands to follow.
Sub-Command #1		
Length	4 N	Size of remaining fields in this sub-command.
Message Header	m A	Only present if Message Header Flag is '1'.
Response Code	2 A	
Error Code	2 A	Error Codes are appropriate to the specified command.
Parameters	?	Output parameters, as appropriate to the specified command.
Sub-Command #2		
Length	4 N	Size of remaining fields in this sub-command.
Message Header	m A	Only present if Message Header Flag is '1'.
Response Code	2 A	
Error Code	2 A	Error Codes are appropriate to the specified command.
Parameters	?	Output parameters, as appropriate to the specified command.
...
Sub-Command #N		
Length	4 N	Size of remaining fields in this sub-command.
Message Header	m A	Only present if Message Header Flag is '1'.
Response Code	2 A	
Error Code	2 A	Error Codes are appropriate to the specified command.
Parameters	?	Output parameters, as appropriate to the specified command.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Modify Key Block Header

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Optional	
Activity: misc.host	

Function: To modify certain fields in a Thales key block.

Notes: The HSM must be authorized if the Key Status field is to be modified.

Only the changes specified in the following table are possible:

Header field	Old Value	New Value
Exportability	E, S	N
Key Status	P	E, L, R
	L	E, R
Mode of Use	B, N	D, E
Mode of Use	C, N	G, V

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'CS'.
Key	'S' + n A	Key Block whose header is to be modified.
Change Field	1 N	Indicates which field in the key block to change; permitted values: '0': key status block (payShield must be appropriately authorized) '1': mode of use field '2': exportability field.
Old Value	n A	Field value to be modified (must not include a ';' character).
Delimiter	1 A	Value ':'.
New Value	n A	New field value to be included in the key block (must not include a '%' character).
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'CT'.
Error Code	2 A	'00': No error 'B7': Invalid change field 'B8': Invalid old value 'B9': Invalid new value 'BA': No key status block in the key block '68': Command disabled or a standard error code.
Modified Key Block	'S' + n A	Modified key block
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a Random Value

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate a random value up to 256 bytes in length.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'N0'. ('N'-zero)
Random Value Length	3 N	Decimal number in the range '001' to '256'
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'N1'.
Error Code	2 A	'00': No error '01': Invalid Random Value Length or a standard error code.
Random Value	n B	Random Value with length as defined by Random Number Length (maximum of 256 bytes)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

8.3 Diagnostic Commands

The payShield 10K provides the following host commands to support diagnostic operations:

Function	Command	Page
<i>Perform Diagnostics</i>	NC (ND)	506
<i>HSM Status</i>	NO (NP)	507
<i>Return Network Information</i>	NI (NJ)	509
<i>Get HSM Loading</i>	J2 (J3)	512
<i>Get Host Command Volumes</i>	J4 (J5)	513
<i>Reset Utilization Statistics</i>	J6 (J7)	514
<i>Get Health Check Accumulated Counts</i>	J8 (J9)	515
<i>Reset Health Check Accumulated Counts</i>	JI (JJ)	517
<i>Get Instantaneous Health Check Status</i>	JK (JL)	518

Perform Diagnostics

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Test the processor, software and the LMK(s). Return the check value for the identified LMK.

Notes: The check value is the same as the value returned for the Console V command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'NC'.
LMK Type	1 A	Optional. If not present, the value '0' is assumed. '0': Return check value of current LMK. '1': Return check value of LMK in Key Change Storage.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ND'.
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.
LMK check	16 N	The LMK check value. This is the value returned by the Console V command.
Firmware number	9 A	The firmware reference number in the form: xxxx-xxxx.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

HSM Status

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To return HSM status information

Notes: Modes 00 and 01 are available; all others reserved for future use

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'NO'.
Mode flag	2 H	Mode Flag: '00': Return status information '01': Return PCI HSM Compliance status '02' ... 'FF': Reserved for future use
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details	
RESPONSE MESSAGE			
Message Header	m A	Returned to the Host unchanged.	
Response Code	2 A	Value 'NP'.	
Error Code	2 A	'00': No error '68': Command disabled or a standard error code.	
Mode '00'			
I/O buffer size	1 N	I/O buffer size: '0': 2K bytes '1': 8K bytes '2': 16K bytes '3': 32K bytes.	
Ethernet type	1 N	Type of Ethernet connection '0': UDP '1': TCP.	
Number of TCP Sockets	4 N	Number of TCP sockets configured (maximum '0128'). Note: In previous versions of firmware, this field was '2 N'.	
Firmware number	9 A	The firmware reference number in the form: xxxx-xxxx.	
Reserved	1 N	Reserved for future use.	
Reserved	4 A	Reserved for future use.	
Mode '01'			
PCI HSM Compliance	1 N	'0' - Some of the security settings relevant to PCI HSM compliance have non-compliant values. The "Enforce key type 002 separation for PCI HSM compliance" setting is one of these. '1' - all security settings relevant to PCI HSM compliance have compliant values. '2' - Some of the security settings relevant to PCI HSM compliance have non-compliant values. The "Enforce key type 002 separation for PCI HSM compliance" setting is <i>not</i> one of these.	
Reserved	10 A	Reserved for future use.	
Mode '02' ... 'FF' Reserved for future use			
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.	
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.	

Return Network Information

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function:

To return information about the Ethernet Host and Management Ports

The HSM will record details about network activity on both its Management and Host Ethernet ports for diagnostic and security purposes. As a diagnostic aid, it can provide useful information when configuring the unit. If reviewed periodically, it can also provide evidence of unexpected network activity, which may require further investigation.

The HSM collects information about each 'endpoint' that communicates with it. The information recorded will depend on the particular protocol that was used to send the packet.

For TCP packets, the HSM records:

- Local TCP port
- Remote IP address and TCP port
- TCP state (e.g. LISTENING, ESTABLISHED, etc.)
- Timestamp (time when connection was initiated)
- For UDP packets, the HSM records:
- Local UDP port
- Remote IP address and UDP port
- Timestamp (time of most recent UDP packet received from this address)

The HSM console command "NETSTAT" provides the same information at the console.

Notes:

Support for other types of Host connections is not currently provided.

Note that the Ethernet statistics do not map directly to the "netstat -p tcp" output at the console because the Ethernet statistics are upper level protocol ignorant (i.e. tcp, udp) etc. The byte counts for the Ethernet statistics include all Ethernet information (e.g. headers and data) whereas netstat byte counts relate to the upper layer protocol data portion. Note also that the Ethernet receive statistics include all packets "seen" by the Ethernet interface regardless of whether they passed up the stack whereas netstat received statistics only record received packets that are passed up the stack.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'NI'.
Network Interface	1 A	'1': Host Port 1 '2': Host Port 2 'H': Host Port 1 + Host Port 2 'M': Management Port 'X': All ports
Ethernet Statistics	1 N	'0': Do not return Ethernet statistics '1': Return Ethernet statistics.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'NJ'.
Error Code	2 A	'00': No error '01': Failed to execute NETSTAT '68': Command disabled '82': Invalid Ethernet Statistics value or a standard error code.
Number Of Records	4 N	Number of records to follow ('N'). Each record consists of up to 6 fields, as below:
Record #1		
Protocol	1 N	The protocol of the recorded packet. '0': TCP '1': UDP '2' ... '9': Reserved.
Local Port	4 H	The port number at this HSM. Only present if Protocol = '0' or '1' (TCP or UDP).
Remote Address	8 H	The IP address of the remote node, for example: C1F06541 = 193.240.101.65 .
Remote Port	4 H	The port number at the remote IP address. Only present if Protocol = '0' or '1' (TCP or UDP).
State	1 N	The TCP state of the connection. '0': ESTABLISHED '1': CLOSED '2' ... '9': Reserved Only present if Protocol = '0' (TCP).
Duration	8 N	Time (in seconds) since the connection was initiated (for TCP), or since the most recent packet was received from the specified IP address (and port – for UDP).

Field	Length & Type	Details
Record #2		
Protocol	1 N	As above
Local Port	4 H	As above
Remote Address	8 H	As above
Remote Port	4 H	As above
State	1 N	As above
Duration	8 N	As above
....
Record #N		
Protocol	1 N	As above
Local Port	4 H	As above
Remote Address	8 H	As above
Remote Port	4 H	As above
State	1 N	As above
Duration	8 N	As above
Total Bytes Sent	16 H	Number of bytes sent on the specified interface. Only present if Ethernet Statistics is '1'.
Total Bytes Received	16 H	Number of bytes received on the specified interface. Only present if Ethernet Statistics is '1'.
Total Unicast Packets Sent	8 H	Number of non-broadcast packets sent on the specified interface. Only present if Ethernet Statistics is '1'.
Total Unicast Packets Received	8 H	Number of non-broadcast packets received on the specified interface. Only present if Ethernet Statistics is '1'.
Total Non-unicast Packets Sent	8 H	Number of broadcast packets sent on the specified interface. Only present if Ethernet Statistics is '1'.
Total Non-unicast Packets Received	8 H	Number of broadcast packets received on the specified interface. Only present if Ethernet Statistics is '1'.
Total Packets Discarded During Send	8 H	Number of packets discarded during send operations on the specified interface. Only present if Ethernet Statistics is '1'.
Total Packets Discarded During Receive	8 H	Number of packets discarded during receive operations on the specified interface. Only present if Ethernet Statistics is '1'.
Total Errors During Send	8 H	Number of errors detected during send operations on the specified interface. Only present if Ethernet Statistics is '1'.
Total Errors During Receive	8 H	Number of errors detected during receive operations on the specified interface. Only present if Ethernet Statistics is '1'.
Total Unknown Packets	8 H	Number of unknown protocols detected during receive operations on the specified interface. Only present if Ethernet Statistics is '1'.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Get HSM Loading

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To return HSM loading information. The command returns, for a range of HSM percentage loading ranges, how many seconds the HSM loading fell into that range. These statistics are accumulated since the last time the data was reset, excluding any periods for which accumulation was suspended.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'J2'.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'J3'.
Error Code	2 A	'00' No error '01' Failed or a standard error code.
Serial Number	12 A	Serial Number of the HSM returning the data.
Start Date	6 H	Date of last reset. Format YYMMDD
Start Time	6 N	Time of last reset. Format HHMMSS
End Date	6 H	Date recording suspended. Format YYMMDD
End Time	6 N	Date recording suspended. Format HHMMSS
Current Date	6 H	Current Date. Format YYMMDD.
Current Time	6 H	Current Time. Format HHMMSS Note: If current date and time are the same as end date and time, then this indicates that the statistics are still being accumulated.
Seconds	10 N	Number of seconds over which data has been accumulated.
Starting Percentage	3 N	Value between 0-100. Indicates the start of this measurement range
Ending Percentage	3 N	Value between 0-100. Indicates the end of this measurement range.
Number Time Periods	10 N	The number of time periods that utilization was within this percentage range
Delimiter	1 A	The value ','
The above 4 fields repeat until the message ends		
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Get Host Command Volumes

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To return the number of times each host command has been used. These statistics are accumulated since the last time the data was reset, excluding any periods for which accumulation was suspended.

Notes: See the *payShield 10K Programmer's manual* for an overview of payShield Utilization Data capabilities.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'J4'.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'J5'.
Error Code	2 A	'00' No error '01' Failed or a standard error code.
Serial Number	12 A	Serial Number of the HSM returning the data.
Start Date	6 N	Date of last reset. Format YYMMDD.
Start Time	6 N	Time of last reset. Format HHMMSS.
End Date	6 N	Date recording suspended. Format YYMMDD.
End Time	6 N	Date recording suspended. Format HHMMSS.
Current Date	6 N	Current Date. Format YYMMDD.
Current Time	6 N	Current Time. Format HHMMSS. Note: If current date and time are the same as end date and time, then this indicates that the statistics are still being accumulated.
Seconds	10 N	Number of seconds that data has been accumulated.
Command Code	2 A	Command Code
Transactions	12 N	The total number of these commands processed since the last reset The above 2 fields repeat until the message ends
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Reset Utilization Statistics

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To reset to zero the accumulated utilization data counts. These counts are returned using the "Get HSM Loading" and "Get Host Command Volumes" host commands.

Notes: See the *payShield 10K Programmer's manual* for an overview of payShield Utilization Data capabilities..

The Utilization statistics are also reset when new software is installed on the HSM.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'J6'.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'J7'.
Error Code	2 A	'00' No error '01' Failed or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Get Health Check Accumulated Counts

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To return the number of times that various events relating to the health of the HSM have occurred. These statistics are accumulated since the last time the data was reset, excluding any periods for which accumulation was suspended.

Notes: See the *payShield 10K Programmer's manual* for an overview of payShield Health Check Data capabilities.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'J8'.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'J9'.
Error Code	2 A	'00' No error '01' Failed or a standard error code.
Serial Number	12 A	Serial Number of the HSM returning the data.
Start Date	6 N	Date of last reset. Format YYMMDD.
Start Time	6 N	Time of last reset. Format HHMMSS.
End Date	6 N	Date recording suspended. Format YYMMDD.
End Time	6 N	Date recording suspended. Format HHMMSS.
Current Date	6 N	Current Date. Format YYMMDD.
Current Time	6 N	Current Time. Format HHMMSS. Note: If current date and time are the same as end date and time, then this indicates that the statistics are still being accumulated.
Reboots	10 N	The number of times the unit has rebooted since last reset of data.
Tampers	10 N	The number of times the unit has tampered since last reset of data
Pin verifies/minute	7 N	The number of times the PIN verifications/minute have been exceeded since last reset of data.
Pin verifies/hour	5 N	The number of times the PIN verifications/hour have been exceeded since last reset of data.
PIN attacks	8 N	The total number of PIN attacks since last reset of data
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Reset Health Check Accumulated Counts

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To reset to zero the accumulated health check data counts. These counts are returned using the "Get Health Check Accumulated Counts" host commands.

Notes: The accumulated counts are also reset when new software is installed on the HSM.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'JI'.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'JJ'.
Error Code	2 A	'00' No error '01' Failed or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Get Instantaneous Health Check Status

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To return the current status of various health-related items.

Notes: Health Check Data capabilities.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'JK'.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

payShield 10K Core Host Commands

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'JL'.
Error Code	2 A	'00' No error '01' Failed or a standard error code.
Serial Number	12 A	Serial Number of the HSM returning the data.
System Date	6 N	Current date. Format YYMMDD
System Time	6 N	Current date. Format HHMMSS
Console State	1 N	Whether the service to process console commands is running. 0 – unknown 1 – running 2 – not running 3 – console disabled by GUI
payShield Manager state	1 N	Whether the service to process payShield Manager messages is running. 0 – unknown 1 – running 2 – not running
Ethernet Host link 1 state	1 N	Whether the Ethernet host port 1 is running. 0 – unknown 1 – running 2 – not running 3 – not configured
Ethernet Host link 2 state	1 N	Whether the Ethernet host port 2 is running. 0 – unknown 1 – running 2 – not running 3 – not configured
Reserved	1 N	0 – RFU
FICON link state	1 N	Whether the FICON link is running. 0 – unknown 1 – running 2 – not running 3 – not configured
Tamper state	1 N	Whether the HSM is in a tamper state or not. 0 – unknown 1 – no tamper 2 – tamper

Field	Length & Type	Details
Note: this section is only present if Tamper State = 2		
Tamper cause	2 N	Cause of the tamper event: 0 = unknown 1 = temp out of range 2 = battery low 3 = erase button pressed 4 = security processor watchdog 5 = power too high 6 = security processor restart 7 = motion detected 8 = case tampered 9 = TSPP Module 10 = General
Tamper Date	6 N	Date of tamper. Format YYMMDD
Tamper Time	6 N	Time of tamper. Format HHMMSS
Number LMKs loaded	2 N	Total number of LMKs loaded
Number Test LMKs loaded	2 N	Number of LMKs that are designated test
Number Old LMKs loaded	2 N	Total number of LMKs loaded in key change storage
LMK id	2 N	ID of loaded LMK
Authorized	1 N	Indicates whether or not the LMK is authorized. 0 = Not authorized 1 = Authorized
Num Auth Activities	2 N	If authorized, the number of authorized activities.
Scheme	1 A	'V' variant, 'K' key block
Algorithm	1 N	The algorithm used by the LMK: 0 = 3DES2Key, 1 = 3DES3Key 2 = AES 256-bit
Status	1 A	'L' live, 'T' test
Comments	0...40 A	Variable length comment string
Delimiter	1 A	The value 'X'14'
The above 8 fields repeated for each LMK		
End LMK List Delimiter	1 A	Marks end of LMK list. Value X'15.
Fraud detection exceeded	1 N	Indicates whether the configured number of PIN verifies/minute or PIN verifies/hour have been exceeded: 0 = not exceeded (or not enabled) 1 = exceeded.
PIN attacks exceeded	1 N	Indicates whether the PIN Attack limit has been exceeded, such that the LMK has been deleted: 0 = not exceeded (or not enabled) 1 = exceeded.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

8.4 Auditing Commands

The payShield 10K provides the following host commands to support audit operations:

Function	Command	Page
<i>Translate Audit Record MAC key</i>	Q0 (Q1)	522
<i>Retrieve Audit Record</i>	Q2 (Q3)	523
<i>Archive (Print) Audit Record</i>	Q4 (Q5)	524
<i>Delete Audit Record</i>	Q6 (Q7)	525
<i>Audit Record Verification</i>	Q8 (Q9)	526

Translate Audit Record MAC key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To translate an audit MAC key from the old LMK to the new LMK.

Notes: The random MAC key used to generate the MAC on the audit record must be translated from the old LMK to the new LMK when the LMK is changed.

This command uses the Management LMK and so it is not necessary to specify the LMK Identifier in the command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Q0'.
MAC key	'U' + 32 H	The MAC key to be translated. For an old Variant LMK, the 'MAC Key' must be encrypted under LMK pair 22-23 variant 7.
	'S' + 32 H	For an old Key Block LMK, the 'MAC Key' must be encrypted under the old LMK.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'Q1'.
Error Code	2 A	'00': No error '10': MAC key parity error '68': Command disabled or a standard error code.
MAC key	'U' + 32 H	The translated MAC Key, encrypted under the current LMK. For a Variant LMK, the translated 'MAC Key' will be encrypted under current LMK pair 22-23 variant 7.
	'S' + 32 H	For a Key Block LMK, the translated 'MAC Key' will be encrypted under the current LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Retrieve Audit Record

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: This command allows a single audit record to be returned to the host system.

Notes: This command cannot be added to the list of commands to be audited. The record returned is the next record in the audit buffer that does not have its 'retrieved' bit set to 1. The data returned includes the audit counter, the timestamp, the MAC, and the MAC key.

This command uses the Management LMK and so it is not necessary to specify the LMK Identifier in the command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Q2'.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'Q3'.
Error Code	2 A	'00': No error '35': No Audit Records found '36': All Audit Records have been retrieved '68': Command disabled or a standard error code.
Audit Record	80 H	The retrieved audit record. See 'Audit Record Format' in the <i>payShield 10K Installation and User Guide</i> manual.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Archive (Print) Audit Record

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To archive records from the HSM Audit Trail buffer onto a printer.

Notes: This command cannot be added to the list of commands to be audited. Starting at the oldest audit record in the HSM it allows between one and 2000 (50,000 from software v1.4a) audit records to be archived by outputting the record in a fixed format to the printer. When an audit record has been archived, it has its 'archived' flag set to 1.

This command uses the Management LMK and so it is not necessary to specify the LMK Identifier in the command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Q4'.
Audit Mode Flag	1 N	Audit Mode, where: '0': Archive the next 'un-archived' record '1': Archive all 'un-archived' records '2': Archive all records.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'Q5'.
Error Code	2 A	'00': No error '35': No Audit Records found '36': All Audit Records already archived '37': Invalid audit mode '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Delete Audit Record

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Required	
Activity: audit.host	

Function: To delete audit records from the HSM Audit Trail buffer.

Notes: This command cannot be added to the list of commands to be audited. Starting at the oldest audit record in the HSM it allows between one and 2000 audit records to be deleted. Only audit records that have been archived, and had their archived flag set to 1, can be deleted.

This command uses the Management LMK and so it is not necessary to specify the LMK Identifier in the command. The authorized activity 'audit.host' must be authorized using the Management LMK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Q6'.
Audit Delete Mode	1 N	Delete mode, as follows: '0': delete retrieved records '1': delete archived records.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'Q7'.
Error Code	2 A	'00': No error '35': No Audit Records found '36': No matching audit records found '68': Command disabled or a standard error code.
Deleted Count	4 N	'0001' ... '2000': Number of audit records deleted.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Audit Record Verification

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To verify a previously extracted audit record.

Notes: This command cannot be added to the list of commands to be audited.

This command verifies the MAC on an audit record using the MAC key sent along with the data.

This command uses the Management LMK and so it is not necessary to specify the LMK Identifier in the command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Q8'.
Audit Record	80 H	The audit record to be verified. See 'Audit Record Format' in the <i>payShield 10K Installation and User Guide</i> manual.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'Q9'.
Error Code	2 A	'00': No error - MAC on audit record verified OK '01': MAC verification failure '10': Parity error on MAC key '68': Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

9 EMV Transaction Processing Commands

9.1 EMV Chip Card Commands

This section describes the payShield 10K functions which are needed to support on-line transaction processing for the various payment schemes under the EMV umbrella. Whilst EMV specifies most of the details pertaining to cards and terminals, the individual schemes have defined their own cryptographic processes for on-line authorization functions.

Key Naming Conventions

The various schemes have adopted different naming conventions for the keys used. For consistency the following convention is used:

Key Description	Name used in this specification	Name used by Visa	Name used by Mastercard
Master Key for Authentication Cryptograms	MK-AC	DMK	Issuer MK
Master Key for Secure Messaging Integrity	MK-SMI	DMK	Issuer MK
Master Key for Secure Messaging Confidentiality	MK-SMC	DMK	Issuer MK
Master Key for Data Authentication Codes	MK-DAC	-	Issuer MK
Master Key for Dynamic Numbers	MK-DN	-	Issuer MK
Derived Key for Authentication Cryptograms	DK-AC	UDK	ICC MK
Derived Key for Secure Messaging Integrity	DK-SMI	UDK	ICC MK
Derived Key for Secure Messaging Confidentiality	DK-SMC	UDK	ICC MK
Derived Key for Dynamic Numbers	DK-DN	-	ICC MK

The payShield 10K provides the following host commands to support EMV chip card operations:

Function	Command	Page
ARQC Verification and/or ARPC Generation (Using Static or Mastercard Proprietary SKD Method)	KQ (KR)	528
ARQC Verification and/or ARPC Generation (Using EMV or Cloud-Based SKD Methods)	KW (KX)	533
ARQC Generation	K4 (K5)	531
Generate Secure Message (EMV 3.1.1)	KU (KV)	537
Generate Secure Message (EMV 4.x)	KY (KZ)	542
Verify Truncated Application Cryptogram (Mastercard CAP)	K2 (K3)	547
Data Authentication Code and Dynamic Number Verification (EMV 3.1.1)	KS (KT)	550
Decrypt Encrypted Counters (EMV 4.x)	K0 (K1)	552

ARQC Verification and/or ARPC Generation (Using Static or Mastercard Proprietary SKD Method)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Optional (see text)	
Activity: diag.host	

Function: Validate an ARQC (or TC/AAC) and, optionally, generate an ARPC. Alternatively, the command can be used to generate an ARPC alone. This function is a general purpose command which will validate an ARQC, TC or AAC.

Notes: Diagnostic data is produced by this command only if the HSM is in Authorized State.

This command supports the following cryptogram methods:

Application	Scheme ID
Visa VIS (CVN 10 or 17)	'0'
Mastercard M/Chip (CVN 10 or 11)	'1'
American Express AEIPS (CVN 01 or 02)	'2'

It is the responsibility of the host system to add any scheme specific padding data to the end of the supplied data prior to submission to the HSM. For some schemes this means appending a byte containing hex 80 to the end of the data. If the data supplied by the host is a multiple of 8 bytes, this command adds no further padding data.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'KQ'.						
Mode Flag	1 N	Mode of operation: '0': Perform ARQC Verification only. '1': Perform ARQC Verification and ARPC Generation. '2': Perform ARPC Generation only. '3': Perform ARQC Verification and Discretionary Data MAC Verification. (This mode requires Scheme ID = '0'.) '4': Perform ARQC Verification and Discretionary Data MAC Verification and ARPC Generation. (This mode requires Scheme ID = '0').						
Scheme ID	1 N	Specifies the Key Derivation Methods to use: '0': EMV Option 'A' ICC Master Key Derivation (Visa VIS) '1': EMV Option 'A' ICC Master Key Derivation and Mastercard Proprietary Session Key Derivation (Mastercard M/Chip) '2': EMV Option 'A' ICC Master Key Derivation (American Express AEIPS).						
MK-AC	32 H or 'U' + 32 H or 'S' + n A	The Issuer Master Key for generating and verifying Application Cryptograms. For a Variant LMK, the 'MK-AC' must be encrypted under LMK pair 28-29 variant 1. For a Key Block LMK, the 'MK-AC' must comply with the following:						
	<table border="1"> <tr> <th style="background-color: #d9eaf7;">Key Usage</th> <th style="background-color: #d9eaf7;">Algorithm</th> <th style="background-color: #d9eaf7;">Mode of Use</th> </tr> <tr> <td style="background-color: #d9eaf7;">'E0'</td> <td style="background-color: #d9eaf7;">T'</td> <td style="background-color: #d9eaf7;">'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'E0'	T'	'X', 'N'	
Key Usage	Algorithm	Mode of Use						
'E0'	T'	'X', 'N'						

Field	Length & Type	Details						
MK-SMI	32 H or 'U' + 32 H or 'S' + n A	The Issuer Master Key for Secure Message with Integrity. Only present if Mode = '3' or '4', and Scheme ID is '0'. For a Variant LMK, the 'MK-SMI' must be encrypted under LMK pair 28-29 variant 2. For a Key Block LMK, the 'MK-SMI' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'E2'</td> <td>'T'</td> <td>'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'E2'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E2'	'T'	'X', 'N'						
PAN/PAN Sequence No	8 B	Pre-formatted PAN/PAN Sequence No.						
ATC	2 B	Application Transaction Counter. Present for all modes. A two byte value must be supplied.						
UN	4 B	Unpredictable Number. Present for all modes. A four byte value must be supplied, though it is not used if Scheme ID is '0'.						
Transaction Data Length	2 H	Length of next field. Can be any length from 1 to 255 bytes. Only present if Mode is '0', '1', '3' or '4'.						
Transaction Data	n B	Variable length data. Only present if Mode is '0', '1', '3' or '4'. If the data supplied is a multiple of 8 bytes, no extra padding is added. If it is not a multiple of 8 bytes additional zero padding is added.						
Delimiter	1 A	Delimiter, to indicate end of Transaction Data, value ';'. Only present if Mode is '0', '1', '3' or '4'.						
ARQC/TC/AAC	8 B	ARQC/TC/AAC to be validated and/or used for ARPC generation.						
ARC	2 B	Authorisation Response Code to be used for ARPC Generation. Only present if Mode is '1', '2' or '4'.						
Discretionary Data MAC	4 B	Discretionary Data MAC returned by the card. Only present if Mode is '3' or '4' and Scheme ID = '0'.						
Discretionary Data Length	2 N	Length of the following field (e.g. '08' or '16'). Only present if Mode is '3' or '4' and Scheme ID = '0'.						
Discretionary Data	n B	Discretionary Data over which the MAC was generated. Only present if Mode is '3' or '4' and Scheme ID = '0'.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'KR'.
Error Code	2 A	<p>'00': No error '01': Warning: ARQC/TC/AAC verification failed '03': Mode = 3 or 4 but Scheme ID ≠ 0 '04': Invalid Mode value '05': Unrecognized Scheme ID '06': Warning: Discretionary MAC verification failed '10': MK-AC parity error '11': MK-SMI parity error '68': Command disabled '80': Transaction Data length error '81': Zero length Transaction Data '82': Invalid Discretionary MAC Data length or a standard error code.</p>
ARPC	8 B	The calculated ARPC. Only returned if Mode is '1', '2' or '4' and if no error is encountered.
Diagnostic data	8 B	Calculated ARQC/TC/AAC. Only returned if the error code is '01' and the HSM is in Authorised State.
Diagnostic MAC data	8 B	Calculated Discretionary Data MAC. Only returned if Mode is 3 or 4, the error code is '06', and the HSM is in Authorized State.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

ARQC Generation

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: None	

Function: To generate an ARQC.

Notes: This command performs a similar function to the KW command, but generates the ARQC rather than validating it. ARQCs generated by this command can be successfully validated using the KW command.

This command supports the following cryptogram methods:

Application	Scheme ID
Visa VIS (CVN 18 or '22')	'2' or '3'
Mastercard M/Chip (CVN 14 or 15) (EMV CSK)	'2'
Indonesian National Standard Chip Card Specification (NSICCS)	'2'
EMV Option 'C' Card Key Generation and EMV CSK	'9'
JCB (CVN 04)	'2'
RuPay (CVN 05 or 06)	'2'

It is the responsibility of the host system to add any scheme specific padding data to the end of the supplied data prior to submission to the HSM. For some schemes this means appending a byte containing hex 80 to the end of the data. If the data supplied by the host is a multiple of 8 bytes, this command adds no further padding data.

Field	Length & Type	Details												
COMMAND MESSAGE														
Message Header	m A	Subsequently returned to the Host unchanged.												
Command Code	2 A	Value 'K4'.												
Mode Flag	1 H	Mode of operation: '0': Generate ARQC.												
Scheme ID	1 A	Specifies the Key Derivation Methods to use: '2': EMV Option 'A' Card Key Derivation and EMV Common Session Key Derivation '3': EMV Option 'B' Card Key Derivation and EMV Common Session Key Derivation '9': EMV Option 'C' Card Key Derivation and EMV Common Session Key Derivation												
MK-AC	'S' + n A	The Issuer Master Key for generating Application Cryptograms. The 'MK-AC' must comply with the following:												
		<table border="1"> <thead> <tr> <th>Scheme ID</th> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'2' or '3'</td> <td>'E0'</td> <td>'T'</td> <td>'N', 'X'</td> </tr> <tr> <td>'9'</td> <td>'E0'</td> <td>'A'</td> <td>'N', 'X'</td> </tr> </tbody> </table>	Scheme ID	Key Usage	Algorithm	Mode of Use	'2' or '3'	'E0'	'T'	'N', 'X'	'9'	'E0'	'A'	'N', 'X'
Scheme ID	Key Usage	Algorithm	Mode of Use											
'2' or '3'	'E0'	'T'	'N', 'X'											
'9'	'E0'	'A'	'N', 'X'											
PAN Length	2 N	Only present for Scheme ID = '3' or '9'. Length in bytes of PAN/PAN Sequence Number field. Valid values '08' to '99'.												

Field	Length & Type	Details
PAN/PAN Sequence No	8 B or n B	The Primary Account Number & Sequence Number used in this transaction. It is the responsibility of the host system to ensure that the PAN/PAN Sequence Number is appropriately padded. For Scheme ID = '2', this field will be fixed at 8 bytes, and should contain the pre-formatted PAN/PAN Sequence No. For Scheme ID = '3' or '9', the field length is specified by the "PAN Length" field.
Delimiter	1 A	Only present for Scheme ID = '3' or '9'. Delimiter, to indicate end of PAN/PAN Sequence No, value ':'.
Application Transaction Counter	2 B	The ATC from the card. This is used for Session Key Generation.
Transaction Data Length	2 H	Length of next field. Can be any length from 1 to 255 bytes.
Transaction Data	n B	Variable length data. For all Scheme IDs except '9', if the data supplied is a multiple of 8 bytes, no extra padding is added. If it is not a multiple of 8 bytes, additional zero padding is added. For Scheme ID = '9', no padding is required.
Delimiter	1 A	Delimiter, to indicate end of Transaction Data, value ':'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'K5'.
Error Code	2 A	'00': No error '03': Invalid Padding Flag '04': Unrecognized Mode Flag '05': Unrecognized Scheme ID '10': MK parity error '68': Command disabled 'F1': Invalid key derivation method 'F2': Invalid ARQC validation method 'F3': MK-AC key block algorithm is not AES 'F5': Invalid session key method or a standard error code.
ARQC	8 B	Only present if Mode Flag = '0'. The calculated ARQC.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

ARQC Verification and/or ARPC Generation (Using EMV or Cloud-Based SKD Methods)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Optional (see text)	
Activity: diag.host	

Function: To validate an ARQC (or TC/AAC) and, optionally, to generate an ARPC. Alternatively, the command can be used to generate an ARPC alone. This function is a general purpose command which will validate an ARQC, TC or AAC.

Notes: Diagnostic data is produced by this command if the HSM is in Authorized State. The diagnostic data consists of a generated ARQC, which is returned to the host if verification of the supplied ARQC fails.

This command performs a similar function to the KQ command, but uses the EMV2000 method or EMV Common Session Key Derivation method for generating the session key.

This command supports the following cryptogram methods:

Application	Scheme ID	MK-AC
Visa VIS (CVN 14)	'0'	112-bit 3DES
Visa VIS (CVN 18 or '22')	'2' or '3'	112-bit 3DES
Visa VCP (CVN '43')	'4'	112-bit 3DES or 128-bit AES or 256-bit AES
Visa VCP QR Code (CVN 44)	'8'	112-bit 3DES
Visa VIS (CVN 16 or 26 or 46 or 47)	'9'	128-bit AES or 256-bit AES
Mastercard M/Chip (CVN 12 or 13) (EMV 2000)	'0'	112-bit 3DES
Mastercard M/Chip (CVN 14 or 15) (EMV CSK)	'2'	112-bit 3DES
Mastercard MCBP	'5'	112-bit 3DES
American Express (CVN 05, 07 and MPVV)	'6'	112-bit 3DES
Discover D-PAS (05 or 06)	'2'	112-bit 3DES
Indonesian National Standard Chip Card Specification (NSICCS)	'2'	112-bit 3DES
Interac (Canada)	'D'	112-bit 3DES
Discover HCE	'7'	112-bit 3DES
EMV Option 'C' Card Key Generation and EMV CSK	'9'	128-bit AES or 256-bit AES
JCB (CVN 01)	'A'	112-bit 3DES
JCB (CVN 02)	'B'	112-bit 3DES
JCB (CVN 04)	'2'	112-bit 3DES
Union Pay (Vers 4.2)	'C'	112-bit 3DES
RuPay (CVN 05 or 06)	'2'	112-bit 3DES

It is the responsibility of the host system to add any scheme specific padding data to the end of the supplied data prior to submission to the HSM. For some schemes this means appending a byte containing hex 80 to the end of the data. If the data supplied by the host is a multiple of 8 bytes, this command adds no further padding data.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'KW'.						
Mode Flag	1 H	<p>Mode of operation:</p> <ul style="list-style-type: none"> '0': Perform ARQC verification only '1': Perform ARQC verification and EMV 4.x Method 1 ARPC generation '2': Perform EMV 4.x method 1 ARPC generation only '3': Perform ARQC verification and EMV 4.x Method 2 ARPC Generation '4': Perform EMV 4.x Method 2 ARPC generation only '5': Perform ARQC verification and D-PAS Method 1 ARPC generation '6': Perform D-PAS Method 1 ARPC generation only '7': Perform American Express MPVV verification only '8': Perform Interac ARQC verification only '9': Perform Interac ARQC verification and ARPC generation 						
Scheme ID	1 A	<p>Specifies the Key Derivation Methods to use:</p> <ul style="list-style-type: none"> '0': EMV Option 'A' Card Key Derivation and EMV2000 Session Key Derivation '1': EMV Option 'B' Card Key Derivation and EMV2000 Session Key Derivation '2': EMV Option 'A' Card Key Derivation and EMV Common Session Key Derivation (also used by Indonesian National Standard Chip Card Specification (NSICCS) and JCB (CVN 04) and RuPay (CVN 05 and 06)) '3': EMV Option 'B' Card Key Derivation and EMV Common Session Key Derivation '4': Visa Cloud-Based Payments using EMV Option 'A' Card Key Derivation (when using a 3DES MK-AC) or EMV Option 'C' Card Key Derivation (when using an AES MK-AC) and Limited Use Key (only valid if Mode Flag = '0') '5': Mastercard Cloud-Based Payments using EMV Option 'A' Card Key Derivation and EMV Common Session Key Derivation (only valid if Mode Flag = '0', '1' or '3') '6': American Express Cloud-Based Payments (only valid if Mode Flag = '0' or '7') '7': Discover OTPK (only valid if Mode Flag = '0') '8': Visa Cloud-Based Payments, QR Code, using EMV Option 'A' Card Key Derivation and Limited Use Key (only valid if Mode Flag = 0) '9': EMV Option 'C' Card Key Derivation and EMV Common Session Key Derivation. (Only valid if Mode Flag = '0', '1', '2', '3' or '4') 'A': JCB (CVN 01): EMV Option 'A' Card Key Derivation and no Session Key Derivation 'B': JCB (CVN 02): EMV Option 'A' Card Key Derivation and JCB Session Key Derivation 'C': Union Pay (Vers 4.2): EMV Option 'A' Card Key Derivation and Union Pay Session Key Derivation. (Only valid if Mode Flag = '0', '1' or '2'.) 'D': Interac EMV Option 'A' and Interac Session Key method <p>The Issuer Master Key for generating and verifying Application Cryptograms (or MPVV if Mode Flag = '7').</p>						
MK-AC	32 H or 'U' + 32 H or 'S' + n A	<p>For a Variant LMK, the 'MK-AC' must be encrypted under LMK pair 28-29 variant 1.</p> <p>For a Key Block LMK, the 'MK-AC' must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'E0'</td> <td>'T', 'A'</td> <td>'X', 'N'</td> </tr> </tbody> </table> <p>Note: For EMV schemes, the MK-AC must be either 112-bit 3DES, 128-bit AES or 256-bit AES.</p>	Key Usage	Algorithm	Mode of Use	'E0'	'T', 'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E0'	'T', 'A'	'X', 'N'						
IV-AC	16 B	Only present for Scheme ID = '0' or '1'. IV for EMV 2000 Session key derivation						
PAN Length	2 N	Only present for Scheme ID = '1', '3', '6', '7' or '9'. Length in bytes of PAN/PAN Sequence Number field. Valid values '08' to '99'.						
PAN/PAN Sequence No	8 B or n B	<p>For Scheme ID = '0', '2', '4', '5', '8', 'A', 'B' or 'C', this field will be fixed at 8 bytes, and should contain the pre-formatted PAN/PAN Sequence No.</p> <p>For Scheme ID = '1', '3', '6', '7' or '9', the field length is specified by the "PAN Length" field.</p> <p>It is the responsibility of the host system to ensure that the PAN/PAN Sequence Number is appropriately padded.</p>						
Delimiter	1 A	Only present for Scheme ID = '1', '3', '6', '7' or '9'. Delimiter, to indicate end of PAN/PAN Sequence No, value ':'.						

Field	Length & Type	Details
Branch/Height parameters	1 N	Only present for Scheme ID = '0' or '1'. '0': Branch factor 2; Tree Height 16 '1': Branch factor 4; Tree Height 8
Application Transaction Counter	2 B	Only present for Scheme ID = '0', '1', '2', '3', '5', '6', '7', '9', 'B' or 'C'. The ATC from the card. This is used for Session Key Generation. For truncated ARQC this will be the last ATC from the host database
Padding Flag	1 N	Only present if Mode Flag= '0' or '1', and Scheme ID = 'C'. Padding flag to indicate if padding is applied to Transaction Data. '0': Input Transaction Data is not padded '1': Input Transaction Data is padded.
YHHHHCC	7 N	Only present for Scheme ID = '4' or '8'. The Year/Hour/Counter value used to derive the Limited Use Key (LUK) that produced the ARQC. Y (0-9) : Least significant digit of current year HHHH (0001-8784) number of hours since Jan 1 st CC (00-99) : counter
UDK Key Derivation Method	1 A	Only present for Scheme ID = '6'. 'A': EMV Option 'A' 'B': EMV Option 'B'
Session Key Method	1 N	Only present for Scheme ID = '6'. '1': EMV Common Session Key Derivation
ARQC Validation Method	2 N	Only present for Scheme ID = '6'. '01': ISO 9797-1 Algorithm 1 3DES CBC IV=0 Pad Mode 2 '03': ISO 9791-1 Algorithm 3 3DES CBC Retail MAC
OTPK Key Derivation Method	1 A	Only present for Scheme ID = '7'. '0': Default EMV or Server PIN based white box using MK-AC, EMV 4.3 option A, EMV CSK. '1': Local CVM using MK-AC, EMV 4.3 option A, EMV CSK, and further CSK using CVD.
CVD	3 B	Only present for Scheme ID = '7' and OTPK Key Derivation Method = '1'. Card Verification Data.
Transaction Data Length	2 H	Only present for Mode Flag = '0', '1', '3', '5', '8' or '9'. Length of next field. Can be any length from 1 to 255 bytes.
Transaction Data	n B	Only present for Mode Flag = '0', '1', '3', '5', '8' or '9'. Variable length data. For Mode Flag = '0', '1', '3' and '5': <ul style="list-style-type: none">• For all Scheme IDs except '9', if the data supplied is a multiple of 8 bytes, no extra padding is added. If it is not a multiple of 8 bytes, additional zero padding is added.• For Scheme ID = '9', no padding is required. For Mode Flag = '8' or '9': <ul style="list-style-type: none">• Padding is applied automatically by this host command. Note: If alternative padding methods are required, it is the responsibility of the host to provide this.
Delimiter	1 A	Only present for Mode Flag = '0', '1', '3', '5', '8' or '9'. Delimiter, to indicate end of Transaction Data, value ':'.
ARQC Mask	8 B	Only present for Scheme ID = '5' or '6'. The mask allows partial ARQC or MPVV values less than 8 bytes to be validated. For example, a mask 0xFFFFFFFF00000000 will compare the first (left-most) 4 bytes of the ARQC.
ARQC/TC/AAC or MPVV	8 B	ARQC/TC/AAC or MPVV to be validated and/or used for ARPC generation. For partial ARQC or MPVV values, 0x00 padding is used to pad to 8 bytes.
ARC	2 B	Only present for Mode Flag = '1', '2' or '9'. Authorisation Response Code. Used in ARPC generation for VIS 1.x, M/Chip 4.x and Interac cards.
CSU	4 B	Only present for Mode Flag = '3', '4', '5' or '6'. Card Status Update. Used to create ARPC for Common Core Definitions (CCD) cards. For D-PAS (Mode Flag = '5' or '6'), the CSU is a 2-byte value and must be right-padded with '0's.
UN	4 B	Only present for Mode Flag = '8' or '9'. The 4-byte Unpredictable Number.

payShield 10K Core Host Commands

Field	Length & Type	Details
Proprietary Authentication Data Length	1 N	Only present for Mode Flag = '3' or '4'. Specifies length of Proprietary Authentication Data field. Valid values '0' ... '8'.
Proprietary Authentication Data	0 ... 8 B	Only present if Proprietary Authentication Data Length field is present, and is non-zero. Contains optional issuer data for transmission to the card in the Issuer Authentication Data of an online transaction.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'KX'.
Error Code	2 A	'00': No error '01': Warning: ARQC/TC/AAC/MPVV verification failure '03': Invalid Padding Flag '04': Unrecognized Mode Flag '05': Unrecognized Scheme ID '06': Invalid YHHHHCC value '10': MK parity error '52': Invalid Branch/Height '68': Command disabled 'F1': Invalid key derivation method 'F2': Invalid ARQC validation method 'F3': MK-AC key block algorithm is not AES 'F5': Invalid session key method 'F8': Invalid OTPK Key Generation Method or a standard error code.
ARPC	8 B	Only present for Modes '1', '2', '3', '4', '5', '6' and '9' if no error is encountered. The calculated ARPC. For Modes '3' and '4', this field consists of the 4-byte calculated ARPC followed by the 4-byte CSU.
Diagnostic data	8 B	Calculated ARQC/TC/AAC/MPVV returned only if the error code is '01' and the HSM is in Authorized State.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Secure Message (EMV 3.1.1)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate a Secure Message with Integrity over data to be sent from the Issuer back to the Card. Optionally, Secure Messaging with Confidentiality is provided in which case the message data must be supplied encrypted under a Transport Key. In this latter case the command first decrypts the message data using the Transport Key before re-encrypting it using a Session Key.

Notes: This command is also used to change or unblock a PIN.

To change the PIN held by an EMV card, the issuer has to validate the existing PIN, and then accept a new PIN in a standard PIN block format. This PIN block is then translated from a standard ATM PIN block format (encrypted under a terminal or zone key) to an application specific PIN block format (encrypted under a confidentiality session key).

To generate a PIN unblock script, use "Mode 0" (integrity only), with an EMV PIN Unblock APDU supplied in the "Plaintext Message Data" field.

This command supports the following cryptogram methods:

Application	Scheme ID
Visa VIS (CVN 10)	'0'
Mastercard M/Chip (CVN 10 or 11)	'1'
American Express AEIPS (CVN 01)	'2'
JCB (CVN 01)	'3'
JCB (CVN 02)	'4'
JCB (CVN 04)	'5'
Union Pay (ver 4.2)	'6'

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'KU'.						
Mode Flag	1 N	'0': Provide only Integrity functionality '1': Provide Integrity and Confidentiality using the same Issuer Master Key '2': Provide Integrity and Confidentiality using different Master Keys '3': Provide Integrity and PIN Block translation for PIN Change, using the same Issuer Master Key '4': Provide Integrity and PIN Block translation for PIN Change, using different Issuer Master Keys.						
Scheme ID	1 N	Identifier for the Scheme: '0': Visa VIS '1': Mastercard M/Chip '2': American Express AEIPS '3': JCB (CVN 01). EMV Option 'A' ICC Master Key Derivation with no session key generation '4': JCB (CVN 02). EMV Option 'A' ICC Master Key Derivation and JCB session key derivation '5': JCB (CVN 04). EMV Option 'A' ICC Master Key Derivation with EMV 4.x Common Session Key Derivation '6': Union Pay. EMV Option A ICC Master key derivation and Union Pay session key derivation. Note: If Scheme ID = '3', '4' or '5' are only permitted when Mode Flag = '0', '1' or '2'. The Master Key for Secure Messaging with Integrity, used to generate a MAC on the message.						
MK-SMI	32 H or 'U' + 32 H or 'S' + n A	For a Variant LMK, the 'MK-SMI' must be encrypted under LMK pair 28-29 variant 2. For a Key Block LMK, the 'MK-SMI' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'E2'</td> <td>'T'</td> <td>'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'E2'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E2'	'T'	'X', 'N'						
PAN/PAN Sequence No	8 B	If Scheme ID is '0', '1', '2', '3', '4', '5' or '6', the following field will be present Pre-formatted PAN/PAN Sequence number.						
Integrity Session Key Data	8 B	If Scheme ID is '0', '1', '2', '3', '4', '5' or '6', the following field will be present Used for Integrity Session Key Generation: For Scheme ID = '0' or '2', (Visa/UKIS, AEIPS) this will be the 2 byte ATC right justified and padded on the left with 6 zero bytes. For Scheme ID = '1', this is an 8 byte random number, RANDi. For Scheme ID = '5', this is the Application Cryptogram returned by the card in response to the first GENERATE AC command.						
Padding Flag	or 2 B 1 N	For Scheme ID = '3', '4' or '6', this will be the 2 byte ATC. If Scheme ID is '6', the following field will be present. Padding Flag to indicate if padding is applied to Plain Text Message Data 0 = Input Plaintext Message Data is not padded 1 = Input Plaintext Message Data is padded						
Plaintext Message Data Length	4 H	If Scheme ID is '3', '4', '5' or '6', or if Mode Flag is '4' and Scheme ID is '1', the following field will be present. Length in bytes of data in next field.						
Plaintext Message Data	n B	If Scheme ID is '3', '4', '5' or '6', or if Mode Flag is '4' and Scheme ID is '1', the following field will be present. The plaintext message, excluding padding (and before any cipher text is inserted).						
Delimiter	1 A	Delimiter of previous field, ':'.						
MK-SMC	32 H or 'U' + 32 H or 'S' + n A	Only present if Mode Flag is '2' or '4'. The Master Key for Secure Messaging with Confidentiality, used to encrypt the message. For a Variant LMK, the 'MK-SMC' must be encrypted under LMK pair 28-29 variant 3. For a Key Block LMK, the 'MK-SMC' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'E1'</td> <td>'T'</td> <td>'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'E1'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E1'	'T'	'X', 'N'						

Field	Length & Type	Details						
TK	32 H or 'U' + 32 H or 'S' + n A	If Mode Flag is '1' or '2' and the Scheme ID is not '6', the following field will be present The Transport Key, used to decrypt the supplied message. For a Variant LMK, the 'TK' must be encrypted under LMK pair 30-31. For a Key Block LMK, the 'TK' must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'D0', '22'</td><td>T'</td><td>'B', 'D', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'D0', '22'	T'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'D0', '22'	T'	'B', 'D', 'N'						
Confidentiality Session Data	8 B	If Mode Flag is '1', '2', '3' or '4' and the Scheme ID is not '6', the following field will be present Used for Confidentiality Session Key Generation. For Scheme ID = '0', '2', '3' or '4', (Visa/UKIS or AEIPS or JCB CVN 01 and 02) this is the 2 byte ATC right justified and padded on the left with 6 zero bytes. For Scheme ID = '1' (Europay/MasterCard) this is a random number, RANDc. For Scheme ID='5' (JCB CVN 04), this is the Application Cryptogram returned by the card in response to the first GENERATE AC command						
Offset	4 H	Only present if Mode Flag = '1', '2', '3' or '4'. The position within Plaintext data to insert Ciphertext data. Must be between '0000' and Plaintext Message Data length. If Offset = n, Ciphertext is inserted AFTER the nth byte of the Plaintext (i.e. if length of Plaintext data is 0039, and Offset is '0039', Ciphertext data is placed at the end of the plaintext message). If Mode Flag = '3' or '4', this is used to specify where to place the new PIN Block within the message provided in the Plaintext Data field.						
If Mode Flag is '1', '2', '3' or '4' and the Scheme ID is not '6', the following three fields must be present.								
Cipher Text Message Data Length	4 H	Length in bytes of data in next field.						
Cipher Text Message Data	n B	This field must be 8, 16, 24 or 32 bytes. Note that no additional padding is performed on the decrypted message before the re-encryption process. If Mode Flag = '1' or '2', this field contains the message to be sent to the card, and is encrypted under the Transport Key (TK). If Mode Flag = '3' or '4': <ul style="list-style-type: none"> • If Destination PIN Block Type ≠ '42', this field contains the New PIN Block, encrypted under the Source PIN Encryption Key. • If Destination PIN Block Type = '42', this field contains the Current PIN Block concatenated with New PIN Block, both encrypted under the Source PIN Encryption Key. 						
Delimiter	1 A	Delimiter of previous field, ':'.						
Source PIN Encryption Key Type	1 N	Only present if Mode Flag = '3' or '4'. For a Variant LMK: Type of PIN Encryption Key: '0': ZPK '1': TPK.						
	or 1 H	For a Key Block LMK: This field is ignored; should be set to 'F'.						
Source PIN Encryption Key	16 H or 'U' + 32 H or T' + 48 H or 'S' + n A	Only present if Mode Flag = '3' or '4'. The source PIN Encryption Key, used to decrypt the supplied new PIN block (in the Cipher Text Message field). For a Variant LMK, the 'Source PIN Encryption Key' must be either: a ZPK, encrypted under LMK pair 06-07, or a TPK, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y". For a Key Block LMK, the 'Source PIN Encryption Key' must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'P0', '71', '72'</td><td>'D', 'T', 'A'</td><td>'B', 'D', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'P0', '71', '72'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '71', '72'	'D', 'T', 'A'	'B', 'D', 'N'						
Source PIN Block Format Code	2 N	Only present if Mode Flag = '3' or '4'. The format code for the source PIN block.						
Destination PIN Block Format Code	2 N	Only present if Mode Flag = '3' or '4', and Scheme ID ≠ '6'. The format code for the destination PIN block: '34': Standard EMV PIN Block '35': Europay / Mastercard Pay Now & Pay Later						

Field	Length & Type	Details						
Primary Account Number (PAN)	n N or 18 H or 12 N 1 A 32 H or 'U' + 32 H or 'S' + n A	'41': Visa / Amex Format Without Using Current PIN '42': Visa / AmexFormat using Current PIN. Only present if Mode Flag = '3' or '4', and Scheme ID ≠ '6'. The Primary Account Number, used to form the PIN Block. If Source PIN Block Format Code = '48': The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present. If Source PIN Block Format Code = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of Source PIN Block Format Code: The 12 right-most digits of the PAN, excluding the check digit. Value ';'. Only present if Source PIN Block Format Code = '48'. Only present if Mode Flag = '3' or '4', and Scheme ID ≠ '6' and Destination PIN Block Format = '41' or '42'. The Issuer Master Key for generating and verifying Application Cryptograms. This is required to create PIN Blocks for Visa PIN Change. For a Variant LMK, the 'MK-AC' must be encrypted under LMK pair 28-29 variant 1. For a Key Block LMK, the 'MK-AC' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'E0'</td> <td>'T'</td> <td>'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'E0'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E0'	'T'	'X', 'N'						
Primary Account Number (PAN)	n N or 18 H or 12 N 1 A 1 N	Only present if Mode Flag = '3' or '4', and Scheme ID = '6'. The Primary Account Number, used to form the PIN Block. If Source PIN Block Format Code = '48': The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present. If Source PIN Block Format Code = '04': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of Source PIN Block Format Code: The 12 right-most digits of the PAN, excluding the check digit. Value ';'. Only present if Source PIN Block Format Code = '48'. Only present if Mode Flag is '3' or '4', and Scheme ID = '6'. The format code for the destination PIN block. '1': Destination PIN block with current (old) PIN '2': Destination PIN block without current (old) PIN						
Source New PIN Block	16 H or 32 H	Only present if Mode Flag is '3' or '4', and Scheme ID = '6'. Source new PIN block, encrypted under the Source PIN Encryption Key. When using a DES Source PIN Encryption Key, this field will be 16 H. When using an AES Source PIN Encryption Key, this field will be 32 H.						
Source Current PIN Block	16 H or 32 H	Only present if Mode Flag is '3' or '4', and Scheme ID = '6'. The Source current PIN block, encrypted under the Source PIN Encryption Key. Only present if Destination PIN Block Format is '1'. When using a DES Source PIN Encryption Key, this field will be 16 H. When using an AES Source PIN Encryption Key, this field will be 32 H.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'KV'.
Error Code	2 A	<p>'00': No error '04': Mode Flag not set to 0,1,2,3,4 '05': Unrecognized Scheme ID '06': Invalid Offset '07': Invalid ciphertext message length parameter '08': Ciphertext message length error '09': TK or ZPK/TPK parity error '10': MK-SMI parity error '11': MK-SMC parity error '50': Source PIN Encryption Key Type, not set to 0 or 1 '51': Invalid message header '52': PIN length error (in New PIN Block) '68': Command disabled '69': PIN Block format has been disabled or a standard error code.</p>
MAC	8 B	Present for all Scheme ID's other than '6': The calculated 8-byte MAC
MAC	8 H	Only present if Scheme ID = '6'. The calculated 4-byte MAC
Encrypted Destination New PIN Block Data	32 H	Only present if Mode Flag = '3' or '4' and Scheme ID = '6'. Encrypted Destination New PIN Data
Re-encrypted ciphertext Data Length	4 H	Only present if Mode Flag = '1', '2', '3' or '4' and the Scheme ID is not '6'. Length in bytes of data in next field.
Re-encrypted ciphertext message Data	n B	Only present if Mode Flag = '1', '2', '3' or '4' and the Scheme ID is not '6'. Re-encrypted Ciphertext message data.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Secure Message (EMV 4.x)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Generate a Secure Message with Integrity over data to be sent from the Issuer back to the Card. Optionally, Secure Messaging with Confidentiality is provided in which case the message data must be supplied encrypted under a Transport Key. In this latter case the command first decrypts the message data using the Transport Key before re-encrypting it using a Session Key.

Notes: This command performs a similar function to the KU command, but uses the EMV2000 method or EMV Common Session Key Derivation method for generating the session key.

This command supports the following cryptogram methods:

Cryptogram Version Number (CVN)	Scheme ID	MK-SMC/SMI
Visa VIS (CVN 14)	'0'	112-bit 3DES
Visa VIS (CVN '22')	'9'	112-bit 3DES
Visa VIS (CVN 18)	'A'	112-bit 3DES
Visa VIS (CVN 16 or 26)	'B'	128-bit or 256-bit AES
Mastercard M/Chip (CVN 12 or 13)	'1'	112-bit 3DES
Mastercard M/Chip (CVN 14 or 15)	'6'	112-bit 3DES
Discover D-PAS (CVN 05 or 06)	'6'	112-bit 3DES
EMV Option 'C' Card Key Derivation and EMV CSK	'8'	128-bit or 256-bit AES

The KU command provided modes to enable the use of the Issuer Master Key for both integrity and confidentiality. This was to support an option in M/Chip 2.1. The M/Chip 4 specification recommends that different keys are used for integrity and confidentiality. To support this recommendation, this command does not allow generation of keys for integrity and confidentiality from the same master key.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'KY'.
Mode Flag	1 N	<p>The following modes define the operation of the Function:</p> <p>'0': Integrity only '1': Reserved for future use '2': Integrity and Confidentiality '3': Reserved for future use '4': Integrity and PIN Change '5': Integrity only. Use Scheme ID field to identify Key Derivation method.</p> <p>Note: Modes 1 & 3 are not used. The KU command used these modes for Integrity and Confidentiality using the same Master Key. This is not supported in the KY command.</p> <p>For Mode = 0, EMV 4.x Option 'A' ICC Master Key Derivation and EMV2000 Session Key Derivation method will be used (for backward compatibility). For all other modes, the Key Derivation method must be specified in the Scheme ID field.</p>

Field	Length & Type	Details						
Scheme ID	1 N	<p>Only present for Mode Flag = '2', '4' or '5'. Identifier for the card Scheme, used to specify the padding and key derivation method.</p> <p>'0': Visa VIS using EMV 4.x Option 'A' ICC Master Key Derivation and EMV2000 Session Key Derivation</p> <p>'1': Mastercard M/Chip using EMV 4.x Option 'A' ICC Master Key Derivation and EMV2000 Session Key Derivation</p> <p>'2': Reserved for future use</p> <p>'3': Reserved for future use</p> <p>'4': CCD using EMV 4.x Option 'B' ICC Master Key Derivation and EMV2000 Session Key Derivation</p> <p>'5': Visa VIS and Indonesian National Standard Chip Card Specification (NSICCS) using EMV 4.x Option 'A' ICC Master Key Derivation and EMV Common Session Key Derivation</p> <p>'6': Mastercard M/Chip and Discover D-PAS using EMV 4.x Option 'A' ICC Master Key Derivation and EMV Common Session Key Derivation</p> <p>'7': CCD using EMV 4.x Option 'B' ICC Master Key Derivation and EMV Common Session Key Derivation</p> <p>'8': CCD using EMV 4.x Option 'C' ICC Master Key Derivation EMV AES Common Session Key Derivation. Only permitted if Mode Flag = '5'.</p> <p>'9': Visa VIS 1.6 using EMV 4.3 Option 'B' ICC Master Key derivation and EMV Common Session Key Generation.</p> <p>'A': Visa VIS 1.6 using EMV 4.3 Option 'B' ICC Master Key derivation and XOR Session Key Generation.</p> <p>'B': Visa VIS 3.0 using EMV 4.4 Option 'C' ICC Master Key derivation and EMV Common Session Key Derivation. Only permitted if Mode Flag = '4'.</p> <p>Used to specify the padding and Key Derivation Methods to use.</p> <p>Note: For Mode Flag = '5', this field only specifies the key derivation method as padding is not relevant.</p>						
MK-SMI	32 H or 'U' + 32 H or 'S' + n A	<p>The Master Key for Secure Messaging with Integrity, used to generate a MAC on the message.</p> <p>For a Variant LMK, the 'MK-SMI' must be encrypted under LMK pair 28-29 variant 2.</p> <p>For a Key Block LMK, the 'MK-SMI' must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'E2'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'E2'	'T', 'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E2'	'T', 'A'	'X', 'N'						
IV-SMI	16 B	Only present for Mode = '0' or when Scheme ID = '0', '1' or '4'. IV for EMV2000 Secure Messaging for Integrity session key derivation						
PAN Length	2 N	Only present for Scheme ID = '4', '7', '8', '9' or 'A'. Number of bytes in PAN/PAN Sequence Number field. Valid values '01' ... '19'. <i>Note: This field indicates the number of bytes used to store the PAN/PSN. If the number of digits in the PAN/PSN is odd, an extra '0' digit must be inserted to the left.</i>						
PAN/PAN Sequence No	8 B or n B	<p>Concatenation of the Primary Account Number (PAN) and the PAN Sequence Number.</p> <p>For Scheme ID = '0', '1', '5' or '6' this field will be fixed at 8 bytes, and will contain the pre-formatted PAN/PSN (in BCD format). <i>Note: It is the responsibility of the host system to ensure that the PAN/PSN is appropriately padded to 8 bytes, according to EMV Option A.</i></p> <p>For Scheme ID = '4', '7', '8', '9' or 'A', this field contains the PAN/PSN (in BCD format). The field length is specified (in bytes) by the PAN length field. <i>Note: It is the responsibility of the host system to ensure that the PAN/PSN is an even number of digits (therefore a whole number of bytes) by pre-pending an extra 0 digit to the left if necessary. The PAN/PSN is then used as in EMV Option B.</i></p> <p><i>Note: If PAN length <= 8 bytes EMV Option A will be used, and the HSM will pad appropriately to 8 bytes if necessary.</i></p>						
Delimiter	1 A	Only present for Scheme ID = '4', '7', '8', '9' or 'A'. Delimiter, to indicate end of PAN/PAN Sequence No, value ';'.						
Branch/Height parameters	1 N	Only present for Mode = '0' or when Scheme ID = '0', '1' or '4'. '0': Branch factor 2; Tree Height 16 '1': Branch factor 4; Tree Height 8						
Application Transaction Counter	2 B	Only present for Mode = '0' or when Scheme ID = '0', '1' or '4' or 'A'. The ATC from the card. This is used for Session Key Generation.						

Field	Length & Type	Details						
Application Cryptogram	8 B	Only present for Scheme ID = '5', '6', '7', '8' or '9'. The Application Cryptogram returned by the card in response to the first GENERATE AC command.						
Plaintext Message Data Length	4 H	Length in bytes of data in next field.						
Plaintext Message Data	n B	The plaintext message, excluding padding (and before any cipher text is inserted).						
Delimiter	1 A	Delimiter of previous field, ';'.						
MK-SMC	32 H or 'U' + 32 H or 'S' + n A	The Master Key for Secure Messaging with Confidentiality, used to encrypt the message. Only present if Mode Flag = '2' or '4'. For a Variant LMK, the 'MK-SMC' must be encrypted under LMK pair 28-29 variant 3. For a Key Block LMK, the 'MK-SMC' must comply with the following: <table border="1"><thead><tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr></thead><tbody><tr><td>'E1'</td><td>'T', 'A'</td><td>'X', 'N'</td></tr></tbody></table>	Key Usage	Algorithm	Mode of Use	'E1'	'T', 'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E1'	'T', 'A'	'X', 'N'						
IV-SMC	16 B	Only present if Mode Flag = '2' or '4' and Scheme ID = '0', '1' or '4'. IV for EMV2000 Secure Messaging for Confidentiality session key derivation.						
TK	32 H or 'U' + 32 H or 'S' + n A	Only present if Mode Flag = '2'. The Transport Key, used to decrypt the supplied message. For a Variant LMK, the 'TK' must be encrypted under LMK pair 30-31. For a Key Block LMK, the 'TK' must comply with the following: <table border="1"><thead><tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr></thead><tbody><tr><td>'D0', '22'</td><td>'T'</td><td>'B', 'D', 'N'</td></tr></tbody></table>	Key Usage	Algorithm	Mode of Use	'D0', '22'	'T'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'D0', '22'	'T'	'B', 'D', 'N'						
Offset	4 H	Only present if Mode Flag = '2' or '4'. Position within Plaintext data to insert Ciphertext data. Must be between '0000' and Plaintext Message Data length. If Offset = n, Ciphertext is inserted AFTER the nth byte of the Plaintext. (i.e. if length of Plaintext data is '0039', and Offset is '0039', then the Ciphertext data is placed at the end of the plaintext message). If Mode Flag = '4', this is used to specify where to place the new PIN block within the message provided in the Plaintext Data field.						
Cipher Text Message Data Length	4 H	Only present if Mode Flag = '2' or '4'. Length in bytes of data in next field.						
Cipher Text Message Data	n B	Only present if Mode Flag = '2' or '4'. This field must be 8, 16, 24 or 32 bytes. Note that no additional padding is performed on the decrypted message before the re-encryption process. If Mode Flag = '2', this field contains the message to be sent to the card, and is encrypted under the Transport Key (TK). If Mode Flag = '4': <ul style="list-style-type: none">If Destination PIN Block Type ≠ '42', this field contains the New PIN Block, encrypted under the Source PIN Encryption Key.If Destination PIN Block Type = '42', this field contains the Current PIN Block concatenated with New PIN Block, both encrypted under the Source PIN Encryption Key.						
Delimiter	1 A	Only present if Mode Flag = '2' or '4'. Delimiter of previous field, ';'.						
Source PIN Encryption Key Type	1 N or 1 H	Only present if Mode Flag = '4'. For a Variant LMK: Type of PIN Encryption Key: '0': ZPK '1': TPK. For a Key Block LMK: This field is ignored; should be set to 'F'.						
Source PIN Encryption Key		Only present if Mode Flag = '4'. The source PIN Encryption Key, used to decrypt the supplied PIN block (in the Cipher Text Message field).						

Field	Length & Type	Details						
	16 H or 'U' + 32 H or 'T' + 48 H or 'S' + n A	For a Variant LMK, the 'Source PIN Encryption Key' must be either: a ZPK, encrypted under LMK pair 06-07, or a TPK, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y". For a Key Block LMK, the 'Source PIN Encryption Key' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'P0', '71', '72'</td> <td>'D', 'T', 'A'</td> <td>'B', 'D', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'P0', '71', '72'	'D', 'T', 'A'	'B', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'P0', '71', '72'	'D', 'T', 'A'	'B', 'D', 'N'						
Source PIN Block Format code	2 N	Only present if Mode Flag = '4'. The format code for the source PIN block.						
Destination PIN Block format code	2 N	Only present if Mode Flag = '4'. When using a 3DES MK-SMC, the following destination PIN block formats are available: '05': ISO 9564-1 Format 1, ANSI X9.8 Format 1 '34': Standard EMV PIN Block '35': Europay/Mastercard Pay Now & Pay Later '41': Visa Format Without Using Current PIN '42': Visa Format using Current PIN '47': ISO 9564-1 & ANSI X9.8 Format 3. When using an AES MK-SMC, the following destination PIN block format is available: '48': ISO 9564-1 Format 4						
Primary Account Number (PAN)	n N or 18 H or 12 N	Only present if Mode Flag = '4'. The Primary Account Number, used to form the PIN Block. If Source PIN Block Format Code or Destination PIN Block Format Code = '48': The 12-19 digit PAN, including the check digit. If present, the delimiter below must also be present. If Source PIN Block Format Code = '04' and Destination PIN Block Format Code ≠ '48': The 18 digit PAN excluding the check digit. If the PAN is less than 18 digits, it must be right-justified and padded with 'F's on the left. For all other values of Source PIN Block Format Code when Destination PIN Block Format Code ≠ '48': The 12 right-most digits of the PAN, excluding the check digit.						
Delimiter	1 A	Only present if Mode Flag = '4' and PIN Block Format Code = '48'. Value ':'.						
MK-AC	32 H or 'U' + 32 H or 'S' + n A	Only present if Mode Flag = '4' and Destination PIN Block Format Code = '41', '42' or '48'. The Issuer Master Key for generating and verifying Application Cryptograms. This is required to create PIN Blocks for Visa PIN Change. For a Variant LMK, the 'MK-AC' must be encrypted under LMK pair 28-29 variant 1. For a Key Block LMK, the 'MK-AC' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'E0'</td> <td>'T'</td> <td>'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'E0'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E0'	'T'	'X', 'N'						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'KZ'.
Error Code	2 A	'00': No error '04': Invalid Mode flag '05': Invalid key scheme '06': Invalid Offset '07': Invalid ciphertext message length parameter '08': Ciphertext message length error '09': TK or ZPK/TPK parity error '10': MK-SMI parity error '11': MK-SMC parity error '23': Invalid PIN block format code '50': Source PIN Encryption Key Type, not set to 0 or 1 '51': MK-AC parity error '52': Invalid Branch/Height '68': Command disabled '69': PIN Block format has been disabled or a standard error code.
MAC	16 B	The calculated MAC. The MAC will be 16 bytes long under one of the following conditions: - Mode = '5' and Scheme ID = '8' - Mode = '4' and Scheme ID = 'B'
Re-encrypted ciphertext Data Length	8 B	The MAC will be 8 bytes long under all other conditions. Only present for Mode Flag = '2' or '4'. Length in bytes of data in next field.
Re-encrypted ciphertext message Data	n B	Only present for Mode Flag = '2' or '4'. Re-encrypted Ciphertext message.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify Truncated Application Cryptogram (Mastercard CAP)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Optional (see text)	
Activity: diag.host	

Function: Validate a Truncated Application Cryptogram (Mastercard CAP).

Notes: This command supports:
 EMV 4.1 methods A and B for ICC Master Key derivation.
 EMV 3.1.1 and EMV 4.1 (including EMV Common Session Key Derivation) methods for session key derivation.
 This command is compatible with the Visa DPA specification.
 Diagnostic data is produced by this command only if the HSM is in Authorized State.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'K2'.						
Mode Flag	1 H	Mode of operation: '0': Perform Truncated AC verification and MAC verification. '00': Mastercard CAP '01': Mastercard CAP with TDS.						
Scheme ID	2 N	'00': Mastercard CAP '01': Mastercard CAP with TDS.						
ICC Master Key Derivation Method	1 N	Identifies the DK-AC key derivation method: '0': EMV 4.1 Master Key Derivation Option A '1': EMV 4.1 Master Key Derivation Option B						
Session Key Derivation Method	1 N	'0': No Session Key SK-AC used for Application Cryptograms '1': Mastercard (M/Chip 2.1 method) '2': EMV 4.1 (EMV2000) method '3': EMV 4.1 (EMV Common Session Key Derivation Method)						
MK-AC (under LMK)	32 H or 'U' + 32 H or 'S' + n A	The Issuer Master Key for generating and verifying Application Cryptograms. For a Variant LMK, the 'MK-AC' must be encrypted under LMK pair 28-29 variant 1. For a Key Block LMK, the 'MK-AC' must comply with the following:						
		<table border="1"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'E0'</td> <td>T'</td> <td>'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'E0'	T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E0'	T'	'X', 'N'						
IV-AC	16 B	Only present for Session Key Derivation Method = '2'. IV for EMV2000 Application Cryptogram session key derivation						
PAN Length	2 N	Only present for ICC Master Key Derivation Method = '1'. Length in bytes of PAN/PAN Sequence Number field. Valid values '01' ... '99'. <i>Note: This field indicates the number of bytes used to store the PAN/PSN. If the number of digits in the PAN/PSN is odd, an extra '0' digit must be inserted to the left.</i>						
PAN/PAN Sequence No	8 B or n B	For ICC Master Key Derivation Method = '0', this field will be fixed at 8 bytes, and will contain the pre-formatted PAN/PSN (in BCD format). <i>Note: It is the responsibility of the host system to ensure that the PAN/PSN is appropriately padded to 8 bytes, according to EMV Option A.</i> For ICC Master Key Derivation Method = '1', this field contains the PAN/PSN (in BCD format). The field length is specified (in bytes) by the "PAN Length" field. <i>Note: It is the responsibility of the host system to ensure that the PAN/PSN is an even number of digits (therefore a whole number of bytes) by pre-pending an extra '0' digit to the left if necessary. The PAN/PSN is then used as in EMV Option B.</i>						

Field	Length & Type	Details
		Note: If "PAN Length" <= 8 bytes, the HSM will pad appropriately to 8 bytes if necessary, according to EMV Option A.
Delimiter	1 A	Only present for ICC Master Key Derivation Method = '1'. Delimiter, to indicate end of PAN/PAN Sequence No, value ':'.
Branch/Height parameters	1 N	Only present for Session Key Derivation Method = '2'. '0': Branch factor 2; Tree Height 16 '1': Branch factor 4; Tree Height 8.
Application Transaction Counter	2 B	A value for the ATC derived by the host based on the following information: The ATC from the last online transaction stored on the host database The ATC provided by the card in the SecureCode message.
UN	4 B	Unpredictable Number. Only present for Session Key Derivation Method = '1'.
Transaction Data Length	2 H	Length of the following field. Can be any value from '00' ... 'FF'.
Transaction Data	n B	Variable length data. If the data supplied is a multiple of 8 bytes, no extra padding is added. If it is not a multiple of 8 bytes, additional zero padding is added. Note: If alternative padding methods are required, it is the responsibility of the host to provide this.
Delimiter	1 A	Delimiter, to indicate end of Transaction Data, value ':'.
Truncated AC	8 B	Cryptogram to be validated. This field contains the truncated EMV cryptogram value from the SecureCode message. This should be right justified into an 8 byte field, padded on the left with zeros. The HSM will generate a cryptogram using the supplied transaction data; truncate using the supplied IPB; then compare with the value provided in this field.
Cryptogram IPB	8 B	The "Cryptogram" element of the IPB.
IPB MAC	4 B	4 byte MAC generated using MI Console command. This MAC protects against unauthorised manipulation of the IPB.
TDS Data Length	4 N	Length of the following field. Can be any even value from '0002'...'9998'. Only present for Scheme ID = '01'.
TDS Data	n H	The TDS Data. Note: It is the responsibility of the host system to ensure that the TDS Data is appropriately padded, as defined in EMV 4.x Book 2 Appendix A1.2. Only present for Scheme ID = '01'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'K3'.
Error Code	2 A	'00': No error '01': Warning: ARQC/TC/AAC verification failed '04': Invalid Mode Flag '05': Invalid Scheme ID '10': MK parity error '52': Invalid Branch/Height '82': IPB MAC Verification error '67': Command not licensed '68': Command disabled or a standard error code.
Diagnostic data	8 B	HSM generated "Truncated AC". This will be right justified into an 8 byte field, padded on the left with zeros. Returned only if the error code is '01' and the HSM is in Authorised State.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Data Authentication Code and Dynamic Number Verification (EMV 3.1.1)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Optional (see text)	
Activity: diag.host	

Function: Verify a Data Authentication Code (DAC) or Dynamic Number (DN).

Notes: Diagnostic data is produced by this command only if the HSM is in Authorized State.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'KS'.						
Mode Flag	1 H	Mode of operation: '0': Perform DAC Verification '1': Perform DN Verification.						
Scheme ID	1 H	Identifier of the Scheme: '1': Mastercard M/Chip.						
MK-DAC	32 H or 'U' + 32 H	The Issuer Master Key for calculating and verifying Data Authentication Codes. Only present only for Mode '0'. For a Variant LMK, the 'MK-DAC' must be encrypted under LMK pair 28-29 variant 4.						
	or 'S' + n A	For a Key Block LMK, the 'MK-DAC' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'E3'</td> <td>'T'</td> <td>'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'E3'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E3'	'T'	'X', 'N'						
MK-DN	32 H or 'U' + 32 H	The Issuer Master Key for calculating and verifying Dynamic Numbers. Only present only for Mode '1'. For a Variant LMK, the 'MK-DN' must be encrypted under LMK pair 28-29 variant 5.						
	or 'S' + n A	For a Key Block LMK, the 'MK-DN' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'E4'</td> <td>'T'</td> <td>'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'E4'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E4'	'T'	'X', 'N'						
PAN/PAN Sequence No	8 B	Pre-formatted PAN/PAN Sequence No. Present for both Mode '0' and '1'.						
DAC	2 B	Data Authentication Code for validation. Only present for Mode '0'.						
DN	2 B	Dynamic Number for validation. Only present for Mode '1'.						
ATC	2 B	Application Transaction Counter. Only present for Mode '1'.						
UN	4 B	Unpredictable Number. Only present for Mode '1'.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'KT'.
Error Code	2 A	'00': No error '01': Warning: DAC or DN verification failed '04': Mode Flag not 0 or 1 '05': Unrecognized Scheme ID '10': MK parity error '68': Command disabled or a standard error code.
Diagnostic Data	2 B	The calculated DAC or DN (depending on the mode selected). Only provided if error code '01' is returned and the HSM is in Authorised State.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Decrypt Encrypted Counters (EMV 4.x)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: Decrypt & return the encrypted counters that the issuer may optionally include in Issuer Application Data.

Notes: The issuer may include the following offline counters in Issuer Application data:

- Offline Cumulative Transaction Amount (OCTA) (6 bytes).
- Offline Consecutive Transaction Number (OCTN) (1 byte).

The issuer may optionally choose that these counters be encrypted. This command will validate the Encrypted Counter data and return the decrypted counters.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'K0' (K-zero).						
Scheme ID	1 N	Identifies the key derivation method: '0': M/Chip 4 using EMV 4.x ICC Master Key Derivation Option A and EMV2000 Session Key Derivation. '1': M/Chip 4 using EMV 4.x ICC Master Key Derivation Option B and EMV2000 Session Key Derivation. '2': M/Chip 4 using EMV 4.x ICC Master Key Derivation Option A and EMV Common Session Key Derivation. '3': M/Chip 4 using EMV 4.x ICC Master Key Derivation Option B and EMV Common Session Key Derivation. '4': M/Chip 4 using EMV 4.x ICC Master Key Derivation Option A and M/Chip 2.1 Proprietary Session Key Derivation. '5': M/Chip 4 using EMV 4.x ICC Master Key Derivation Option B and M/Chip 2.1 Proprietary Session Key Derivation.						
MK-AC		The Issuer Master Key for generating and verifying Application Cryptograms.						
	32 H or 'U' + 32 H	For a Variant LMK, the 'MK-AC' must be encrypted under LMK pair 28-29 variant 1.						
	or 'S' + n A	For a Key Block LMK, the 'MK-AC' must comply with the following:						
		<table border="1"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'E0'</td> <td>'T'</td> <td>'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'E0'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E0'	'T'	'X', 'N'						
IV-AC	16 B	Only present for Scheme ID = '0' or '1'. IV for EMV2000 Application Cryptogram session key derivation						
PAN Length	2 N	Only present for Scheme ID = '1', '3' or '5'. Length in bytes of PAN/PAN Sequence Number field. Valid values '01' ... '99'. <i>Note: This field indicates the number of bytes used to store the PAN/PSN. If the number of digits in the PAN/PSN is odd, an extra '0' digit must be inserted to the left.</i>						
PAN/PAN Sequence No	8 B or n B	For Scheme ID = '0', '2' or '4', this field will be fixed at 8 bytes, and should contain the pre-formatted PAN/PSN (in BCD format). <i>Note: It is the responsibility of the host system to ensure that the PAN/PSN is appropriately padded to 8 bytes, according to EMV Option A.</i> For Scheme ID = '1', '3' or '5', this field contains the PAN/PSN (in BCD format). The field length is specified (in bytes) by the "PAN Length" field. <i>Note: It is the responsibility of the host system to ensure that the PAN/PSN is an even number of digits (therefore a whole number of bytes) by pre-pending an extra '0' digit to the left if necessary. The PAN/PSN is then used as in EMV Option B.</i>						

payShield 10K Core Host Commands

Field	Length & Type	Details
COMMAND MESSAGE		
Delimiter	1 A	Note: If "PAN Length" <= 8 bytes, the HSM will pad to 8 bytes if necessary, according to EMV Option A.
Branch/Height parameters	1 N	Only present for Scheme ID = '1', '3' or '5'. Delimiter, to indicate end of PAN/PAN Sequence No, value ':'.
UN	4 B	Only present for Scheme ID = '0' or '1'. '0': Branch factor 2; Tree Height 16 '1': Branch factor 4; Tree Height 8.
Application Transaction Counter	2 B	Only present for Scheme ID = '4' or '5'. Unpredictable Number.
Encrypted Counters	8 B	The Encrypted Counter data, containing the OCTA and OCTN
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'K1'.
Error Code	2 A	'00': No error '01': Encrypted Counter verification failure '05': Invalid Scheme ID '10': MK parity error '52': Invalid Branch/Height '68': Command disabled or a standard error code.
OCTA	6 B	Offline Cumulated Transaction Amount.
OCTN	1 B	Offline Consecutive Transaction Number.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

10 EMV Chip, Contactless & Mobile Issuing

10.1 Contactless Cards Data Preparation Commands

Use of this command requires the optional Contactless Cards Data Preparation license.

The HSM provides the following host command to support generation of the data required for issuing magnetic stripe based Contactless Cards:

Function	Command	Page
<i>Generate IVCVC3 and Static CVC3</i>	NY (NZ)	555

Generate IVCVC3 and Static CVC3

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Generate IVCVC3 & CVC3 or PINIVCVC3 & PINCVC3.

Notes: Mastercard's PayPass requires an IVCVC3 for card personalization. Calculation of the Static CVC3 requires the IVCVC3 which is a MAC calculated over the static part of Track₁ or Track₂ data using the DK-CVC3. This command creates the IVCVC3 and the CVC3 from the Track (1 or 2) Data provided.

Mobile PayPass requires the use of a PINIVCVC3 value for the calculation of the PINCVC3.

From the Mastercard Mobile PayPass M/Chip specifications:

The PINIVCVC3 is an issuer proprietary static data object that is used as input for the generation of the CVC 3 cryptogram when the reader supports the Mobile extensions and when the PIN has been successfully verified offline.

PIN initialization vector (PINIVCVC3) = initialization vector (IVCVC3) XOR '9559'

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'NY'.						
Scheme ID	1 N	Identifier for Card Scheme: '1': Mastercard PayPass (IVCVC3 and CVC3) '2': Mastercard PayPass (PINIVCVC3 and PINCVC3) Other values are RFU.						
MK-CVC3	32 H or 'U' + 32 H or 'S' + n A	The Issuer Master Key for calculating the CVC3. For a Variant LMK, the MK-CVC3 is encrypted under LMK 28-29/7. For a Key Block LMK, the MK-CVC3 must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'E0', 'E6', '32'</td> <td>'T'</td> <td>'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'E0', 'E6', '32'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E0', 'E6', '32'	'T'	'X', 'N'						
Key Derivation Method	1 A	Method to be used to derive a unique key from the Master Key: 'A': EMV 4.1 Book 2 Option A method 'B': EMV 4.1 Book 2 Option B method						
Derivation Data	n N	Concatenation of the Primary Account Number and 2 digit Sequence Number for the card. If the Sequence Number is not available it should be specified as '00'.						
Delimiter	1 A	Delimiter. Value ';'.						
Track Data Length	3 N	The length of the following field.						
Track Data	n B	Static Track (1 or 2) Data.						
Delimiter	1 A	Delimiter. Value ';'.						
Unpredictable Number	8 N	Random number provided to the card by the terminal during a PayPass transaction.						
ATC	5 N	Decimal value of Application Transaction Counter. Max value 65535 (2 byte field).						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'NZ'.
Error Code	2 N	'00': No error '04': Unrecognized Key Derivation Method '05': Invalid Scheme ID '10': MK-CVC3 Parity Error 'EA': MK-CVC3 – key block specific error or a standard error code.
If Error Code = 'EA', the following field will be present:		
Additional Error Code	2 A	The key block specific error code
IVCVC3/PINIVCVC3	5 N	The calculated IVCVC3 or PINIVCVC3.
Static CVC3/PINCVC3	5 N	The calculated CVC3 or PINCVC3. In cases where only 3 or 4 digits are required, the application can truncate the returned value.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

10.2 EMV-based Cards Data Preparation Commands

The HSM provides the following host commands to support generation of the data required for basic EMV-based cards:

Function	Command	Page
<i>Generate Issuer RSA Key Set and Public Key Certificate</i>	KE (KF)	558
<i>Validate an Issuer Public Key Certificate</i>	KG (KH)	561
<i>Generate Static Data Authentication Signature</i>	KM (KN)	564
<i>Generate Card RSA Key Set and Public Key Certificate</i>	KO (KP)	566
<i>Import a Certification Authority Self-Signed Certificate</i>	KK (KL)	571
<i>EMV Sign Data</i>	IK (IL)	574
<i>EMV Recover Data</i>	IM (IN)	576

Generate Issuer RSA Key Set and Public Key Certificate

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Variant LMK	Authorization: Required Activity: generate.rsa.host
Key Block LMK	Authorization: Required Activity: generate.03.host

Function: Generate an Issuer RSA Key Set and return the Public Key in the form of a Self-Signed Issuer Public Key Certificate following the format of the card association specified in the command.

Alternatively, generate a Self-Signed Issuer Public Key Certificate following the format of the card association specified in the command using a Private/Public key pair previously generated by this command. The command will verify that the Private/Public key pair correspond to each other.

Notes: The RSA Key Type for the Private Key will be set to 2 (Signature and Key Management). A Public Exponent of 65537 ($2^{16} + 1$) will be used unless another is specified. If a Public Exponent is supplied, it must be 3 or 65537; otherwise, an error will be returned by the HSM and no processing will take place.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'KE'.
Scheme ID	1 N	'0': Visa VSDC '1': Mastercard '2': American Express AEIPS V4.1 '3': JCB '4': Union Pay '5': Discover
Mode Flag	1 N	'0': Generate Issuer Key Pair and certificate, using Strong Primes '1': Generate certificate only with provided Issuer Key Pair '2': Generate Issuer Key Pair and certificate using Standard Primes
Hash Identifier	2 N	Identifier of algorithm used to hash data: '01': SHA-1
Signature Identifier	2 N	Identifier of signature algorithm: '01': RSA
If Mode Flag = '0' or '2', the following 5 fields must be present as noted below:		
Key Length	4 N	Modulus length in bits (must be a multiple of 8) minimum value = 0400, maximum value = 2040.
Authentication Data	n A	Optional. Additional data to be included in the Public Key MAC calculation (must not include ';').
Delimiter	1 A	Mandatory Delimiter. Value ';'.
Public Exponent Length	4 N	Optional. Length, in bits, of the Public Exponent. Must be supplied if Public Exponent is present in command message.

Field	Length & Type	Details					
Public Exponent	n B	Optional. If supplied, it must follow guidelines described in the command notes. If not supplied then a default exponent of 65537 will be used.					
If Mode Flag = '1', the following 4 fields must be present as noted below:							
Issuer Private Key Length	4 N	Length of the Issuer Private Key.					
	or 4 H	For a Variant LMK, the length, in bytes, of the Issuer Private Key field. For a Key Block LMK, this field is ignored and should be set to 'FFFF'.					
Issuer Private Key	n B	The Issuer Private Key, encrypted under the LMK.					
	or 'S' + n B	For a Variant LMK, the Issuer Private Key is encrypted under LMK 34-35. For a Key Block LMK, the Issuer Private Key must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'03'</td> <td>'R'</td> <td>'S', 'D', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'03'	'R'
Key Usage	Algorithm	Mode of Use					
'03'	'R'	'S', 'D', 'N'					
Delimiter	1 A	Mandatory Delimiter. Value ':'.					
Issuer Public Key	n B	Issuer Public Key, DER encoded (unsigned) in ASN.1 format (sequence of modulus and exponent)					
The following fields must be present as noted below:							
Delimiter	1 A	Mandatory Delimiter. Value ':'.					
For Scheme-ID = '0', '1', '2', '3' and '4', the following 2 fields must be present:							
Issuer Identifier (BIN)	8 H	Leftmost 3-8 digits from the Primary Account Number (PAN) padded to the right with Hex 'F's.					
Certificate Expiration Date	4 N	Expiration date of certificate in Month and Year (MMYY) format.					
For Scheme-ID = '0' (Visa VSDC), the following 2 fields providing the data to be included in the self-signed certificate must be present. (See <i>Card Issuing Appendix A – Self-Signed Issuer Public Key Certificate Format</i> (Visa)).							
Service Identifier	8 H	Identifies the specific Visa service padded to the right with Hex '0's.					
Tracking Number	6 N	Certificate tracking number assigned by Visa.					
For Scheme-ID = '1' (Mastercard), the following 2 fields providing the data to be included in the self-signed certificate must be present (See <i>Card Issuing Appendix B – Self-Signed Issuer Public Key Certificate Format</i> (Mastercard)).							
Certificate Serial Number	6 H	Certificate tracking number.					
Issuer Public Key Index	6 H	Issuer assigned unique public key identifier.					
For Scheme-ID = '2' (American Express AEIPS V4.1), the following 2 fields providing the data to be included in the self-signed certificate must be present (See <i>Card Issuing Appendix C – Self-Signed Issuer Public Key Certificate Format</i> (American Express)):							
Service Identifier	8 H	Identifies the specific American Express Product Identifier.					
Tracking Number	6 N	Transmittal tracking number.					
For Scheme-ID = '3' (JCB), the following 2 fields providing the data to be included in the self-signed certificate must be present:							
Certificate Serial Number	6 H	Certificate tracking number.					
Issuer Public Key Index	6 H	Issuer assigned unique public key identifier.					
For Scheme-ID = '4' (Union Pay), the following 2 fields providing the data to be included in the self-signed certificate must be present:							
Service Identifier	8 H	Identifies the specific Union Pay service padded to the right with Hex '0's.					
Tracking Number	6 N	Application record No. in the issuer public key					
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.					
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.					
If Key Block LMK, the following fields must be present:							
Delimiter	1 A	Value '&'. Optional; can only be present when the generated private key is to be exported; if present, the following field must also be present.					
Modified Export Value	1 A	Character to be placed in the exportability field (byte 11) of the exported private key; only permitted values are 'N', 'S'; must be present if the above Delimiter is present.					
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.					
Message Trailer	n A	Optional. Maximum length 32 characters.					

Field	Length & Type	Details						
RESPONSE MESSAGE								
Message Header	m A	Returned to the Host unchanged.						
Response Code	2 A	Value 'KF'.						
Error Code	2 N	<p>'00': No error '05': Invalid Scheme ID or Mode Flag '06': Invalid hash or signature identifier or a standard error code. For Mode = '0', '2' or '4' only: '03': Key Length error '07': Public exponent length error '08': Supplied public exponent value is not allowed For Mode = '1' or '3' only: '02': Public Key does not conform to encoding rules '09': Invalid Public key / Private key pair 'E8': Private Key – key block error 'E9': Public Key – key block error</p>						
If Error Code = 'E8' or 'E9', the following field will be present:								
Additional Error Code	2 A	The key block specific error code						
If Mode Flag = '0' or '2', the following 4 fields will be present:								
MAC	4 B	Only present if using a Variant LMK. MAC on Issuer Public Key and Authentication Data calculated using LMK 36-37.						
Issuer Public Key	n B or 'S' + n B	<p>The Issuer Public Key.</p> <p>For a Variant LMK, the Issuer Public Key, DER encoded (unsigned) in ASN.1 format (sequence of modulus and exponent).</p> <p>For a Key Block LMK, the Issuer Public Key will conform to:</p> <table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'02'</td> <td>'R'</td> <td>'V'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'02'	'R'	'V'
Key Usage	Algorithm	Mode of Use						
'02'	'R'	'V'						
Issuer Private Key Length	4 N	Only present if using a Variant LMK. Length, in bytes, of the Issuer Private Key field.						
Issuer Private Key	n B or 'S' + n B	<p>The Issuer Private Key.</p> <p>For a Variant LMK, the Issuer Private Key is encrypted under LMK 34-35.</p> <p>For a Key Block LMK, the Issuer Private Key will conform to:</p> <table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'03'</td> <td>'R'</td> <td>'S'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'03'	'R'	'S'
Key Usage	Algorithm	Mode of Use						
'03'	'R'	'S'						
For Scheme-ID = '0', '1', '2', '3' or '4', the following fields will be present:								
Certificate Length	4 N	Length, in bytes, of Self-Signed Certificate.						
Self-Signed Issuer Public Key Certificate	n B	<p>Self-Signed Issuer Public Key Certificate (the concatenation of the Clear Data and the Self-Signed Certificate). See the appropriate appendix, depending on Scheme ID:</p> <ul style="list-style-type: none"> <i>Card Issuing Appendix A – Self-Signed Issuer Public Key Certificate Format (Visa)</i> <i>Card Issuing Appendix B – Self-Signed Issuer Public Key Certificate Format (Mastercard)</i> <i>Card Issuing Appendix C – Self-Signed Issuer Public Key Certificate Format (American Express)</i> 						
Hash Length	2 N	Length in hex characters of hash results in next field. This length will depend on the hash algorithm specified in the command message. For SHA-1, this length will be '40'.						
Hash Value	n H	Hash value required for transfer of self-signed Issuer Public Key data as defined by Scheme ID.						
For Scheme-ID = '5', the following field will be present:								
Issuer Public Key Modulus	n B	The Issuer Public Key Modulus value.						
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.						
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.						

Validate an Issuer Public Key Certificate

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Validate an Issuer public key certificate returned by the Certificate Authority and return the Public Key with its associated MAC. Optionally, verify the Public Key in the certificate corresponds to the Private Key for the key pair.

Notes: A complete Issuer Public Key Certificate comprises an Unsigned Data section, an Issuer Public Key Certificate and, for American Express, Visa and Union Pay certificates, an optional Detached Signature. The Detached Signature is a signature on the first two parts of the certificate and will be validated by this command if present in the provided certificate.

Compatibility Note: In this revision, the command has been enhanced to also return the Hash in the Detached Signature, if present in the Public Key Certificate, for American Express and Visa certificates.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'KG'.						
Scheme ID	1 N	'0': Visa VSDC '1': Mastercard '2': American Express AEIPS V4.1 '3': JCB '4': Union Pay '5': Discover						
CA Public Key MAC	4 B	Only present if using a Variant LMK. MAC on Public Key and Authentication Data calculated using LMK 36-37.						
CA Public Key	n B	CA Public key, DER encoded (unsigned) in ASN.1 format (Sequence of modulus, exponent).						
	or 'S' + n B	For a Variant LMK, the CA Public Key, DER encoded (unsigned) in ASN.1 format (sequence of modulus and exponent). For a Key Block LMK, the CA Public Key must comply with:						
		<table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'02'</td> <td>'R'</td> <td>'N', 'V'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'02'	'R'	'N', 'V'
Key Usage	Algorithm	Mode of Use						
'02'	'R'	'N', 'V'						
CA Authentication Data	n A	Only present if using a Variant LMK. Optional; additional data to be included in the CA public key MAC calculation (must not include ';').						
Delimiter	1 A	Mandatory Delimiter. Value ';'.						
Certificate Length	4 N	Length, in bytes, of the Issuer Certificate.						
Issuer Certificate	n B	Issuer Certificate, comprising of the Unsigned Data and the Issuer Public Key Certificate. See the appropriate appendix, depending on Scheme ID: <ul style="list-style-type: none"> • <i>Card Issuing Appendix D – Issuer Public Key Certificate Format (Visa)</i> • <i>Card Issuing Appendix E – Issuer Public Key Certificate Format (Mastercard)</i> • <i>Card Issuing Appendix F – Issuer Public Key Certificate Format (American Express)</i> For Scheme ID = '0' (Visa VSDC) and Scheme ID = '2' (American Express AEIPS V4.1), the Issuer certificate may also include a Detached Signature.						
Delimiter	1 A	Mandatory Delimiter. Value ';'.						
Issuer Authentication Data	n A	Optional. Additional data to be included in the Issuer Public Key MAC calculation (must not include ';').						
Delimiter	1 A	Mandatory Delimiter. Value ';'.						
Issuer Private Key Length	4 N or 4 H	Length of the Issuer Private Key. For a Variant LMK, the length, in bytes, of the Issuer Private Key field. For a Key Block LMK, this field is ignored and should be set to 'FFFF'.						
Issuer Private Key	n B or 'S' + n B	The Issuer Private Key. For a Variant LMK, the Issuer Private Key is encrypted under LMK 34-35. For a Key Block LMK, the Issuer Private Key must comply with:						
		<table border="1"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'03'</td> <td>'R'</td> <td>'S', 'D', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'03'	'R'	'S', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'03'	'R'	'S', 'D', 'N'						
Delimiter	1 A	Mandatory Delimiter. Value ';'.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details						
RESPONSE MESSAGE								
Message Header	m A	Returned to the Host unchanged.						
Response Code	2 A	Value 'KH'.						
Error Code	2 N	<p>'00': No error '01': MAC verification failure '05': Invalid Scheme ID '06': Invalid Hash or Signature algorithm '07': Certificate Hash validation failure '08': CA PK does not conform to encoding rules '09': Invalid Public key / Private key pair '76': Public key length error '78': Private key length error '80': Certificate length error '81': Invalid Certificate Format (Header or Trailer) 'E8': Invalid Private Key Block 'E9': Invalid Certificate Format Identifier or a standard error code.</p> <p>For Scheme ID = '0', '2' or '4' only:</p> <p>'52': Invalid Certificate Extension Header '53': Detached Signature format error '54': Detached Signature length error '55': Detached Signature error</p>						
If Error Code = 'E8' or 'E9', the following field will be present:								
Additional Error Code	2 A	The key block specific error code						
MAC	4 B	Only present if using a Variant LMK. MAC on Issuer Public Key and Authentication Data calculated using LMK 36-37.						
Issuer Public Key	n B	<p>The Issuer Public key.</p> <p>For a Variant LMK, the Issuer Public Key, DER encoded (unsigned) in ASN.1 format (sequence of modulus and exponent).</p>						
	or 'S' + n B	<p>For a Key Block LMK, the Issuer Public Key will conform to:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'02'</td> <td>'R'</td> <td>'V'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'02'	'R'	'V'
Key Usage	Algorithm	Mode of Use						
'02'	'R'	'V'						
Hash Length	2 N	Length in hex characters of hash results in next field. This length will depend on the hash algorithm specified in the certificate. For SHA-1 this length will be 40.						
Hash Value	n H	Hash Value from Issuer Public Key Certificate.						
Issuer Identification Number	8 H	Issuer Identifier recovered from Issuer Public Key Certificate.						
Certificate Expiry Date	4 N	Certificate Expiration Date (MMYY) recovered from the Issuer Public Key Certificate.						
Certificate Serial/Tracking Number	6 H	Certificate Serial/Tracking Number recovered from the Issuer Public Key Certificate.						
For Scheme 0 (Visa VSDC) and 2 (American Express AEIPS V4.1) and '4' (Union Pay), the following fields will be present. Refer to <i>Card Issuing Appendix D – Issuer Public Key Certificate Format</i> (Visa) or <i>Card Issuing Appendix F – Issuer Public Key Certificate Format</i> (American Express) respectively for details on Detached Signatures.								
Detached Signature Hash Length	2 N	Length in hex characters of hash results in next field. This length will depend on the hash algorithm specified in the detached signature. For SHA-1, this length will be '40'. If a Detached Signature is not present in the Certificate, the length field will be '00' and the next field will not be present.						
Detached Signature Hash Value	n H	Hash value in Detached Signature.						
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.						
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.						

Generate Static Data Authentication Signature

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Sign Card Data using Issuer's Private Key

Notes: Automatic DAC generation is provided as an option (used by Mastercard schemes).

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'KM'.						
Hash Identifier	2 N	Identifier of algorithm used to hash data. '01': SHA-1						
Data Authentication Code	2 B	Data Authentication Code. A value must always be supplied but it will be ignored if the optional parameters at the end are supplied in which case the DAC is calculated.						
Data Length	4 N	Length of Static Authentication Data field.						
Static Authentication Data	n B	Static authentication data.						
Delimiter	1 A	Mandatory Delimiter. Value ':'.						
Issuer Private Key Flag	2 N	Flag to indicate location of the Issuer's Private key: If flag = '99' use Issuer Private key provided with command else flag = index of stored Issuer Private key.						
Issuer Private Key Length	4 N or 4 H	Length of the Issuer Private Key. Only present if Issuer Private Key Flag = '99'.						
Issuer Private Key	n B or 'S' + n B	The Issuer Private Key. Only present if Private Key Flag = '99'. For a Variant LMK, the Issuer Private Key is encrypted under LMK 34-35. For a Key Block LMK, the Issuer Private Key must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'03'</td> <td>'R'</td> <td>'S', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'03'	'R'	'S', 'N'
Key Usage	Algorithm	Mode of Use						
'03'	'R'	'S', 'N'						
Delimiter	1 A	Optional Delimiter. Value ':'. Indicates the presence of the following 2 fields which allow a DAC to be calculated.						
If above Delimiter is present, the following 2 fields must be present:								
MKDAC	32 H or 'U' + 32 H or 'S' + n A	Issuer Master Key for Data Authentication Code. For a Variant LMK, the MKDAC is encrypted under LMK 28-29/4. For a Key Block LMK, the MKDAC must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'E3'</td> <td>'T'</td> <td>'B', 'X', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'E3'	'T'	'B', 'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E3'	'T'	'B', 'X', 'N'						
PAN/PSN	16 N	Concatenation of the rightmost 14 digits of the Primary Account Number and 2 digit Sequence Number for the card. Pad on left with zeroes if required. If the Sequence Number is not available it should be specified as '00'.						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'KN'.
Error Code	2 N	'00': No error '04': Invalid Private key flag '06': Invalid hash identifier '10': Parity error on MK DAC 'E8': Invalid Private key block 'E9': Invalid MK-DAC key block or a standard error code.
If Error Code = 'E8' or 'E9', the following field will be present:		
Additional Error Code	2 A	The key block specific error code
Signature Length	4 N	Length, in bytes, of the SDA signature.
Signature	n B	Calculated SDA signature.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Card RSA Key Set and Public Key Certificate

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Generate a Card RSA Key Set and create the requested Certificate for the Public Key signed by the Issuer's Private Key.

Alternatively, create the requested certificate using the provided Public Key, reformatting and exporting the associated Private Key as requested. The command will verify that the provided Public Key corresponds to the Private Key for the key pair. The Key Type of the Private Key provided must be set to 3 (ICC Key).

Notes: A Public Exponent of 65537 ($2^{16} + 1$) will be used unless another is specified. If a Public Exponent is supplied, it must be 3 or 65537; otherwise, an error will be returned by the HSM and no processing will take place. See *Card Issuing Appendix H – Private Key Encodings* for discussion on alternative Chinese Remainder Theorem output formats.

Compatibility Note: In this revision, Mode 1 has been changed and it **will not** be backwards compatible. Originally, this mode only required the Card Public Key and it now requires both the Card Public and Private keys so that the Private Key can be formatted as required by card personalization systems. Previously, there was no functionality in the HSM to provide the Card Private Key in the required format. This has now been addressed. In addition, the provided Card Public key will no longer require a MAC since the command will verify that the key corresponds to the provided Private Key.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'KO'.
Scheme ID	1 N	'0': Visa VSDC '1': Mastercard '2': American Express AEIPS V4.1 '3': JCB '4': Union Pay '5': Discover <i>The Scheme ID parameter is not used in the processing at this time. It is included for any future differentiations in the Schemes.</i>
Certificate Type	1 N	'0': Card Public Key Certificate '1': Card PIN Encipherment Public Key Certificate
Mode Flag	1 N	'0': Generate RSA Key Set and Certificate, using Strong Primes '1': Generate Certificate with provided Public Key and export the provided Private Key under the KEK in the requested format '2': Generate RSA Key Set and Certificate, using Standard Primes
RSA Key Mode Flag	1 N	Indicates the type of keys required '0': Keys with $q > p$ '2': Keys with $p > q$ <i>Note: For provided key sets, the command will verify the type of key provided and modify the key parameters to comply with this condition.</i>
If Mode Flag = '0' or '2', the following field must be present:		
Key Length	4 N	Modulus length in bits (must be a multiple of 8) minimum value = '0400', maximum value = '2040'.
The following fields must be present as noted below:		
Card Private Key Output format	2 N	Output format for Card Private Key:

		'03': Output in the form of 5 Chinese Remainder Theorem components CBC encrypted under the KEK. See <i>Card Issuing Appendix H – Private Key Encodings</i> '04': Output the private key exponent (d) and modulus (n) encrypted under the KEK. See <i>Card Issuing Appendix H – Private Key Encodings</i> for format description. '05': Output the private key in the form of 5 CRT components encrypted under the KEK (format 03) and also in private key exponent (d) and modulus (n) encrypted under the KEK (format 04).						
Delimiter	1 A	Value ';'. Optional; if present, the following field must also be present.						
Padding Mode	1 N	Only present if above Delimiter is present. '0': Append '00' padding if CRT component blocks, or private modulus and exponent blocks, require it to become a multiple of 8 bytes. <i>Note: This is the default for Exponent/Modulus format if Padding Mode is not present.</i> '1': For DES KEK, append either 4 byte (8000 0000) or 8 byte mandatory padding (8000 0000 0000 0000) to CRT components or private modulus and exponent so the result is a multiple of 8 bytes. For AES KEK, append either 4 byte (8000 0000), 8 byte (8000 0000 0000 0000), 12 byte (8000 0000 0000 0000 0000 0000) or 16 byte (8000 0000 0000 0000 0000 0000 0000 0000) mandatory padding to CRT components or private modulus and exponent so the result is a multiple of 16 bytes. <i>Note: This mode should only be used if the proper key sizes are used.</i> '2': Append mandatory single byte of '80' followed by '00' bytes, as required, to make CRT component blocks, or private modulus and exponent blocks, a multiple of 8 bytes. <i>Note: The default for CRT format, if Padding Mode is not present, is a single byte of 80 followed by 00 bytes to make a multiple of 8, ONLY IF, it is not already a multiple of 8.</i>						
KEK		The Key Encryption Key, used to encrypt the Card Private Key components.						
	32 H or 'U' + 32 H or 'T' + 48 H	For a Variant LMK, the KEK is encrypted under LMK 24-25/1.						
	or 'S' + n B	For a Key Block LMK, the KEK must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'54'</td> <td>'T', 'A'</td> <td>'B', 'E', 'D', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'54'	'T', 'A'	'B', 'E', 'D', 'N'
Key Usage	Algorithm	Mode of Use						
'54'	'T', 'A'	'B', 'E', 'D', 'N'						

If Card Private Key Output Format = '04' or '05', the following fields must be present as noted below:

Encrypt Mode	1 N	Mode used to encrypt the Card Private Exponent and Modulus and, if Key Output Format is 05, also the CRT components: '0': ECB mode '1': CBC mode
IV	8 B or 16 B	Initialisation Vector. Only present if Encrypt Mode = '1'. If KEK algorithm = 'A' and Encrypt Mode = '1', the IV will be 16 bytes otherwise 8 bytes.
Delimiter	1 A	Value ';'. Optional; if present, the following field must also be present.
Card Private Modulus and Private Exponent Length Bytes Mode	1 N	Only present if the previous delimiter was specified. NOTE: This option does not change the format of the encrypted Private Modulus and Private Exponent fields. It only controls whether the encrypted output data is preceded by clear length bytes. If neither this parameter nor the previous delimiter is present, no length bytes will be added in the output. '0': No length bytes are prepended to the encrypted private modulus and private exponent output fields (default). '1': Length bytes are prepended to the encrypted private modulus and private exponent output fields.
Length Bytes	1 N	The number of bytes that are used to specify the length of the key components before component encryption. See <i>Card Issuing Appendix H – Private Key Encodings</i> for format description. Valid entries are '0', '1' or '2'. If this value is zero then no length parameter must be present in the key component block output. For Card Private Key Output Format = '03', a length byte of '1' will automatically be used. (Applies to all key components – modulus, exponent, CRT components.)

If Mode Flag = '0' or '2', the following 3 fields must be present as noted below:

Card Public Exponent Length	4 N	Optional. Length, in bits, of the Card Public Exponent. Must be supplied if Card Public Exponent is present in command message.
-----------------------------	-----	---

Card Public Exponent	n B	Optional. If supplied, it must follow guidelines described in the command notes. If not supplied then a default exponent of 65537 will be used.						
Delimiter	1 A	Mandatory Delimiter. Value ':'.						
If Mode Flag = '1', the following 4 fields must be present as noted below:								
Card Private Key Length	4 N or 4 H	For a Variant LMK, this is the length of the Card Private Key field. For a Key Block LMK, this field is ignored and should be set to 'FFFF'.						
Card Private Key	n B or 'S' + n B	The Card Private Key. For a Variant LMK, the Card Private Key is encrypted under LMK 34-35. For a Key Block LMK, the Card Private Key must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'04'</td> <td>'R'</td> <td>'S', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'04'	'R'	'S', 'N'
Key Usage	Algorithm	Mode of Use						
'04'	'R'	'S', 'N'						
Delimiter	1 A	Mandatory Delimiter. Value ':'.						
Card Public Key	n B	Card Public Key, DER encoded (unsigned) in ASN.1 format (sequence of modulus and exponent)						
The following fields must be present as noted below:								
Hash Identifier	2 N	Identifier of algorithm used to hash data: '01': SHA-1						
Signature Identifier	2 N	Identifier of signature algorithm: '01': RSA						
Primary Account Number (PAN)	20 H	Application PAN data to be included in certificate. Data supplied is left justified and padded on the right with hex 'F's.						
Certificate Expiration Date	4 N	Expiration date of certificate in Month and Year (MMYY) format to be included in the certificate.						
Certificate Serial No.	6 H	Certificate tracking number to be included in the certificate.						
Data Length	3 N	Length, in bytes, of Static Authentication Data field. Only present if Certificate Type = '0'.						
Static Authentication Data	n B	Static authentication data. Only present if Certificate Type = '0'.						
Terminator	1 A	Mandatory Delimiter. Value ':'.						
Issuer Private Key Flag	2 N	Flag to indicate location of the Issuer's Private Key: If Flag = '99' use Private Key provided with command else Flag = index of stored Private Key.						
If Issuer Private Key Flag = '99', the following 2 fields must be present:								
Issuer Private Key Length	4 N or 4 H	For a Variant LMK, this is the length of the Issuer Private Key field. For a Key Block LMK, this field is ignored and should be set to 'FFFF'.						
Issuer Private Key	n B or 'S' + n B	The Issuer Private Key. For a Variant LMK, the Issuer Private Key is encrypted under LMK 34-35. For a Key Block LMK, the Issuer Private Key must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'03'</td> <td>'R'</td> <td>'S', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'03'	'R'	'S', 'N'
Key Usage	Algorithm	Mode of Use						
'03'	'R'	'S', 'N'						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'KP'.
Error Code	2 N	<p>'00': No error '04': Invalid Issuer Private Key Flag '05': Invalid Scheme ID, Cert. Type or Mode Flag '06': Invalid Hash or Signature Identifier '09': Invalid Length Bytes value '10': KEK Parity Error '52': Invalid private key output format '53': Invalid Encrypt Mode '54': Invalid Padding Mode '58': Mandatory padding does not result in multiple of 8 bytes '60': Invalid Private Modulus and Exponent Length Bytes Mode 'DA': KEK – key block error 'ED': Issuer Private Key – key block error or a standard error code.</p> <p>For Mode = '0' or '2' only:</p> <p>'03': Key Length error '07': Public exponent length error '08': Supplied public exponent value is not allowed '51': Invalid RSA Key Mode Flag</p> <p>For Mode = '1' only:</p> <p>'02': Public Key does not conform to encoding rules '55': Card Private Key Length error '56': Card Private Key error '57': Public key / Private key pair mismatch '59': Private Key provided is not Type 3 (ICC) 'E8': Card Private Key – key block error 'E9': Card Public Key – key block error</p>
If Error Code = 'DA', 'E8', 'E9' or 'ED', the following field will be present:		
Additional Error Code	2 A	The key block specific error code
If the Card Private Key Output format = '03' or '05', the following 6 fields will be present:		
Card Private Key Component Length	1 B	Length, in bytes, of each of the following 5 fields.
p (KEK)	n B	Prime p encrypted under the KEK.
q (KEK)	n B	Prime q encrypted under the KEK.
d1 (KEK)	n B	d1 = d mod (p-1) encrypted under the KEK.
d2 (KEK)	n B	d2 = d mod (q-1) encrypted under the KEK.
q-1 mod p (KEK)	n B	Modular inverse of q encrypted under the KEK.
If the Card Private Key Output format = '04' or '05', the following 2 or 4 fields will be present:		
Card Private Exponent Encrypted Length	2 B	Only present if Card Private Modulus and Exponent Length Bytes Mode = '1'. The length of the entire encrypted Private Exponent Block.
Card Private Key Exponent (KEK)	n B	Card Private Key component formatted in Private Key Exponent/Modulus format (see <i>Card Issuing Appendix H – Private Key Encodings</i> , encrypted under the KEK
Card Private Modulus Encrypted Length	2 B	Only present if Card Private Modulus and Exponent Length Bytes Mode = '1'. The length of the entire encrypted Private Modulus Block.
Card Private Key Modulus (KEK)	n B	Card Private Key modulus formatted in Private Key Exponent/Modulus format (see <i>Card Issuing Appendix H – Private Key Encodings</i> , encrypted under the KEK
The following fields will always be present:		
Card (ICC) Certificate length	2 H or 4 H	Length, in bytes, of the Card Certificate in the next field. If the Issuer Public Key modulus is less than 256, then this field will be of length 2 H. If the Issuer Public Key modulus is 256 or above, then this field will be of length 4 H.
Card (ICC) Certificate	n B	Signed Card Certificate. Refer to <i>Card Issuing Appendix G – Format of Card (ICC) Public Key Certificate</i> for format.

Field	Length & Type	Details
Card (ICC) Public Key Remainder length	2 H or 4 H	Length, in bytes, of the Card Public Key Remainder in the next field. May indicate zero if $N_{IC} \leq N_I - 42$. If the Card Public Key Remainder is less than 256, then this field will be of length 2 H. If the Card Public Key Remainder is 256 or above, then this field will be of length 4 H.
Card (ICC) Public Key Remainder	n B	Card Public Key Remainder. If the above field indicates zero length (because $N_{IC} \leq N_I - 42$), this field will not be present.
Card (ICC) Public Key Exponent Length	2 H or 4 H	Length, in bytes, of the Card Public Key Exponent in the next field. If the Card Public Key Exponent is less than 256, then this field will be of length 2 H. If the Card Public Key Exponent is 256 or above, then this field will be of length 4 H.
Card (ICC) Public Key Exponent	n B	Card Public Key Exponent.
Card (ICC) Public Key Modulus Length	4 H	Length, in bytes, of the Public Key Modulus in the next field.
Card (ICC) Public Key Modulus	n B	Card Public Key Modulus
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Notations:

N_I	=	Length of the Issuer Public Key Modulus
N_{IC}	=	Length of the Card (ICC) Public Key Modulus

Import a Certification Authority Self-Signed Certificate

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Variant LMK	Authorization: Required Activity: import.rsa.host
Key Block LMK	Authorization: Required Activity: import.02.host

Function: Validate a Certification Authority (CA) public key certificate and return the CA Public Key with its associated MAC and the certificate Expiration Date. For Mastercard, the function will also return the Certificate Serial Number and the Hash for verification of the transferred Public Key.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'KK'.
Scheme ID	1 N	'0': Visa VSDC '1': Mastercard '2': American Express AEIPS V4.1 '3': JCB '4': Union Pay '5': Discover
Certificate Length	4 N	Length, in bytes, of the CA Self-Signed Certificate.
CA Self-Signed Certificate	n B	CA Self-Signed Certificate comprised of the Clear Data and the CA Public Key Certificate. See the appropriate appendix, depending on Scheme ID: <ul style="list-style-type: none"> <i>Card Issuing Appendix L – Self Signed CA Public Key Certificate Format (Visa)</i> <i>Card Issuing Appendix M – Self Signed CA Public Key Certificate Format (Mastercard)</i> <i>Card Issuing Appendix N - Self Signed CA Public Key Certificate Format (American Express)</i>
Delimiter	1 A	Mandatory Delimiter. Value ';'.
Authentication Data	n A	Optional. Additional data to be included in the CA Public Key MAC calculation (must not include ';').
Delimiter	1 A	Only present if the previous field above is present. Delimiter. Value ';'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
If Key Block LMK, the following fields must be present:		
Delimiter	1 A	Value '#'.
Key Version Number	2 N	Key Version Number field, to be included in the key block header; permitted values: '00' to '99';
Exportability	1 A	Exportability field, to be included in the key block header; only permitted values are 'N', 'E' or 'S';

Field	Length & Type	Details
Number of Optional Blocks	2 N	Number of Optional Blocks specified below; permitted values '00' to '08'; must be present if the above Delimiter is present.
For each optional block, the following three fields must be specified. Note: if the Number of Optional Blocks = '00', then none of the following three fields should be present.		
Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
Optional Block Length	2 H	Number of characters in the optional block (including identifier and length); permitted values X'04 to X'FF; if value = X'04, then the following field is not present.
Optional Block Data	n A	Optional block data.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details						
RESPONSE MESSAGE								
Message Header	m A	Returned to the Host unchanged.						
Response Code	2 A	Value 'KL'.						
Error Code	2 N	'00': No error '05': Invalid Scheme ID '06': Invalid Hash or Signature algorithm indicator '07': Certificate Hash validation failure '08': Mismatch between common clear and signed certificate data '80': Certificate length error '81': Invalid Certificate Format (Header, Trailer or Format value) or a standard error code						
MAC	4 B	For a Variant LMK, the MAC on CA Public Key and Authentication Data calculated using LMK 36-37.						
CA Public Key	n B or 'S' + n B	The CA Public Key, protected by the LMK. For a Variant LMK, the CA Public Key, DER encoded (unsigned) in ASN.1 format (sequence of modulus and exponent). The CA Public Key will conform to the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'02'</td> <td>'R'</td> <td>'V'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'02'	'R'	'V'
Key Usage	Algorithm	Mode of Use						
'02'	'R'	'V'						
For Scheme ID = '0', '1', '2', '3', '4', the following field will be present:								
Certificate Expiration Date	4 N	Certificate Expiration Date (MMYY) recovered from the CA Public Key Certificate.						
For Scheme ID = '1' (Mastercard) the following 3 fields will be present (See <i>Card Issuing Appendix M – Self Signed CA Public Key Certificate Format</i> (Mastercard)):								
Certificate Serial Number	6 H	Certificate Serial Number recovered from the CA Public Key Certificate.						
Verification Hash Length	2 N	Length in hex characters of hash result in next field. This length will depend on the hash algorithm specified in the certificate. For SHA-1 this length will be 40.						
Verification Hash Value	n H	Hash for confirmation of CA Public Key transfer. (Includes ID of Certificate, Public Key Index, Modulus and Exponent)						
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.						
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.						

EMV Sign Data

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Generate a digital signature over a message, as defined in EMV Book 2, using an RSA Private Key. Return the encrypted message.

Notes: The message will not be padded and must be of the same size as the modulus length of provided Private Key or an error will be returned.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IK'.						
Mode Flag	1 N	'0': No formatting or padding of message data						
Signature Identifier	2 N	Identifier of signature algorithm: '01': RSA						
Message Length	4 N	Length, in bytes, of message data.						
Message Data	n B	Message data for signature						
Delimiter	1 A	Value ';'.						
Private Key Flag	2 N	Flag to indicate location of the Private key for signature: '00' ... '20': index of stored private key '99': use private key provided with command						
If Private Key Flag = '99', the following 2 fields must be present:								
Private Key Length	4 N or 4 H	For a Variant LMK, this is the length of the Private Key field. For a Key Block LMK, this field is ignored and should be set to 'FFFF'.						
Private Key	n B or 'S' + n B	The Private Key. For a Variant LMK, the Private Key is encrypted under LMK 34-35. For a Key Block LMK, the Private Key must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'03'</td> <td>'R'</td> <td>'S', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'03'	'R'	'S', 'N'
Key Usage	Algorithm	Mode of Use						
'03'	'R'	'S', 'N'						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IL'.
Error Code	2 A	<p>'00': No error '04': Invalid Private Key Flag '05': Invalid Mode Flag '06': Invalid Signature Identifier '27': Private Key / message length mismatch 'D1': Private Key – key block error or a standard error code</p>
If Error Code = 'D1', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
If Error Code = '00', the following 2 fields will be present:		
Message Length	4 N	Length, in bytes, of signed message data.
Message Data	n B	Signed message data.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

EMV Recover Data

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Recover message data from a digitally signed message, as defined in EMV Book 2, using an RSA Public Key. Return the decrypted message.

Notes: No verification, checking, or removal of padding, will be performed on the decrypted message data.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IM'.						
Mode Flag	1 N	'0': No formatting or padding of message data						
Signature Identifier	2 N	Identifier of signature algorithm: '01': RSA						
Message Length	4 N	Length, in bytes, of message data.						
Message Data	n B	Message data for signature						
Delimiter	1 A	Value ';'.						
Public Key MAC	4 B	Only present if using a Variant LMK. MAC on Public Key and Authentication Data calculated using LMK 36-37.						
Public Key	n B or 'S' + n B	Public Key, DER encoded (unsigned) in ASN.1 format (Sequence of modulus, exponent). For a Variant LMK, the Public Key, DER encoded (unsigned) in ASN.1 format (sequence of modulus and exponent). For a Key Block LMK, the Public Key must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'02'</td> <td>'R'</td> <td>'V', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'02'	'R'	'V', 'N'
Key Usage	Algorithm	Mode of Use						
'02'	'R'	'V', 'N'						
Authentication Data	n A	Only present if using a Variant LMK. Optional; additional data to be included in the Public Key MAC calculation (must not include ';').						
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IN'.
Error Code	2 A	<p>'00': No error '01': MAC verification failure '05': Invalid Mode Flag '06': Invalid Signature Identifier '08': Public Key does not conform to encoding rules 'D2': Public Key – key block error or a standard error code</p>
If Error Code = 'D2', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
If Error Code = '00', the following 2 fields will be present:		
Recovered Message Length	4 N	Length, in bytes, of the Recovered Message Data.
Recovered Message Data	n B	Recovered message data.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

10.3 MULTOS Card Data Preparation Commands

The HSM provides the following host commands to support the building of MULTOS Application Load Units (ALUs) and the associated key management:

Function	Command	Page
<i>Import MULTOS Transport Key Certifying Key</i>	I2 (I3)	579
<i>Import MULTOS Hash Modulus Key</i>	I4 (I5)	580
<i>Translate MULTOS KTU</i>	I6 (I7)	581
<i>MULTOS ALU Generator – Allocate ALU Area</i>	I8 (I9)	585
<i>MULTOS ALU Generator – Load Block</i>	I8 (I9)	586
<i>MULTOS ALU Generator – Load Clear Data</i>	I8 (I9)	587
<i>MULTOS ALU Generator – Load Cipher Data</i>	I8 (I9)	589
<i>MULTOS ALU Generator – Generate Checksum</i>	I8 (I9)	592
<i>MULTOS ALU Generator – Encrypt Area</i>	I8 (I9)	594
<i>MULTOS ALU Generator – Generate Signature</i>	I8 (I9)	596
<i>MULTOS ALU Generator – Generate KTU</i>	I8 (I9)	598
<i>MULTOS ALU Generator – Return ALU</i>	I8 (I9)	600
<i>MULTOS ALU Generator – Release ALU</i>	I8 (I9)	601

Import MULTOS Transport Key Certifying Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To import a MULTOS Transport Key Certifying Key (TKCK) from MULTOS format and return the public key in DER encoded ASN.1 format (TKCK_PK).

Notes: The exponent is always assumed to be 3.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'I2'
Mode Flag	1 N	Flag to indicate TKCK format '1': TKCK format (See <i>Card Issuing Appendix J – MULTOS Transport Key Certifying Key File Format</i>) <i>This field can be expanded in the future to accommodate other certificate types.</i>
TKCK Length	4 N	Length, in bytes, of the next field
TKCK	n B	MULTOS Transport Key Certifying Key
Delimiter	1 A	Value ';'
Authentication Data	n A	Optional. Additional data to be included in the Public Key MAC calculation (must not include ';')
Delimiter	1 A	Mandatory Delimiter. Value ';'.
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'I3'
Error Code	2 N	'00': No error '04': Invalid Mode Flag '05': TKCK format, data, or hash error '80': TKCK length error or a standard error code.
MAC TKCK_PK	4 B	MAC on Transport Key Certifying Key and authentication data, calculated using LMK 36-37
TKCK_PK	n B	Transport Key Certifying Key in ASN.1 DER encoded format
TKCK Identifier	4 H	TKCK Identifier
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Import MULTOS Hash Modulus Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To import a MULTOS Hash Modulus Key from MULTOS format and return the public key in DER encoded ASN.1 format.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'I4'
Mode Flag	1 N	Reserved. Must be 0.
Hash Modulus Length	4 N	Length, in bytes, of next field
Hash Modulus	n B	Hash Modulus. See <i>Card Issuing Appendix K – MULTOS Hash Modulus File Format</i> for format.
Delimiter	1 A	Value ';'
Public Exponent Length	4 N	Optional. Length, in bits, of the Public Exponent. Must be supplied if Public Exponent is present in command message.
Public Exponent	n B	Optional. If supplied then it must be odd; if not supplied then a default exponent of 3 will be used.
Delimiter	1 A	Mandatory Delimiter. Value ';'
Authentication Data	n A	Optional. Additional data to be included in the MAC calculation over the Hash Modulus (must not contain ';')
Delimiter	1 A	Mandatory Delimiter. Value ';'
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'I5'
Error Code	2 N	'00': No error '04': Invalid Mode Flag '05': Hash Modulus format, data, or hash error '07': Public exponent length error '08': Invalid public exponent '80': Hash Modulus Length error or a standard error code.
MAC	4 B	MAC on Hash Modulus key and authentication data, if supplied, calculated using LMK 36-37
Hash Modulus	n B	Hash Modulus Key in ASN.1 DER encoded format
Hash Modulus Identifier	4 H	Hash Modulus Identifier
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate MULTOS KTU

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To translate a Key Transformation Unit (KTU Prime) from encryption under a Key Encryption Key (KEK) to the standard MULTOS KTU format encrypted under either an RSA public key or diversified key (Step One).

Notes:

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value '16'
Version Flag	1 N	Flag to indicate MULTOS version: '0': MULTOS v3.0 '1': MULTOS v4.0 '2': MULTOS v4.0 with hash verification '3': MULTOS Step One
KEK	'U' + 32 H or 'T' + 48 H	KEK encrypted under LMK 24 25/1.
KTU Length	3 N	Length, in bytes, of next field (maximum of 256)
KTU Prime	n B	KTU encrypted under the KEK
Delimiter	1 A	Value ','
If Version Flag = 0, 1 or 2, the following 7+4 fields must be present:		
Tkck_pk MAC	4 B	MAC on Transport Key Certifying Key, and optional authentication data, calculated using LMK 36-37
tkck_pk	n B	Transport Key Certifying Key in ASN.1 DER encoded format.
TKCK_PK Authentication Data	n A	Optional. Additional data included in the MAC calculation (must not include ',')
Delimiter	1 A	Mandatory Delimiter. Value ','
MCD_PK_C Length	3 N	Length, in bytes, of the next field
MCD_PK_C	n B	Card Public Key Certificate (see <i>Card Issuing Appendix I – MULTOS Card Public Key Certificate Format</i>)
Delimiter	1 A	Value ','
If Version Flag = 2, the following 4 fields must be present:		
Hash Modulus MAC	4 B	MAC on Hash Modulus, and optional authentication data, calculated using LMK 36-37
Hash Modulus	n B	Hash Modulus Key, in ASN.1 DER encoded format
Hash Modulus Authentication Data	n A	Optional; additional data included in the MAC calculation (must not include ',')
Delimiter	1 A	Mandatory Delimiter. Value ','
If Version Flag = 3, the following field must be present:		
MK-KE	'U' + 32 H or 'T' + 48 H	The Master KTU Encipherment key encrypted under LMK 24-25/8.
Enablement_Data_Production_Date	1 B	Date on which Enablement Data for the target card was created. The byte corresponds to the number of months since January 1998.
MCD_NO	8 B	MCD Number for the KTU
MCD_ID	6 B	MCD ID used to generate diversified key.
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.

payShield 10K Core Host Commands

LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'I7'
Error Code	2 N	<p>'00': No error</p> <p>'01': TKCK MAC verification failure</p> <p>'04': Invalid ALU Identifier</p> <p>'07': TKCK_PK does not conform to encoding rules</p> <p>'08': Invalid TKCK_PK length</p> <p>'09': KTU Prime length error</p> <p>'10': KEK parity error</p> <p>'11': MK-KE parity error</p> <p>'50': Hash Modulus does not conform to encoding rules</p> <p>'51': Hash Modulus MAC verification failure</p> <p>'52': Card Certificate Hash validation failure</p> <p>'53': Card Public Key modulus length mismatch</p> <p>'54': Invalid KTU header</p> <p>'55': KTU too long for Card Public Key</p> <p>'56': TKCK_PK – MCD_PK ≥ 56</p> <p>'80': MCD_PK_C length error</p> <p>or a standard error code.</p>
KTU Length	3 N	Length in bytes of the next field
KTU	n B	Standard MULTOS KTU, encrypted under the smart card RSA public key
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

MULTOS ALU Generator - Introduction

The MULTOS ALU Generator function consists of a series of sub commands (described in the following sections) in the I8 command which are used in the appropriate sequence to generate unprotected, protected, or confidential MULTOS Application Load Units (ALUs).

Typical sequencing of sub-commands to build an ALU for an EMV application would be as follows:

Sub Command	Description
<u>Allocate ALU Area</u>	Create an initialized ALU Area
<u>Load Block (Code)</u>	Load application code into ALU Code Block
<u>Load Block (FCI)</u>	Load FCI data into ALU FCI Block
<u>Load Block (DIR)</u>	Load DIR data into ALU DIR Block
<u>Load Block (Data)</u>	Load static application data in ALU Data Block
<u>For each card:</u>	
<u>Load Clear Data (TLV)</u>	<i>Load personalized data items into ALU Data Block</i>
<u>Load Cipher Data (PIN)</u>	<i>Load enciphered PIN into ALU</i>
<u>Load Cipher Data (DES Key)</u>	<i>Load enciphered EMV UDKs into ALU</i>
<u>Load Cipher Data (RSA key)</u>	<i>Load EMV ICC RSA private keys into ALU</i>
<u>Generate Checksum ()</u>	<i>Generate checksums over data areas</i>
<u>Encrypt Area ()</u>	<i>Encipher areas under KTU keys</i>
<u>Generate Signature ()</u>	<i>Sign or MAC the ALU (protected ALU)</i>
<u>Generate KTU ()</u>	<i>Encipher KTU under card key (confidential ALU)</i>
<u>Return ALU ()</u>	<i>Return completed ALU to host</i>
<u>Release ALU Area ()</u>	<i>Delete ALU and release work areas</i>

The generic structure of the I8 command is described in the following table. The parameters, error codes, and returned data peculiar to each sub command are described in the subsequent sections on each sub-command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'I8'
Sub Command Code	2 N	'01': Allocate ALU Area '02': Load Block '03': Load Clear Data '04': Load Cipher Data '05': Not used. Reserved '06': Generate Checksum '07': Encrypt Area '08': Generate Signature '09': Generate KTU '10': Return ALU '11': Release ALU Area
Sub Command parameters are defined in the sections below.		
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'I9'
Error Code	2 N	'00': No error '02': Invalid sub command value or a specific subcommand error code or a standard error code.
Refer to sections below for error codes and parameters returned by each Sub Command Code		
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

MULTOS ALU Generator – Allocate ALU Area

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Initial command to allocate and lock a memory block for building the Application Load Unit. All subsequent subcommands reference this block using an ALU identifier. The memory block is released using the Release ALU Area sub command. Multiple ALU areas can be assigned and individually referenced using the identifier.

Notes: If the ALU Identifier has already been used or there is not enough memory available to assign to an ALU area, an error will be returned.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'I8'
Sub Command Code	2 N	'01': Allocate ALU Area
ALU Identifier	8 A	Unique identifier for allocated ALU area
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'I9'
Error Code	2 N	'00': No error '02': Invalid sub command value '04': Invalid ALU Identifier (identifier already in use) '06': Memory allocation error or a standard error code.
Assigned ALU Areas	2 N	Total number of assigned ALU areas, including this one. Note: This parameter is returned even if Error Code 06 is returned, except it will only contain the number of ALU areas already allocated.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

MULTOS ALU Generator – Load Block

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: This sub-command is used to load initialised or static blocks into the ALU prior to personalisation, for example Code, FCI and DIR blocks. A default Data Block may also be loaded which can then be personalised for each card using the Load Clear Data and Load Cipher Data sub commands.

Notes: The Data Block loaded by this function will be saved and used to re-initialize the Data Block area when the completed ALU is returned so that multiple ALUs can be built using a common data template. See Release ALU sub-command for additional details. The loading of a Data Block will clear all activities on a previously loaded Data Block.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'I8'
Sub Command Code	2 N	'02': Load Block
ALU Identifier	8 A	Unique identifier for allocated ALU area
Block Type	1 N	Type of block being loaded '1': DIR '2': FCI '3': Code '4': Data
Block Length	4 H	Length of Block Data
Block Data	n B	Block Data to load into ALU
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'I9'
Error Code	2 N	'00': No error '02': Invalid sub command value '03': Illegal operation, specified ALU is in use '04': Invalid ALU Identifier (identifier not known) '05': Invalid Block Type '06': Memory allocation error or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

MULTOS ALU Generator – Load Clear Data

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: This sub command is used to personalise data elements in the Data, FCI or DIR blocks. The data elements personalised with this function are only clear data elements. Enciphered data elements, such as PINs and Keys, are loaded using the Load Cipher Data sub command.

Notes: If the Block Type is = 4 and the clear data is being loaded over any part of cipher data which has already been loaded, or the Encrypt Area sub command has been executed over any part of the Data Block, this sub command will return an error.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value '18'
Sub Command Code	2 N	'03': Load Clear Data
ALU Identifier	8 A	Unique identifier for allocated ALU area
Block Type	1 N	Type of block being loaded '1': DIR '2': FCI '4': Data
Offset	4 H	Indicates the offset from the start of the Block (Note: An offset of 0 indicates the first byte in the Block)
Data Length	4 H	Length of next field
Data	n B	Data to load at Offset
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'I9'
Error Code	2 N	<p>'00': No error '02': Invalid sub command value '03': Illegal operation, specified ALU is in use '04': Invalid ALU Identifier (identifier not known) '05': Invalid Block Type '06': Memory allocation error '07': Data range error, exceeds maximum block length '09': Illegal operation, clear data overlaps loaded cipher data or encryption of Data Block has already started or a standard error code.</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

MULTOS ALU Generator – Load Cipher Data

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: This sub command is used to personalise enciphered data elements in the Data block, for example PINs and Keys. Clear data elements are loaded using the Load Clear Data sub command.

Input for the different types of enciphered data elements in this command needs to be in the following formats:

PIN blocks encrypted under ZPK (formats will not be checked)

Use Translate PIN commands JG (LMK to ZPK) or CC (ZPK to ZPK)

Triple DES keys encrypted under a KEK

Use Derive Card Unique DES Keys command (KI)

RSA keys as 5 CRT components encrypted under a KEK

Use Generate Card RSA Key Set and Public Key Certificate command (KO)

Data encrypted under a DEK using ECB or CBC format

Use Encrypt Data Block command 'M0'

Notes: For CRT components, the function will remove any length and padding bytes from the components and puts them in the specified location as defined by the Component Placement Flag.

If the Encrypt Area sub command has been executed over any part of the Data Block, this sub command will return an error.

Compatibility Note: In this revision, parameters for Cipher Data Type = '3' have been changed and it will not be backwards compatible. Previously, there was no "Length Bytes" parameter in the command message and therefore it was not possible to remove it, or the padding, from the CRT components. This has now been addressed.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'I8'
Sub Command Code	2 N	'04': Load Cipher Data
ALU Identifier	8 A	Unique identifier for the ALU to receive the data.
Block Type	1 N	Reserved, Must be 4.
Cipher Data Type	1 N	'1': PIN Block encrypted under ZPK '2': Triple DES Key encrypted under KEK '3': RSA private key in CRT format encrypted using CBC under KEK (See <i>Card Issuing Appendix H – Private Key Encodings</i>) '4': Data ECB or CBC encrypted under DEK '5': RSA private key in CRT format encrypted using ECB under KEK (See <i>Card Issuing Appendix H – Private Key Encodings</i>)
Encryption Key	'U' + 32 H or 'T' + 48 H	Encryption Key encrypted under the appropriate LMK. KEK encrypted under LMK 24-25/1. ZPK encrypted under LMK 06-07. DEK encrypted under LMK 32-33.

Field	Length & Type	Details
Offset	4 H	Indicates the offset from the start of the Data Block (Note: An offset of 0 indicates the first byte in the block)
If Cipher Data Type = '1', the following field must be present:		
PIN Block	16 H	PIN block encrypted under the ZPK
If Cipher Data Type = '2', the following 2 fields must be present:		
DK (KEK)	'X' + 16 B	The derived unique key encrypted under the KEK
Atalla Variant	1 / 2 N	Optional. Only required if DK was encrypted under the KEK with Atalla variant
If Cipher Data Type = '3' or '5', the following 8 fields must be present:		
Private Key Component Length	1 B	Length, in bytes, of each of the following 5 fields.
p (KEK)	n B	Prime p encrypted under KEK using triple DES.
q (KEK)	n B	Prime q encrypted under KEK using triple DES.
d1 (KEK)	n B	d1 = d mod (p-1) encrypted under KEK using triple DES.
d2 (KEK)	n B	d2 = d mod (q-1) encrypted under KEK using triple DES.
q-1 mod p (KEK)	n B	Modular inverse of q encrypted under KEK using triple DES.
Length Bytes	1 N	Number of bytes used to specify the length of the key component in the field. See <i>Card Issuing Appendix J – MULTOS Transport Key Certifying Key File Format</i> for format description. Valid entries are 0, 1 or 2. If this value is zero the component will be expected to have mandatory padding consisting of a single byte of '80' followed by '00' bytes, as required, to make the CRT component block a multiple of 8 bytes.
Component Placement Flag	1 N	'0': Decrypted components will be concatenated in the following order - d1, d2, p, q, q-1 mod p. '1': Decrypted components will be concatenated in the following order - d1, d2, p, q, q-1 mod p - with p, q and q-1 mod p shifted as a block, if necessary, to begin on an 8 byte boundary with binary 0s filling any vacated space
If Cipher Data Type = '4', the following 4 fields must be present:		
Encryption Mode	1 N	'0': ECB '1': CBC
IV	16 H	Only present if Encryption Mode = 1 IV value
Message Length	4 H	Length of the following field in bytes
Encrypted Message	n B	Data encrypted under the DEK
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

payShield 10K Core Host Commands

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'I9'
Error Code	2 N	<p>'00': No error '02': Invalid sub command value '03': Illegal operation, specified ALU is in use '04': Invalid ALU Identifier (identifier not known) '05': Invalid Block Type or Cipher Data Type '06': Memory allocation error '07': Data range error, exceeds maximum block length '08': Invalid Component Placement Flag or Encryption Mode '09': Illegal operation, encryption of Data Block has already started '10': Encryption Key Parity Error '11': DK Parity Error '50': Invalid CRT component length byte contents '51': Invalid CRT component padding characters '80': CRT components, or Encrypted Message, length error or a standard error code.</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

MULTOS ALU Generator – Generate Checksum

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: This sub command calculates a MULTOS checksum over sections of the Data Block. Checksums may be computed over plain text areas and areas that contain deciphered elements such as PINs and Keys. This command is usually called once the Data section has been personalised.

Notes: Checksums generated over data loaded using the Load Cipher Data sub command will require encryption if the '*Protect MULTOS Cipher Data Checksums*' HSM security setting is set to 'Yes'. If encryption is not required (parameter set to 'No'), checksum calculations must encompass at least the entire data type that was loaded (PIN, Key, etc.) with the Load Cipher Data sub command. An error will be returned if a checksum is to be generated over partial PINs, Keys, etc.

Unprotected checksums generated over sensitive data such as PIN, Keys, etc. can present a security risk. It is strongly recommended that such checksums be encrypted.

If the Encrypt Area sub command has been executed over any part of the Data Block, this sub command will return an error.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'I8'
Sub Command Code	2 N	'06': Generate Checksum
ALU Identifier	8 A	Unique identifier for the ALU to carry out the operation.
Block Type	1 N	Reserved, Must be 4.
Offset	4 H	Indicates the offset from the start of the Data Block to the start the checksum operation. (Note: An offset of 0 indicates the first byte in the block)
Length	4 H	Number of bytes over which to calculate the checksum.
Checksum Method	1 N	'1': Standard MULTOS checksum.
Checksum IV	8 H	Initial Value for checksum process. Should be set to 0x5AA55AA5 as defined by MULTOS.
Checksum Result Offset	4 H	Indicates offset from the start of the Data Block for placing the calculated 4 byte checksum value (Note: An offset of 0 indicates the first byte in the block)
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'I9'
Error Code	2 N	'00': No error '02': Invalid sub command value '03': Illegal operation, specified ALU is in use '04': Invalid ALU Identifier (identifier not known) '05': Invalid Block Type or Checksum Method '07': Data range error, exceeds block length '08': Checksum result range error, exceeds block length '09': Illegal operation, checksum over partial cipher data, or encryption of Data Block has already started or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

MULTOS ALU Generator – Encrypt Area

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: This sub command is used to encrypt areas of the Data Block that contain cryptographic data elements such as PINs and Keys that have been loaded using the Load Cipher Data sub command or checksums created using the Generate Checksum sub command if protected checksums are required. This command also creates Area Descriptors that define the encrypted areas for inclusion in the KTU.

Notes: The use of Encryption Methods '01' and '03' require that the '*Enable Single-DES*' HSM security setting be set to "YES" or the sub command will return an error.

All data should be loaded and checksums generated before executing the Encrypt Area sub command. Once this command is executed on any area of the Data Block, the loading of clear or cipher data (sub commands 4 and 5) or the generation of checksums (sub command 6) will be prohibited.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'I8'
Sub Command Code	2 N	'07': Encrypt Area
ALU Identifier	8 A	Unique identifier for the ALU to carry out the operation.
Block Type	1 N	Reserved, Must be 4.
Offset	4 H	Indicates the offset from the start of the Data Block to start the encryption operation. (Note: An offset of 0 indicates the first byte in the block)
Length	4 H	Number of bytes to encrypt. Minimum length is 8 bytes. Must be a multiple of 8 bytes.
Encryption Method	2 N	'01': DES-1 CBC with single length DES key (using decrypt operation) '02': Triple DES-1 CBC with double length DES key (using decrypt, decrypt, decrypt operations) The following settings should only be used for StepOne. '03': DES CBC with single length DES key '04': Triple DES CBC with double length DES key
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'I9'
Error Code	2 N	<p>'00': No error '02': Invalid sub command value '03': Illegal operation, specified ALU is in use '04': Invalid ALU Identifier (identifier not known) '05': Invalid Block Type '07': Data range error, exceeds block length '08': Invalid Encryption Method '80': Invalid Length or a standard error code.</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

MULTOS ALU Generator – Generate Signature

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

- Function:** This sub-command is required for protected ALUs and generates a signature over the Application Unit using either the Application Provider Private Key or the Application Signature Key (for Step One). The signature is generated after sensitive data elements in the Data Block have been encrypted using the Encrypt Area sub command.
- Notes:** If there are any unprotected data elements remaining in the Data Block (loaded with Load Cipher Data sub command or generated with the Generate Checksum sub command, when protected checksums are required, but not subsequently protected using the Encrypt Area sub command), this command will not generate a signature and will return an error.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'I8'
Sub Command Code	2 N	'08': Generate Signature
ALU Identifier	8 A	Unique identifier for the ALU to carry out the operation.
Version Flag	1 N	Flag to indicate MULTOS version: '0': MULTOS v3.0 '1': MULTOS v4.0 '3': MULTOS Step One
If Version Flag = '0' or '1', the following 8 fields must be present:		
Private Key Flag	2 N	Flag to indicate location of the Private Key; '00' ... '98': index of stored private key '99': use private key provided with command.
Private Key Length	4 N	Optional. Must be present if Private key flag = '99' Length in bytes of the following field
Application Provider Private Key	n B	Optional. Must be present if Private key flag = '99' Private key encrypted under LMK 34-35
Hash Algorithm	1 N	'1': MULTOS Asymmetric Hash This field can be expanded in the future to accommodate other Hash types.
If Hash Algorithm = '1', the following 4 fields must be present:		
Hash Modulus MAC	4 B	MAC on Hash Modulus key and optional authentication data calculated using LMK 36-37.
Hash Modulus	n B	Hash Modulus Key in ASN.1 DER encoded format.
Hash Modulus Authentication Data	n A	Optional; additional data included in MAC calculation (must not include ';')
Delimiter	1 A	Mandatory Delimiter. Value ':'
If Version Flag = '3', the following 3 fields must be present:		
MK-AS	'U' + 32 H or 'T' + 48 H	The Master Application Signature (MAC) key encrypted under LMK 24-25/9.
Key Diversification Flag	1 N	'0': MAC generated using MK-AS '1': MAC generated using diversified key
MCD_ID	6 B	Only present if Key Diversification Flag = 1 MCD ID used to generate diversified key.
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.

payShield 10K Core Host Commands

Field	Length & Type	Details
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value '19'
Error Code	2 N	<p>'00': No error '02': Invalid sub command value '03': Illegal operation, specified ALU is in use '04': Invalid ALU Identifier (identifier not known) '05': Invalid Version Flag '06': Memory allocation error '07': Invalid Hash Algorithm or Key Diversification Flag '08': Invalid Private Key Flag '09': Illegal signature over unprotected sensitive data '11': MK-AS parity error '50': Hash Modulus does not conform to encoding rules '51': Hash Modulus MAC verification failure or a standard error code.</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

MULTOS ALU Generator – Generate KTU

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: This sub-command is used to generate the Key Transformation Unit for confidential ALUs. The command can generate KTUs encrypted under the specific Card Public key or a KTU Prime encrypted under a temporary key if the target card is unknown. The Translate KTU command may be used to translate from KTU Prime to a card specific KTU once the target card is known.

Notes: If there are any unprotected data elements remaining in the Data Block (loaded with Load Cipher Data sub command or generated with the Generate Checksum sub command, when protected checksums are required, but not subsequently protected using the Encrypt Area sub command), this command will not generate a KTU and will return an error.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'I8'
Sub Command Code	2 N	'09': Generate KTU
ALU Identifier	8 A	Unique identifier for the ALU to carry out the operation.
KTU Type	1 N	'1': KTU Prime, encryption under KEK '2': KTU, encryption under the card public key '3': KTU, encryption under a diversified key (Step One).
Version Flag	1 N	Flag to indicate MULTOS version: '0': MULTOS v3.0 '1': MULTOS v4.0 '2': MULTOS v4.0 with hash verification
Application ID	17 B	Application Identifier consisting of the AID length (1 byte) followed by the AID (n bytes) and padding (0xFF bytes to fill 17 bytes).
If KTU Type = '1', the following field must be present:		
KEK	'U' + 32 H or 'T' + 48 H	KEK encrypted under LMK 24 25/1.
If KTU Type = '2', the following 12 fields must be present:		
Tkck_pk MAC	4 B	MAC on Transport Key Certifying Key, and optional authentication data, calculated using LMK 36-37.
tkck_pk	n B	Transport Key Certifying Key in ASN.1 DER encoded format.
TKCK_PK Authentication Data	n A	Optional. Additional data included in the MAC calculation (must not include ';')
Delimiter	1 A	Mandatory Delimiter. Value ';'
MCD_PK_C Length	3 N	Length, in bytes, of the next field
MCD_PK_C	n B	MULTOS Card Public Key Certificate (See <i>Card Issuing Appendix I – MULTOS Card Public Key Certificate Format</i>)
Delimiter	1 A	Value ';'
If Version Flag = '2', the following 4 fields must be present:		
Hash Modulus MAC	4 B	MAC on Hash Modulus, and optional authentication data, calculated using LMK 36-37.
Hash Modulus	n B	Hash Modulus Key, in ASN.1 DER encoded format
Hash Modulus Authentication Data	n A	Optional; additional data included in the MAC calculation (must not include ';')
Delimiter	1 A	Mandatory Delimiter. Value ';'.

Field	Length & Type	Details
If KTU Type = 3, the following 3 fields must be present:		
MK-KE	'U' + 32 H or 'T' + 48 H	The Master KTU Encipherment key encrypted under LMK 24-25/8.
Enablement_Data_Production_Date	1 B	Date on which Enablement Data for the target card was created. The byte corresponds to the number of months since January 1998.
MCD_NO	8 B	MCD Number for the KTU
MCD_ID	6 B	MCD ID used to generate diversified key.
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'I9'
Error Code	2 N	'00': No error '01': TKCK MAC verification failure '02': Invalid sub command value '03': Illegal operation, specified ALU is in use '04': Invalid ALU Identifier (identifier not known) '05': Invalid KTU Type or Version Flag '06': Memory allocation error '07': TKCK_PK does not conform to encoding rules '08': No Area Descriptors defined '09': Unprotected sensitive data remains in Data Block '10': KEK parity error '11': MK-KE parity error '50': Hash Modulus does not conform to encoding rules '51': Hash Modulus MAC verification failure '52': Card Certificate Hash validation failure '53': Invalid TKCK_PK length '54': Card Public Key modulus length mismatch '55': KTU too long for Card Public Key '56': TKCK_PK – MCD_PK ≥ 56 '80': MCD_PK_C length error or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

MULTOS ALU Generator – Return ALU

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: This sub command returns the completed ALU to the Host.

It will then delete the internal Signature and KTU areas, if present, and re-initialize the Data Block area to the last one loaded using the Load Block sub command in case that a new ALU based on the same common data needs to be created.

Notes: If there are any unprotected data elements remaining in the Data Block (loaded with Load Cipher Data sub command or generated with the Generate Checksum sub command, when protected checksums are required, but not subsequently protected using the Encrypt Area sub command), or if Area Descriptors have been generated with the Encrypt Data sub command and a KTU has not been created, this command will return an error and no further processing will take place.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'I8'
Sub Command Code	2 N	'10': Return ALU
ALU Identifier	8 A	Unique identifier for the ALU to be returned.
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'I9'
Error Code	2 N	'00': No error '02': Invalid sub command value '03': Illegal operation, specified ALU is in use '04': Invalid ALU Identifier (identifier not known) '08': KTU has not been created and protected '09': Unprotected sensitive data remains in ALU or a standard error code.
ALU Length	4 H	Length of the ALU
ALU	n B	The completed Application Load Unit
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

MULTOS ALU Generator – Release ALU

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: This sub command releases the allocated memory and frees all allocated resources created during the ALU Generator command.

Notes: It is the responsibility of the calling application to de-allocate all ALU areas once the completed ALU(s) has been successfully retrieved.

A method is provided to clear all ALU areas in case the application has lost track of ALU Identifiers and cannot individually clear them. If the ALU Identifier "ClearAll" (case insensitive) is used in this sub-command, all ALU areas will be released **except** for any ALU areas currently being worked on by another sub-command. This case will only occur in multi-threaded applications where other threads are actively working on ALUs. It is recommended that the "ClearAll" method is only used when there is no work currently taking place on ALUs in order to prevent unexpected release of ALUs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'I8'
Sub Command Code	2 N	'11': Release ALU
ALU Identifier	8 A	Unique identifier for the ALU to release.
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'I9'
Error Code	2 N	'00': No error '02': Invalid sub command value '03': Illegal operation, specified ALU is in use '04': Invalid ALU Identifier (identifier not known) or a standard error code.
Assigned ALU Areas	2 N	Total number of remaining assigned ALU areas.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

10.4 Chip Card Personalization Commands

The HSM provides the following host commands to support the secure operations required for general purpose card personalization:

Function	Command	Page
<i>Establish Secure Session with Chip Card</i>	IC (ID)	603
<i>Prepare Secure Message for Chip Card</i>	IE (IF)	610
<i>Verify and Decrypt Response Secure Message from Chip Card</i>	II (IJ)	617

Establish Secure Session with Chip Card

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Support the establishment of a secure session with a chip card, using mutual authentication, based on the EMV Common Personalization Specification (CPS) and Global Platform (GP).

The following protocols are supported:

Secure Channel Protocol 02 (SCP02) "i" = 0x15

Secure Channel Protocol 02 (SCP02) "i" = 0x55

Support for the specific process for Mastercard PayPass Magnetic Stripe Cards

Support for static personalization method where the card application is personalized with a single Personalisation Secret Key (PSK).

Secure Channel Protocol 03 (SCP03)

Notes: There are two methods under EMV CPS and GP SCP02 that can be used to establish a secure personalization channel with the card application as described below.

Indirect (Explicit) Method:

In this method, the Data Preparation Process does not need to have knowledge of the process used to establish a secure personalization session with a chip card. Therefore, two security zones exist in this process - a security zone between the Data Preparation Process and the Personalization Process and another security zone between the Personalization Process and the chip card.

The Personalization Process establishes a secure session with the chip card by issuing the INITIALISE UPDATE and EXTERNAL AUTHENTICATE commands. Through this process, the session keys and cryptograms required to establish a secure session with a chip card are generated.

Direct (Implicit) Method:

This method is not supported at this time.

For the above methods, this function uses the provided INITIALISE UPDATE responses to generate the data for the EXTERNAL AUTHENTICATE command, as well as derive the keys needed for personalization of the chip card. The keys are returned encrypted under the LMK for use by the Prepare Secure Message for Chip Card command. The Global Platform specific options for Security Level which include the use of an R-MAC are also supported. If an option which includes an R-MAC is defined, the R-MAC key will also be derived and returned encrypted under the LMK. This key will be handled as a 'ZAK' so that messages from the chip card can be validated using the "Verify MAC" command in the HSM.

For the Mastercard PayPass Magnetic Stripe method, the function will only derive the KD Personalization Key which will be used for authenticating messages to the card and securing sensitive data. The key is returned encrypted under the LMK for use by the Prepare Secure Message for Chip Card command.

C-MAC is a MAC generated by the Host over the APDU command message.

R-MAC is a MAC generated by the Card over the APDU response message.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IC'.						
Secure Channel Method	1 N	<p>'0': Indirect (Explicit) initiation of secure channel by the personalization system, with Card Keys derived from KMC. (Global Platform SCP02 "i" = 0x15 method).</p> <p>'1': Indirect (Explicit) initiation of secure channel by the personalization system, with Card Keys provided in the command. (Global Platform SCP02 "i" = 0x15 method).</p> <p>'2': Mastercard PayPass Magnetic Stripe Cards. Perso Key derived from KMC.</p> <p>'4': Indirect (Explicit) initiation of secure channel by the personalization system, with Card Keys derived from KMC. (Global Platform SCP02 "i" = 0x55 method).</p> <p>'5': Indirect (Explicit) initiation of secure channel by the personalization system, with Card Keys provided in command. (Global Platform SCP02 "i" = 0x55 method).</p> <p>'6': Indirect (Explicit) initiation of Open Platform secure channel by the personalization system using a single personalization key PSK. (Static authentication method).</p> <p>'7': Secure Channel Protocol 03 (SCP03)</p>						
If Secure Channel Method = '6' or '7', the following field will be present:								
Card Key Generation Mode	1 N	<p>'0': Card key(s) derived from master KMC key (not valid for Secure Channel Method '7')</p> <p>'1': Card keys provided in command</p>						
If Secure Channel Method = '0', '2' or '4', or if Secure Channel Method = '6' and Card Key Generation Mode = '0', the following 2 fields must be present:								
KMC	<p>32 H or 'U' + 32 H or 'T' + 48 H</p> <p>or 'S' + n A</p>	<p>The Master Personalization Key.</p> <p>For a Variant LMK, the KMC is encrypted under LMK 24-25/2.</p> <p>For a Key Block LMK, the KMC must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'E7'</td><td>'T'</td><td>'X', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'E7'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'E7'	'T'	'X', 'N'						
Derivation Data	<p>6 B</p> <p>16 B</p>	<p>Data used to generate the card static diversified keys.</p> <p>If Secure Channel Method is '0' or '4', these are the 6 least significant bytes of KEYDATA typically from the response to an INITIALISE UPDATE command to the card. If Secure Channel Method is 2, this field is ignored and set to 6 bytes of 0x00.</p> <p>If Secure Channel Method is '6', this will be the 16 byte PSK derivation data.</p>						
If Secure Channel Method = '1' or '5', the following 3 fields must be present:								
CK-ENC	<p>'U' + 32 H or 'T' + 48 H</p> <p>or 'S' + n A</p>	<p>Card Key for encryption session key generation.</p> <p>For Variant LMK, the CK-ENC encrypted under LMK 36-37/3.</p> <p>For a Key Block LMK, the CK-ENC must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'37'</td><td>'T'</td><td>'X', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'37'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'37'	'T'	'X', 'N'						
CK-MAC	<p>'U' + 32 H or 'T' + 48 H</p> <p>or 'S' + n A</p>	<p>Card Key for integrity session key generation.</p> <p>For Variant LMK, the CK-MAC is encrypted under LMK 36-37/4.</p> <p>For a Key Block LMK, the CK-MAC must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'38'</td><td>'T'</td><td>'X', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'38'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'38'	'T'	'X', 'N'						
CK-DEK	<p>'U' + 32 H or 'T' + 48 H</p> <p>or 'S' + n A</p>	<p>Card Key for card data encryption session key generation.</p> <p>For Variant LMK, the CK-DEK is encrypted under LMK 36-37/5.</p> <p>For a Key Block LMK, the CK-DEK must comply with the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'39'</td><td>'T'</td><td>'X', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'39'	'T'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'39'	'T'	'X', 'N'						
If Card Key Generation Method = '1', the following 3 fields must be present:								

Field	Length & Type	Details						
PSK	'U' + 32 H or 'S' + n A	Only present if Secure Channel Method = '6'. The Personalisation System Key. For a Variant LMK, the PSK is encrypted under LMK 24-25/5. For a Key Block LMK, the PSK must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'40'</td><td>'T'</td><td>'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'40'	'T'	'N'
Key Usage	Algorithm	Mode of Use						
'40'	'T'	'N'						
CK-ENC	'S' + n A	Only present if Secure Channel Method = '7'. Card Key for cryptograms. The CK-ENC must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'37'</td><td>'A'</td><td>'X'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'37'	'A'	'X'
Key Usage	Algorithm	Mode of Use						
'37'	'A'	'X'						
CK-MAC	'S' + n A	Only present if Secure Channel Method = '7'. Card Key for authentication. The CK-MAC must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'38'</td><td>'A'</td><td>'X'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'38'	'A'	'X'
Key Usage	Algorithm	Mode of Use						
'38'	'A'	'X'						
For all values of Secure Channel Method, the following field must be present:								
Key Scheme (LMK)	1 A	For Variant LMK, Indicates the scheme for encrypting derived keys under the LMK. See the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> for a list of schemes. Valid value is 'U'. For Key Block LMK, this field must be set to 'U'.						
If Secure Channel Method = '0', '1', '4', '5' or '6', the following 2 fields must be present (SCP02):								
Host Challenge	8 B	Random number provided by the Personalization System on INITIALISE UPDATE command to the card						
Sequence Counter	2 B	Sequence counter returned by the INITIALISE UPDATE command to the card which is used for derivation of the card session keys						
If Secure Channel Method = '7', the following 3 fields must be present (SCP03):								
Card Challenge Mode	1 N	'0': Random. Card challenge and cryptogram passed to command '1': Predictive. Card challenge and cryptogram generated by command						
Host Challenge	8 B	Random number provided by Personalization System						
Sequence Counter	3 B	Sequence counter returned by the INITIALISE UPDATE command to the card which is used for derivation of the card session keys.						
If Secure Channel Method = '0', '1', or '6', the following 2 fields must be present (SCP02 i='15'):								
Card Challenge	6 B	Random number generated by the card in response to the INITIALISE UPDATE command						
Card Cryptogram	8 B	Cryptogram generated by the card in response to INITIALISE UPDATE command and used by the Host to authenticate the card						
If Secure Channel Method = '7' and Card Challenge Mode = '0', the following 2 fields must be present (SCP03):								
Card Challenge	8 B	Random number generated by the card in response to the INITIALISE UPDATE command						
Card Cryptogram	8 B	Cryptogram generated by the card in response to INITIALISE UPDATE command and used by the Host to authenticate the card						
If Secure Channel Method = '4' or '5' (SCP02 i='55') or Secure Channel Method = '7' and Card Challenge Mode = '1' (Predictive), the following 3 fields must be present:								
AID Length	2 N	The length of the following AID field (must be even).						
AID	n H	The Application Identifier used to generate a pseudo random card challenge.						
Delimiter	1 A	Delimiter. Value ';'.						
If Secure Channel Method = '0', '1', '4', '5', '6' or '7', the following fields must be present:								
Initial APDU Header	5 B	Initial APDU header for EXTERNAL AUTHENTICATE command (CLA, INS, P1, P2, Lc). Typically [0x80, 0x82, 0x00, 0x00, 0x10] but must be specified.						
Security Level	1 B	Level of security for all secure messaging commands following the EXTERNAL AUTHENTICATE command. For Secure Channel Methods 0,1,4,5,6 (SCP02) valid values are: '0x00': No secure messaging '0x01': C-MAC '0x03': Encryption and C-MAC						

Field	Length & Type	Details
		'0x10': R-MAC '0x11': C-MAC and R-MAC '0x13': Encryption, C-MAC and R-MAC For Secure Channel Method 7, (SCP03) valid values are: '0x00': No secure messaging '0x01': C-MAC '0x03': Command encryption and C-MAC '0x11': C-MAC and R-MAC '0x13': Command encryption, C-MAC and R-MAC '0x33': Command encryption, C-MAC, R-MAC and response encryption
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ID'.
Error Code	2 N	<p>'00': No error '05': Invalid Secure Channel Method '06': Invalid Security Level '07': Card Cryptogram verification error '08': CK-DEK parity error '09': Invalid card key generation mode '10': KMC, PSK or CK-MAC parity error '11': CK-ENC parity error '37': Invalid card challenge mode '80': AID length error 'E4': KMC – key block error 'E5': CK-ENC – key block error 'E6': CK-MAC – key block error 'E7': CK-DEK – key block error 'E8': PSK – key block error or a standard error code.</p>
If Error Code = 'E4', 'E5', 'E6', 'E7' or 'E8', the following field will be present:		
Additional Error Code	2 A	The key block specific error code
If Secure Channel Method = '0', '1', '4', '5' or '6' (SCP02), the following fields will be present:		
APDU Header	5 B	APDU header for the EXTERNAL AUTHENTICATE command (CLA, INS, P1, P2, Lc).
Host Cryptogram	8 B	Host cryptogram for the EXTERNAL AUTHENTICATE command so that the card can authenticate the Host
Card Cryptogram	8 B	Cryptogram which would be generated by the card and used by the Host to authenticate the card. Only present if Secure Channel Method = '4' or '5'.
Authentication C-MAC	8 B	C-MAC for the EXTERNAL AUTHENTICATE command and for use as initial C-MAC in Prepare Secure Message for Chip Card command

Field	Length & Type	Details						
If Secure Channel Method = '0', '1', '4' or '5', the following fields will be present:								
SK-ENC	'U' + 32 H or 'S' + n A	Session Key for cryptograms and encrypting card messages (APDU Data), if required. For a Variant LMK, the SK-ENC is encrypted under LMK 24-25/3. For a Key Block LMK, the SK-ENC will comply with the following: <table border="1"><thead><tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr></thead><tbody><tr><td>'47'</td><td>'T'</td><td>'B'</td></tr></tbody></table>	Key Usage	Algorithm	Mode of Use	'47'	'T'	'B'
Key Usage	Algorithm	Mode of Use						
'47'	'T'	'B'						
Session Key for authenticating card messages (C-MAC). For a Variant LMK, the SK-MAC is encrypted under LMK 24-25/4. For a Key Block LMK, the SK-MAC will comply with the following: <table border="1"><thead><tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr></thead><tbody><tr><td>'48'</td><td>'T'</td><td>'G'</td></tr></tbody></table>	Key Usage	Algorithm	Mode of Use	'48'	'T'	'G'		
Key Usage	Algorithm	Mode of Use						
'48'	'T'	'G'						
SK-MAC	'U' + 32 H or 'S' + n A	Session Key for encrypting secret card data (e.g. application keys and PINs). For a Variant LMK, the SK-DEK is encrypted under LMK 24-25/5. For a Key Block LMK, the SK-DEK will comply with the following: <table border="1"><thead><tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr></thead><tbody><tr><td>'49'</td><td>'T'</td><td>'B'</td></tr></tbody></table>	Key Usage	Algorithm	Mode of Use	'49'	'T'	'B'
Key Usage	Algorithm	Mode of Use						
'49'	'T'	'B'						
Only present if Security Level is 0x10, 0x11, or 0x13 Session Key for authenticating card responses (R-MAC). For a Variant LMK, the SK-RMAC is encrypted under LMK 26-27. For a Key Block LMK, the SK-RMAC will comply with the following: <table border="1"><thead><tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr></thead><tbody><tr><td>'48'</td><td>'T'</td><td>'V'</td></tr></tbody></table>	Key Usage	Algorithm	Mode of Use	'48'	'T'	'V'		
Key Usage	Algorithm	Mode of Use						
'48'	'T'	'V'						
If Secure Channel Method = '6' and Card Key Generation Method = '0', the following field will be present:								
PSK	'U' + 32 H or 'S' + n A	The Personalisation System Key. For a Variant LMK, the PSK is encrypted under LMK 24-25/5. For a Key Block LMK, the SK-ENC will comply with the following: <table border="1"><thead><tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr></thead><tbody><tr><td>'40'</td><td>'T'</td><td>'N'</td></tr></tbody></table>	Key Usage	Algorithm	Mode of Use	'40'	'T'	'N'
Key Usage	Algorithm	Mode of Use						
'40'	'T'	'N'						
If Secure Channel Method = '2' (Mastercard PayPass MS Cards), the following field will be present:								
KD-PERSO	'U' + 32 H or 'S' + n A	KD Personalization Key for authenticating messages and encrypting sensitive data. For a Variant LMK, the KD-PERSO is encrypted under LMK 24-25/5. For a Key Block LMK, the KD-PERSO will comply with the following: <table border="1"><thead><tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr></thead><tbody><tr><td>'40'</td><td>'T'</td><td>'N'</td></tr></tbody></table>	Key Usage	Algorithm	Mode of Use	'40'	'T'	'N'
Key Usage	Algorithm	Mode of Use						
'40'	'T'	'N'						
If Secure Channel Method = '7' (SCP03), the following fields will be present:								
APDU Header	5 B	APDU header for the EXTERNAL AUTHENTICATE command (CLA, INS, P1, P2, Lc).						
Host Cryptogram	8 B	Host cryptogram for the EXTERNAL AUTHENTICATE command so that the card can authenticate the host.						
Authentication C-MAC	8 B	C-MAC for the EXTERNAL AUTHENTICATE command.						
C-MAC Chaining Value	16 B	The initial C-MAC value for the Prepare Secure Message command.						
Card Cryptogram	8 B	Only present if Card Challenge Mode = '1'. The generated card cryptogram.						
SK-MAC	'S' + n A	Session Key for authenticating card messages (C-MAC). The SK-MAC will comply with the following: <table border="1"><thead><tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr></thead><tbody><tr><td>'48'</td><td>'A'</td><td>'G'</td></tr></tbody></table>	Key Usage	Algorithm	Mode of Use	'48'	'A'	'G'
Key Usage	Algorithm	Mode of Use						
'48'	'A'	'G'						
If Security Level = 0x03, 0x13 or 0x33, the following fields will be present:								
SK-ENC	'S' + n A	Session Key for cryptograms and encrypting card messages. The SK-ENC will comply with the following: <table border="1"><thead><tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr></thead></table>	Key Usage	Algorithm	Mode of Use			
Key Usage	Algorithm	Mode of Use						

Field	Length & Type	Details								
		'47'	'A'	'B'						
If Security Level = 0x11, 0x13 or 0x33, the following fields will be present:										
SK-RMAC	'S' + n A	Session Key for authenticating card responses (R-MAC). The SK-RMAC will comply with the following:								
		<table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'48'</td><td>'A'</td><td>'V'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'48'	'A'	'V'		
Key Usage	Algorithm	Mode of Use								
'48'	'A'	'V'								
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.								
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.								

Prepare Secure Message for Chip Card

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: This function prepares the personalization messages for transmission to a chip card after a secure session has been established based on the process defined for EMV Common Personalization Specification (CPS) and Global Platform (GP) Secure Channel Protocol 2 (SCP02).

The following protocols are supported:

- Secure Channel Protocol 02 (SCP02) "i" = 0x15
- Secure Channel Protocol 02 (SCP02) "i" = 0x55
- Support for the specific process for Mastercard PayPass Magnetic Stripe Cards
- Support for static personalization method where the card application is personalized with a single Personalisation Secret Key (PSK).
- Secure Channel Protocol 03 (SCP03)

Note that using SCP03 requires the use of an AES Key Block LMK.

Notes: There are two methods under EMV CPS and GP SCP02 that can be used to provide personalization data to the card application. Each method is described below.

Indirect (Explicit) Method:

Card data is prepared by the Data Preparation Process and sent to the Personalization Process for programming on a chip card. The Personalization Process decrypts (from under a KEK, or appropriate key) and re-encrypts (under the SK-DEK) any sensitive data, such as application keys and PINs, and creates the Application Protocol Data Unit (APDU) messages that are sent to the chip card. If secure messaging is required, the card messages are MAC protected (C-MAC), and optionally encrypted using the session keys generated when the secure session was established.

Direct (Implicit) Method:

This method is not supported at this time.

For the above methods, this function prepares the APDU message(s) performing translation of sensitive data from the Data Preparation Process key(s) to the chip card key, if required. Support is provided for single or multiple Data Groupings to be included in a single APDU message as well as extended APDU command data lengths. All Global Platform commands are supported, including STORE DATA and PUT KEY. Depending on the Security Level established with the card, as specified in the parameters, the function will generate a C-MAC over the message and encrypt the APDU data elements where required. If the Security Level is set to require C-MAC or Encryption, bit 3 of the CLA will be automatically set to 1 by the function (typically yielding a byte of 0x84). The Global Platform specific C-MAC will always be generated with the logical channel numbers in the CLA byte (bits 1 and 2) set to 0 regardless of their setting in the Initial APDU Header. No modifications will be made to any other settings of the Initial APDU Header. The Global Platform specific options for C-MAC generation with encrypted ICVs and unmodified or modified APDUs are also supported.

For the Mastercard PayPass Magnetic Stripe method, the function prepares the APDU message and performs the translation of the KD-CVC3 key from the Data Preparation Process key to the chip card key. A MAC will also be generated over the message using the chip card key.

C-MAC is a MAC generated by the Host over the APDU command message.

NOTE: The Global Platform STORE DATA APDU is identified by an INS value of 0xE2 and bit 8 of the CLA byte set in the Initial APDU Header.

To support the ISO 7816 command APPEND RECORD which also uses an INS value of 0xE2, an additional optional flag 'GP Version Identifier' has been added which if set to '99' disables the checking for the GP STORE DATA command.

Field	Length & Type	Details									
COMMAND MESSAGE											
Message Header	m A	Subsequently returned to the Host unchanged.									
Command Code	2 A	Value 'IE'.									
Secure Channel Method	1 N	<p>'0': Indirect (Explicit) initiation of secure channel by the personalization system '1': Direct (Implicit) initiation of secure channel using pre-computed APDUs. Not supported at this time. '2': Mastercard PayPass Magnetic Stripe Cards <i>Note: For this method, the KD-PERSO key provided for encryption in the data groupings will also be used to generate the MAC. Only a single APDU will be created with a 1 byte length field (Lc).</i> '6': Indirect (Explicit) initiation of Open Platform secure channel by the personalization system using a single personalization key PSK. (SCP02) '7': Secure Channel Protocol 03 (SCP03)</p>									
If Secure Channel Method = '0', '6' or '7' the following field must be present:											
Security Level	1 B	<p>Level of security for the chip card message created by this command. Must match level set with EXTERNAL AUTHENTICATE command. For Secure Channel Method 0 or 6 (SCP02) valid values are: '0x00': No secure messaging '0x01': C-MAC '0x03': Encryption and C-MAC '0x10': R-MAC '0x11': C-MAC and R-MAC '0x13': Command encryption, C-MAC and R-MAC For Secure Channel Method 7, (SCP03) valid values are: '0x00': No secure messaging '0x01': C-MAC '0x03': Command encryption and C-MAC '0x11': C-MAC and R-MAC '0x13': Command encryption, C-MAC and R-MAC '0x33': Command encryption, C-MAC, R-MAC and response encryption</p>									
If Secure Channel Method = '0' or '6' (SCP02) and Security Level = 0x01, 0x03, 0x11 or 0x13, the following fields must be present:											
SK-MAC or PSK	'U' + 32 H or 'S' + n A	<p>Session Key for authenticating messages (C-MAC) or the Personalisation Master Key.</p> <p>For a Variant LMK: If Secure Channel Method = '0', the SK-MAC will be encrypted under Variant 4 of LMK pair 24-25. If Secure Channel Method = '6', the PSK will be encrypted under variant 5 of LMK pair 24-25.</p> <p>For a Key Block LMK, the SK-MAC or PSK in key block format; must comply with one of the following:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> </thead> <tbody> <tr> <td>'48' (SK-MAC)</td> <td>'T'</td> <td>'G'</td> </tr> <tr> <td>'40' (PSK)</td> <td>'T'</td> <td>'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'48' (SK-MAC)	'T'	'G'	'40' (PSK)	'T'	'N'
Key Usage	Algorithm	Mode of Use									
'48' (SK-MAC)	'T'	'G'									
'40' (PSK)	'T'	'N'									

Field	Length & Type	Details						
Initial C-MAC	8 B	The C-MAC from the previous APDU command or from EXTERNAL AUTHENTICATE for the first C-MAC						
ICV Encryption Flag	1 N	Global Platform option to encrypt previous C-MAC for use as ICV '0': Do not encrypt previous C-MAC before using it as ICV '1': Encrypt previous C-MAC before using it as ICV						
C-MAC Flag	1 N	Use Global Platform C-MAC generation process and options (previous C-MAC used as IV for MAC) '0': Modify APDU prior to C-MAC generation (set secure messaging bit of CLA to 1 and include C-MAC length in Lc byte) '1': Do not modify APDU prior to C-MAC generation Use EMV CPS C-MAC generation process (previous C-MAC prepends MAC data, use IV of binary zeroes) '9': Modify APDU for C-MAC generation (set secure messaging bit of CLA to 1 and include C-MAC length in Lc byte)						
If Secure Channel Method = '0' or '6' (SCP02) and Security Level = 0x03 or 0x13, the following field must be present:								
SK-ENC	'U' + 32 H or 'S' + n A	<p>Session Key for cryptograms and encrypting card messages (APDU), if required, encrypted under the LMK.</p> <p>For a Variant LMK, the SK-ENC is encrypted under variant 3 of LMK pair 24-25.</p> <p>For a Key Block LMK, the SK-ENC must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'47'</td><td>'T'</td><td>'B'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'47'	'T'	'B'
Key Usage	Algorithm	Mode of Use						
'47'	'T'	'B'						
If Secure Channel Method = '7' and Security Level is not 0x00, the following fields must be present:								
SK-MAC	'S' + n A	<p>Session Key for cryptograms and encrypting card messages (APDU), if required, encrypted under the LMK.</p> <p>The SK-ENC must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'48'</td><td>'A'</td><td>'G'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'48'	'A'	'G'
Key Usage	Algorithm	Mode of Use						
'48'	'A'	'G'						
C-MAC Chaining Value	16 B	C-MAC Chaining from the previous APDU command or the initial C-MAC value returned from the EXTERNAL AUTHENTICATE.						
Initial ICV Counter	6 N	The counter is set to 1 following a successful EXTERNAL AUTHENTICATE command and incremented for each subsequent APDU command with the secure session.						
If Secure Channel Method = '7' and Security Level = 0x03, 0x13 or 0x33, the following field must be present:								
SK-ENC	'S' + n A	<p>Session Key for cryptograms and encrypting card messages (APDU), if required, encrypted under the LMK.</p> <p>The SK-ENC must comply with the following:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'47'</td><td>'A'</td><td>'B'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'47'	'A'	'B'
Key Usage	Algorithm	Mode of Use						
'47'	'A'	'B'						
If Secure Channel Method = '0', '2', '6' or '7', the following fields must be present (as indicated):								
Initial APDU Header	4 B	<p>Initial APDU header for command [CLA, INS, P1, P2]</p> <p>Note: Lc will be automatically generated by the function.</p> <p>It is the responsibility of the host to specify the following:</p> <ul style="list-style-type: none"> CLA: Bit 8 set to 1 to denote a Global Platform command otherwise 0 for ISO 7816 CLA: Bits 1 and 2 to denote the channel (default 00) INS: Identifies the APDU. P1: The value depends upon the INS value. P2: The value depends upon the INS value. <p>The 'IE' command will copy the Initial APDU Header to the output APDU header and will make the following changes:</p> <p>If bit 8 of CLA is set denoting Global Platform and the Security Level is either 1 or 3, the CLA bit 3 will be set to 1 otherwise 0.</p> <p>The command will set bits 1 and 2 of the CLA byte to 00 for C-MAC processing however their initial values will be preserved for output.</p> <p>If INS=0xE2 and bit 8 of the CLA byte is set denoting STORE DATA:</p> <ul style="list-style-type: none"> the P2 value will be incremented for each additional APDU message created as a result of the APDU data length exceeding the maximum length of the command. Bits 5 & 4 of P1 should be set appropriately to match the DGI/TLV length setting as specified by the (optional) GP Version Identifier parameter later 						

Field	Length & Type	Details
Command Length	1 N	<p>in this command (as defined in Table 11-89 STORE DATA Reference Control Parameter 1 of Global Platform Card Specification Version 2.3.1).</p> <p>Maximum length of command</p> <p>'0': Lc = 1 byte. Maximum of 255 bytes for <u>overall</u> command, including APDU header.</p> <p>'1': Lc = 1 byte with a maximum length of 255.</p> <p>'2': Lc = 2 bytes with a maximum length of 65,535.</p> <p>'3': Lc = 1 byte with a maximum length of 255 bytes for the overall command, including the APDU header.</p> <p><i>Note: If the data groups provided cannot be accommodated in a single command, multiple commands will be created as required.</i></p> <p><i>Note: Secure Channel Method 2 only supports a single command.</i></p> <p><i>Note: In this mode, the length will be preceded by 0x00 for a total of 3 bytes. Only a single command will be created.</i></p> <p><i>Note: Not valid for Secure Channel Method 2.</i></p> <p><i>Note: If the data groups provided cannot be accommodated in a single command for '3', multiple commands will be created as required, and the DataGroup length will be coded in 3 bytes (preceded by 0xFF and followed by 2 bytes length).</i></p> <p><i>Note: For short data where no multiple commands are created, this mode should behave exactly same as mode '0'.</i></p> <p><i>Note: Only valid for Secure Channel Method 0.</i></p>
DG Count	2 N	<p>For STORE DATA APDUs identified by INS value 0xE2 in the initial APDU Header, DG Count represents the Number of Data Groupings for the command i.e the number of individual DGIs to be concatenated into a single STORE DATA APDU command.</p> <p>NOTE: STORE DATA APDUs are identified by an INS value of 0xE2 and bit 8 of the CLA byte set in the Initial APDU Header.</p> <p>For all other APDUs, DG Count represents the number of data elements that are appended together to build the APDU data.</p>
Delimiter	1 A	Value ';'. Optional; only present if the following field is present AND the Secure Channel Method = '0' or '6' or '7'.
Output Mode	1 N	<p>'0': pack DGIs into one APDU.</p> <p>'1': wrap each DGI into a separate APDU.</p> <p>'2': pack DGIs into one APDU and automatically set Last Store Data indicator (Bit 8) in P1 for last APDU generated</p> <p>'3': wrap each DGI into a separate APDU and automatically set Last Store Data indicator (Bit 8) in P1 for last APDU generated</p> <p>Optional; only present if the Secure Channel Method = '0'.</p>
The following fields must be repeated for each Data Group:		
DGI	2 B	<p>Identifier of the Data Group.</p> <p>NOTE: this is only applicable when INS=0xE2 STORE DATA otherwise this field is ignored and should be set with 0x00 0x00.</p>
DG Type Flag	1 A	<p>Data Group data type</p> <p>'0': Clear Data</p> <p>'1': Key(s) encrypted under a KEK, ECB mode.</p> <p>'2': Key encrypted under a KEK, CBC mode.</p> <p>'3': PIN Block encrypted under a ZPK.</p> <p>'4': Clear Data to be encrypted under SK-DEK. Must be a multiple of 8 bytes.</p> <p>'5': The Key encrypted under the LMK.</p> <p><i>Note: Encrypted Keys and PIN Blocks should be in format required by the card. (e.g. PIN Block Format 05). No format conversion will be performed.</i></p> <p><i>If multiple keys are provided for a DG Type 1 group, they are to be concatenated without the Key Scheme indicator. All keys must be of the type and length defined by the Key Scheme (KEK) parameter.</i></p>
If DG Type Flag = '1', '2' or '3', the following field must be present:		
Decryption Key		<p>Key to decrypt DG data.</p> <p><i>Optional, only has to be provided with the first Data Group using this key if multiple Data Groups requiring the same key are provided.</i></p>
	'U' + 32 H or 'T' + 48 H	<p>For a Variant LMK:</p> <p>If DG Type Flag = 1 or 2: KEK encrypted under LMK 24-25/1.</p> <p>If DG Type Flag = 3: ZPK encrypted under LMK 06-07.</p>

Field	Length & Type	Details																					
	or 'S' + n A	For a Key Block LMK, the Decryption Key must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'54' (KEK)</td><td>'T'</td><td>'B', 'D', 'E', 'N'</td></tr> <tr> <td>'72' (ZPK)</td><td>'T'</td><td>'B', 'D', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'54' (KEK)	'T'	'B', 'D', 'E', 'N'	'72' (ZPK)	'T'	'B', 'D', 'N'												
Key Usage	Algorithm	Mode of Use																					
'54' (KEK)	'T'	'B', 'D', 'E', 'N'																					
'72' (ZPK)	'T'	'B', 'D', 'N'																					
If DG Type Flag = '1', '2', '3' or '4', the following 4 fields must be present:																							
Delimiter	1 A	Mandatory Delimiter. Value ':'.																					
Key Scheme (KEK)	1 A	If a Key Scheme was used to encrypt keys under KEK, it should be specified here. See the Key Scheme Table in the <i>payShield 10K Host Programmer's manual</i> . Default scheme 'X'. <i>Optional. Only used if DG Type Flag = 1 and Decryption Key is provided.</i>																					
Delimiter	1 A	For a Key Block LMK, this field is ignored and should be set to '0'.																					
IV	8 B	Mandatory Delimiter. Value ':'. Initialization Vector for CBC mode decryption. Only present if DG Type Flag = 2.																					
If Secure Channel Method = '0', '2' or '6' and DG Type Flag = '1', '2', '3', '4' or '5', the following field must be present:																							
SK-DEK or KD-Perso or PSK (if not previously loaded)	'U' + 32 H or 'S' + n A	Session Key for encrypting secret card data (e.g. application keys and PINs) encrypted under the LMK. <i>Optional, only has to be provided when DG Type Flag = 1, 2, 3, or 4 with the first Data Group requiring the key if multiple Data Groups requiring the key are provided.</i> For a Variant LMK, the session Key is encrypted under LMK 24-25/5. For a Key Block LMK, the session Key must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'49' (SK-DEK)</td><td>'T'</td><td>'E', 'B'</td></tr> <tr> <td>'40' (PSK)</td><td>'T'</td><td>'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'49' (SK-DEK)	'T'	'E', 'B'	'40' (PSK)	'T'	'N'												
Key Usage	Algorithm	Mode of Use																					
'49' (SK-DEK)	'T'	'E', 'B'																					
'40' (PSK)	'T'	'N'																					
If Secure Channel Method = '7' and DG Type Flag = '1', '2', '3', '4' or '5', the following field must be present:																							
CK-DEK	'S' + n A	The Card key for encrypting secret card data e.g. application keys and PINs. For a Key Block LMK, the card key must comply with the following: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'39'</td><td>'A'</td><td>'B'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'39'	'A'	'B'															
Key Usage	Algorithm	Mode of Use																					
'39'	'A'	'B'																					
Delimiter	1 A	Mandatory Delimiter. Value ':'.																					
If DG Type Flag = '5', the following field must be present:																							
Key Type Code	3 H	For Variant LMK, the field indicates the LMK pair and variant under which the key provided in the DG Data is encrypted under. Valid values are: '30D': CK-ENC encrypted under LMK pair 36-37 variant 3 '40D': CK-MAC encrypted under LMK pair 36-37 variant 4 '50D': CK-DEK encrypted under LMK pair 36-37 variant 5 '507': PSK encrypted under LMK pair 24-25 variant 5 For Key Block LMK, this field will be ignored and should be set to 'FFF'.																					
For all DG Type Flag values, the following 4 fields must be present:																							
DG Length	2 B	Length of the Data Group If DG Type Flag = '5', this field will be ignored.																					
DG Data	n B 16 H 'S' + n A	Data Group Data If DG Type Flag = 0, 1, 2 or 4. If DG Type Flag = 3, this is the PIN Block. <i>Note: DG Length above would be '08'.</i> If DG Type Flag = 5, this is the key encrypted under the LMK. For Secure Channel Methods = '0' and '6', the following keys are valid: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'37' (CK-ENC)</td><td>'T'</td><td>'X'</td></tr> <tr> <td>'38' (CK-MAC)</td><td>'T'</td><td>'X'</td></tr> <tr> <td>'39' (CK-DEK)</td><td>'T'</td><td>'X'</td></tr> <tr> <td>'40' (PSK)</td><td>'T'</td><td>'N'</td></tr> </tbody> </table> For Secure Channel Method = '7', the following keys are valid: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'37' (CK-ENC)</td><td>'A', 'T'</td><td>'X'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'37' (CK-ENC)	'T'	'X'	'38' (CK-MAC)	'T'	'X'	'39' (CK-DEK)	'T'	'X'	'40' (PSK)	'T'	'N'	Key Usage	Algorithm	Mode of Use	'37' (CK-ENC)	'A', 'T'	'X'
Key Usage	Algorithm	Mode of Use																					
'37' (CK-ENC)	'T'	'X'																					
'38' (CK-MAC)	'T'	'X'																					
'39' (CK-DEK)	'T'	'X'																					
'40' (PSK)	'T'	'N'																					
Key Usage	Algorithm	Mode of Use																					
'37' (CK-ENC)	'A', 'T'	'X'																					

Field	Length & Type	Details			
DG End Delimiter	1 A	'38' (CK-MAC)	'A', 'T'	'X'	
		'39' (CK-DEK)	'A', 'T'	'X'	
		'40' (PSK)	'T'	'N'	
DG End Delimiter	1 A	Mandatory Delimiter. Value ':'. (semicolon)			
All DG End Delimiter	1 A	Mandatory Delimiter. Value ':'. (colon)			
GP Version Delimiter	1 A	Value '\$'. Optional; if present, the following field must also be present.			
GP Version Identifier	2 N	Indicates to which GP Card Specification this command must conform The valid values are: '01': Command conforms to GP Card Specification 2.2 '99': Command does not conform to the GP Card Specification			
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.			
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.			
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.			
Message Trailer	n A	Optional. Maximum length 32 characters.			

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IF'.
Error Code	2 N	<p>'00': No error '05': Invalid Secure Channel Method '06': Invalid Security Level '07': Invalid DG Type Flag '08': SK-DEK parity error '09': Decryption Key parity error '10': SK-MAC or PSK parity error '11': SK-ENC parity error '50': Invalid ICV Encryption Flag '51': Invalid C-MAC Flag '52': Invalid Command Length '53': Decryption Key required and not available '54': SK-DEK required and not available '55': Length of APDU Data exceeds limit '56': Data Groupings block error (delimiter) '57': Maximum number of APDU messages exceeded '58': Invalid Key Type Code 'DA': Decryption key block error 'E1': SK-MAC key block error 'E2': SK-ENC key block error 'E3': SK-DEK or KD-PERSO key block error 'E8': PSK key block error 'F2': Invalid GP Version Identifier 'F3': DG Type Flag '5' key block error 'F4': Key type not allowed for this secure channel or a standard error code.</p>
If Error Code = 'DA', 'E1', 'E2', 'E3' or 'E8', the following field will be present:		
Additional Error Code	2 A	Key Block specific error code
If Secure Channel Method = '0', '6' or '7', the following 5 fields will be present:		
APDU Message Count	1 N 2 N	<p>Number of commands generated by the function. Note: If Command Length = 2, only a single command will be returned. If Output Mode is '0' or '2'. If Output Mode is '1' or '3'.</p>
The following 3 fields will be repeated for each APDU message:		
APDU Header n	5 or 7 B (if Command Length = 2)	<p>APDU header for command [CLA, INS, P1, P2, Lc]. Note: If Command Length = 2, the Lc byte will be 0x00 followed by an additional 2 bytes indicating the data block length (3 bytes total)</p>
APDU Data Block n	n B	<p>APDU data (Length Lc) - Data Groupings and MAC, if required. Note: The last 8 bytes of the last, or only, APDU Data Block may consist of a C-MAC, if required by the function. This may be needed for use as the Initial C-MAC in the next Prepare Secure Message for Chip Card function. Note: If Command Length = 3, the Data Group Length will be coded in 3 bytes (0xFF followed by an additional 2 bytes indicating the data group length).</p>
APDU End Delimiter	1 A	Delimiter. Value ';' (semicolon)
All APDU End Delimiter	1 A	Delimiter. Value ':' (colon)
If Secure Channel Method = '2', the following 2 fields will be present:		
APDU Header	5 B	APDU header for command [CLA, INS, P1, P2, Lc].
APDU Data Block	n B	APDU data (Length Lc)
If Secure Channel Method = '7' and Security Level is not 0x00, the following 2 fields will be present:		
C-MAC Chaining Value	16 B	The C-MAC computed on the final APDU message.
Final ICV Counter	6 N	The ICV value used on the final APDU message.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify and Decrypt Response Secure Message from Chip Card

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Verify response R-MAC and optionally decrypt response data from APDU response

Notes: Depending on the security level defined in the initiation of the Secure Channel, all subsequent APDU responses within the Secure Channel may require secure messaging by use of an R-MAC for integrity and encryption for confidentiality. This command checks the integrity of the response command and decrypts the response data. No encryption is applied to a response where there is no response data field and in this case the message shall be protected only.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'II'.						
Secure Channel Method	1 N	'7': Secure Channel Protocol 03 (SCP 03)						
Security Level	1 B	Valid values ae: '0x11': C-MAC and R-MAC '0x13': Command encryption, C-MAC and R-MAC '0x33': Command encryption, C-MAC, R-MAC and response encryption						
SK-RMAC	'S' + n A	Session Key for authenticating response messages (R-MAC) encrypted under the Key Block LMK which should conform to: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'48'</td> <td>'A'</td> <td>'V', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'48'	'A'	'V', 'N'
Key Usage	Algorithm	Mode of Use						
'48'	'A'	'V', 'N'						
C-MAC Chaining Value	16 B	The C-MAC Chaining from the previous APDU command or from EXTERNAL AUTHENTICATE for the first C-MAC.						
SK-ENC	'S' + n A	Only present if Security Level is '0x33'. Session Key for encrypting response messages encrypted under the Key Block LMK which should conform to: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'47'</td> <td>'A'</td> <td>'B', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'47'	'A'	'B', 'N'
Key Usage	Algorithm	Mode of Use						
'47'	'A'	'B', 'N'						
Encryption Counter	5 N	The Encryption Counter's start value shall be set to 1 for the first command following a successful EXTERNAL AUTHENTICATE command. The Off-Card entity shall increment the Encryption Counter for each subsequent APDU command sent within the secure channel session.						
Response Data Length	4 N	The length of the Response Data.						
Response Data	n B	The APDU response data either plain text or encrypted according to the Security Level.						
R-MAC	8 B	The R-MAC generated on the APDU Response Data.						
Status Words	2 B	Status bytes returned in APDU response message.						
LMK Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.						
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by License; must be present if the above Delimiter is present.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IJ'.
Error Code	2 N	'00': No error '05': Invalid Secure Channel Method '06': Invalid Security Level 'E2': SK-ENC – key block error 'E4': SK-RMAC – key block error 'E5': R-MAC verification error
If Error Code = 'E2' or 'E4', the following field will be present:		
Additional Error Code	2 A	Key Block specific error code
If Security Level = 0x33, the following 2 fields will be present:		
Response Data Length	4 N	The length of the plaintext Response Data field.
Response Data	n B	The decrypted plaintext Response Data.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

10.5 Mobile Device Provisioning Commands

The HSM provides the following host commands to support the secure operations required for provisioning cryptographic material to a mobile device:

Function	Command	Page
<i>Validate Authentication Code</i>	IQ (IR)	620
<i>Generate Remote Management Secure Message</i>	IU (IV)	621
<i>Validate and Recover Remote Management Secure Message from the MPA</i>	IW (IX)	627

Validate Authentication Code

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Optional	
Activity: diag.host	

Function: Validate Authentication Code.

The Authentication Code is generated by the Mobile Payment Application (MPA) and sent to the host Credentials Management System (CMS) during the initialization phase, allowing the CMS to authenticate the MPA.

Notes: The Authentication code is generated using the Session ID, the Mobile Device Identifier and MPA Fingerprint.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'IQ'.
CMSMPA_ID	32 B	The Mobile Payment Application Identifier. Generated by the CMS and loaded on the MPA at initialization.
Encrypted Session ID LMK	32 B	The Session ID encrypted under the AES Key Block LMK.
MPA_FPG	32 B	The Mobile device finger print returned by the MPA
CMSMPA_AUTH	32 B	The Authentication Code generated by the MPA
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IR'.
Error Code	2 A	'00': No error '01': Failed to validate authentication code 'A1': Invalid LMK scheme Or a standard error code
If Error Code = '01' and the HSM is in Authorized State, the following field will be present:		
Diagnostic Data	32 B	The calculated CMSMPA_AUTH.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Remote Management Secure Message

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Generate Remote Management Secure Message

Notes: The Remote Management session keys are used to create a secure data block for transfer from the host Credentials Management System (CMS) to the Mobile Payment Application (MPA).

The format of the message from CMS to MPA is of the form:

Counter || Encrypted Message data || MAC

where Counter is incremented for each message.

This function allows the host to create message payloads containing both plain text and cipher text data generated by the data preparation systems into a secure message encrypted and protected using the Remote Management Session keys.

Note that the Single Use Key Block (DC_SUK) is generated using the 'IY' command.

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IU'.						
Mode	1 N	<p>'0': Encrypt and MAC the payload using the remote management session keys MS_KEY_CONF, MS_KEY_MAC</p> <p>'1': Encrypt the payload using AES ECB mode under the transport key.</p> <p>'2': As Mode '0' but with binary key data elements converted to ASCII Hex format so that the plain text payload is suitable for interpretation by a JSON format parser.</p> <p>'3': Encipher the payload with a Transport Key using CCM (Counter based with CBC MAC) encryption.</p> <p>'4': Encipher the payload with the remote management master keys M_KEY_CONF using AES CBC and MAC protect with M_KEY_MAC using AES MAC Algorithm 1 in ISO/IEC 9797-1 with padding method 2.</p>						
If Mode is '0' or '2', the following 3 fields must be present:								
Message Counter	5 N	The message counter is maintained by the CMS and is incremented for each message sent from the CMS to MPA. Maximum value is 65535.						
MS_KEY_CONF	'S' + n A	The Remote Management Session Key for message confidentiality, encrypted under AES Key Block LMK and which must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'35'</td><td>'A'</td><td>'B', 'D', 'E', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'35'	'A'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'35'	'A'	'B', 'D', 'E', 'N'						
MS_KEY_MAC	'S' + n A	The Remote Management Session Key for message integrity, encrypted under AES Key Block LMK and which must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'36'</td><td>'A'</td><td>'C', 'G', 'N', 'V'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'36'	'A'	'C', 'G', 'N', 'V'
Key Usage	Algorithm	Mode of Use						
'36'	'A'	'C', 'G', 'N', 'V'						
If Mode is '1', the following field must be present:								
Transport Key	'S' + n A	The Transport Key encrypted under the AES Key Block LMK which must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'55'</td><td>'A'</td><td>'E', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'55'	'A'	'E', 'N'
Key Usage	Algorithm	Mode of Use						
'55'	'A'	'E', 'N'						
If Mode is '3', the following fields must be present:								
Cipher Mode	1 N	Cipher used to encrypt the payload. Valid values are: '0': AES						
Transport Key	'S' + n A	The transport key, which must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'24'</td><td>'A'</td><td>'B', 'N'</td></tr> </table>	Key Usage	Algorithm	Mode of Use	'24'	'A'	'B', 'N'
Key Usage	Algorithm	Mode of Use						
'24'	'A'	'B', 'N'						
MAC Length	2 N	The length of the MAC (TLen). Valid values are 04, 06, 08, 10, 12, 14, and 16 bytes.						
Number of bytes to encode message length	1 N	The length MLen in bytes required to store the message length. The maximum length of the message is $2^{8 \times \text{MLen}}$. Valid values are 2 to 8 bytes. MLen = 1 is reserved.						
Nonce length	2 N	The length of the Nonce field (NLen). The maximum length is 15-MLen bytes.						
Nonce	n B	The Nonce value.						
Delimiter	1 A	Value ':'.						
Authentication Data Length	6 N	The length of the Authentication Data field (ALen). Zero if not required.						
Authentication Data	n B	The Authentication Data.						
Delimiter	1 A	Value ':'.						
If Mode is '4', the following fields must be present:								
Block Cipher	1 N	Cipher used to encrypt the payload. Valid values are: '0': AES						
Block Cipher Mode	1 N	The block cipher mode used to encrypt the payload. Valid values are: '0': CBC						
IV	32 H	Only present if Block Cipher Mode = '0'. Initialization Vector.						
MAC Algorithm	1 N	'0': CBC-MAC (AES only)						

payShield 10K Core Host Commands

Field	Length & Type	Details						
Padding Method	1 N	'0': ISO 9797 Padding Method 2 (i.e. add 0x80 and pad with 0x00).						
M_KEY_CONF	'S' + n A	The Remote Management Session Key for message confidentiality, encrypted under AES Key Block LMK and which must comply with the following:						
		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'33'</td><td>'A'</td><td>'X', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'33'	'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'33'	'A'	'X', 'N'						
M_KEY_MAC	'S' + n A	The Remote Management Session Key for message integrity, encrypted under AES Key Block LMK and which must comply with the following:						
		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'34'</td><td>'A'</td><td>'X', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'34'	'A'	'X', 'N'
Key Usage	Algorithm	Mode of Use						
'34'	'A'	'X', 'N'						
For all modes, the following field must be present:								
Message Data Item Count	2 N	The number of Message Data Items to load into a single message payload.						

Field	Length & Type	Details																																				
The following fields are repeated for each Message Data Item																																						
Message Data Item Type	2 N	<p>Valid Message Data Item Types for Modes '0' and '3' are:</p> <ul style="list-style-type: none"> '00': Clear Data '01': Key encrypted under a KEK, 3DES ECB mode (decrypted key added to output block as binary data.) '02': Key encrypted under a KEK, 3DES CBC mode (decrypted key added to output block as binary data.) '03': PIN Block encrypted under a ZPK (decrypted PIN block added to output block as ASCII hex.) '06': Key encrypted under a KEK, AES ECB mode translated to encryption under the mobile Data encryption Key (key encrypted under mobile data encryption key added to output block as binary data) <p>Valid Message Data Item Types for Mode '2' are:</p> <ul style="list-style-type: none"> '00': Clear Data '01': Key encrypted under a KEK, 3DES ECB mode (decrypted key added to output block as ASCII hex.) '02': Key encrypted under a KEK, 3DES CBC mode (decrypted key added to output block as ASCII hex.) '03': PIN Block encrypted under a ZPK (decrypted PIN block added to output block as ASCII hex.) '06': Key encrypted under a KEK, AES ECB mode translated to encryption under the mobile Data encryption Key (key encrypted under mobile data encryption key added to output block as ASCII hex) <p>Valid Message Data Item Types for Mode '1' are:</p> <ul style="list-style-type: none"> '05': Key encrypted under the Key Block LMK <p>The keys types supported are:</p> <p>The M_KEY_CONF and M_KEY_MAC which must conform to:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'33', '34'</td><td>'A'</td><td>'X', 'N'</td></tr> </tbody> </table> <p>The ZPK must conform to:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'72'</td><td>'A'</td><td>'D', 'N'</td></tr> </tbody> </table> <p>The DEK must conform to:</p> <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'21'</td><td>'A'</td><td>'B', 'N'</td></tr> </tbody> </table> <p>Valid Message Data Item Types for Mode '04' are:</p> <ul style="list-style-type: none"> '00': Plain text data '07': Session ID encrypted under the Key Block LMK (decrypted session ID added to block as ASCII hex). <p>Key to decrypt the Message Data Item.</p> <p>Not required when Message Data Item Type is '00' or '05'.</p> <p>If multiple Message Data Items requiring the same key are provided, then this field must be provided with the first Message Data Item. However, it is optional for the remaining Message Data Items using the same key.</p> <p>If Message Data Item Type is:</p> <ul style="list-style-type: none"> '01' or '02': KEK encrypted under the LMK: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'54'</td><td>'T'</td><td>'B', 'D', 'N'</td></tr> </tbody> </table> <ul style="list-style-type: none"> '03': ZPK encrypted under the LMK <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'P0', '72'</td><td>'T'</td><td>'B', 'D', 'N'</td></tr> </tbody> </table> <ul style="list-style-type: none"> '06': Transport Key encrypted under the LMK: <table border="1"> <thead> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> </thead> <tbody> <tr> <td>'21', '24', '54'</td><td>'A'</td><td>'B', 'N'</td></tr> </tbody> </table>	Key Usage	Algorithm	Mode of Use	'33', '34'	'A'	'X', 'N'	Key Usage	Algorithm	Mode of Use	'72'	'A'	'D', 'N'	Key Usage	Algorithm	Mode of Use	'21'	'A'	'B', 'N'	Key Usage	Algorithm	Mode of Use	'54'	'T'	'B', 'D', 'N'	Key Usage	Algorithm	Mode of Use	'P0', '72'	'T'	'B', 'D', 'N'	Key Usage	Algorithm	Mode of Use	'21', '24', '54'	'A'	'B', 'N'
Key Usage	Algorithm	Mode of Use																																				
'33', '34'	'A'	'X', 'N'																																				
Key Usage	Algorithm	Mode of Use																																				
'72'	'A'	'D', 'N'																																				
Key Usage	Algorithm	Mode of Use																																				
'21'	'A'	'B', 'N'																																				
Key Usage	Algorithm	Mode of Use																																				
'54'	'T'	'B', 'D', 'N'																																				
Key Usage	Algorithm	Mode of Use																																				
'P0', '72'	'T'	'B', 'D', 'N'																																				
Key Usage	Algorithm	Mode of Use																																				
'21', '24', '54'	'A'	'B', 'N'																																				
Delimiter	1 A	Only present if Decryption Key is reused from previous Message Data Item. Value ':'.																																				
IV	8 B	Only present if Message Data Item Type = '02'. Initialization Vector for CBC mode decryption.																																				

Field	Length & Type	Details						
Encryption Key	'S' + n A	Only present if Message Data Item Type = '06'. The application KEK encrypted under the LMK and which must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'21'</td> <td>'A'</td> <td>'B', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'21'	'A'	'B', 'N'
Key Usage	Algorithm	Mode of Use						
'21'	'A'	'B', 'N'						
Delimiter	1 A	Only present if Encryption Key is reused from previous Message Data Item. Value ';'.						
Message Data Item Length	6 N	The length of the Message Data Item field						
Message Data Item	n B	The plain text or encrypted Message Data						
Message Data Item Delimiter	1 A	Mandatory Delimiter. Value ';' (semi-colon).						
All Message Data Item Delimiter	1 A	Mandatory Delimiter. Value ':' (colon).						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IV'.
Error Code	2 A	<p>'00': No error '05': Length of Message Data does not equal Message Data Item Length '06': Message Counter exceeds maximum value '07': Invalid Message Data Item value '08': Key parity error '09': Message Data is not a multiple of cipher block size bytes 'D1': M_KEY_CONF – key block error 'D2': M_KEY_MAC – key block error 'D3': Invalid message Data Item Length 'D4': MS_KEY_CONF or Transport Key – key block error 'D5': MS_KEY_MAC – key block error 'D7': message length exceeds maximum 'DA': Decryption Key – key block error 'DB': Message Data Item Type 5 - key block error or mobile Data Encryption Key error 'DC': Invalid Mode value 'DD': Key usage not allowed 'E1': Invalid Cipher Mode 'E2': Invalid MAC length 'E3': Invalid Number of bytes to encode message length 'E4': Invalid Nonce length 'E5': Invalid Authentication Data Length 'E7': Invalid key length 'E8': Invalid block cipher mode 'E9': Invalid MAC Algorithm 'EA': Invalid Pad Mode 'A1': Invalid LMK scheme Or a standard error code.</p>
If Error Code ≠ '00', the following 2 fields will be present:		
Additional Error Code	2 A	The key block specific error code, or '00' if not relevant.
Additional Error Code 2	2 A	The number of the Message Data Item causing the error, or '00' if not relevant.
If Mode = '0' or '2', the following 4 fields will be present:		
Encrypted Message Data Length	6 N	The length of the Encrypted Message Data field.
Encrypted Message Data	n B	The Message Data encrypted under the MS_KEY_CONF session key using AES in Counter (CTR) mode.
MAC	8 B	The MAC using AES and MAC Algorithm 1 in ISO/IEC 9797-1 with padding method 2 over the Encrypted Message Data using the MS_KEY_MAC session key.
DC_CP Hash Code	32 B	The SHA 256 hash code generated over the plain text message data.
If Mode = '1', the following 2 fields will be present:		

Field	Length & Type	Details
Encrypted Message Data Length	6 N	The length of the Encrypted message Data field.
Encrypted Message Data	n B	The Message Data encrypted under the transport key using AES in ECB mode.
If Mode = '3', the following 2 fields will be present:		
Encrypted Message Data Length	6 N	The length of the Encrypted Message Data field.
Encrypted Message Data	n B	The Message Data encrypted under the Transport Key using Counter with CBC-MAC (CCM).
If Mode = '4', the following 3 fields will be present:		
Encrypted Message Data Length	6 N	The length of the Encrypted Message Data field.
Encrypted Message Data	n B	The Message Data encrypted under M_KEY_CONF using 'Block Cipher' and 'Block Cipher Mode'.
Encrypted Message MAC	8 B	MAC over the Encrypted Message Data using M_KEY_MAC and 'MAC Algorithm'.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Validate and Recover Remote Management Secure Message from the MPA

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Validate and Recover Remote Management Secure Message from the Mobile Payment Application (MPA).

The Remote Management session keys are used to decrypt and authenticate the remote management response data from the MPA.

This command currently returns plain text.

Notes: The format of the message from the MPA to Credentials Management System (CMS) is:

Counter || Encrypted Message data || MAC

where Counter is incremented for each message.

This command cannot be used to validate data generated by Validate Remote Management Secure Message (IU).

Field	Length & Type	Details						
COMMAND MESSAGE								
Message Header	m A	Subsequently returned to the Host unchanged.						
Command Code	2 A	Value 'IW'.						
Version Delimiter	1 A	Value '='. Optional; if present, the following field must also be present.						
Version	1 N	Command Version Number. Valid values are: '1' – Decrypt remote management message using remote management session keys and AES Counter mode. Message Data Lengths specified as 4 N. '2' – Decrypt remote management message using remote management session keys and AES Counter mode. Message Data Lengths specified as 6 N. '3' – Decrypt remote management message using transport key and Counter based CBC-MAC (CCM).						
If Version is '1' or '2', the following fields must be present.								
Message Counter	5 N	The message counter is maintained by the MPA and is incremented for each message from the MPA to CMS. Maximum value is 65535 or 0x00FFFF						
MS_KEY_CONF	'S' + n A	The Remote Management Session Key for message confidentiality, encrypted under AES Key Block LMK and which must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'35'</td> <td>'A'</td> <td>'B', 'D', 'E', 'N'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'35'	'A'	'B', 'D', 'E', 'N'
Key Usage	Algorithm	Mode of Use						
'35'	'A'	'B', 'D', 'E', 'N'						
MS_KEY_MAC	'S' + n A	The Remote Management Session Key for message integrity, encrypted under AES Key Block LMK and which must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode of Use</th> </tr> <tr> <td>'36'</td> <td>'A'</td> <td>'C', 'G', 'N', 'V'</td> </tr> </table>	Key Usage	Algorithm	Mode of Use	'36'	'A'	'C', 'G', 'N', 'V'
Key Usage	Algorithm	Mode of Use						
'36'	'A'	'C', 'G', 'N', 'V'						
If Mode is '3', the following fields must be present:								
Cipher Mode	1 N	Cipher used to encrypt the payload. Valid values are: '0': AES						

Field	Length & Type	Details						
Transport Key	'S' + n A	The transport key, which must comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr> <tr> <td>'24'</td><td>'A'</td><td>'B', 'N'</td></tr> </table> <p>The key length is 128 bits.</p>	Key Usage	Algorithm	Mode of Use	'24'	'A'	'B', 'N'
Key Usage	Algorithm	Mode of Use						
'24'	'A'	'B', 'N'						
MAC Length	2 N	The length of the MAC (TLen). Valid values are 04, 06, 08, 10, 12, 14, and 16 bytes.						
Number of bytes to encode message length	1 N	The length MLen in bytes required to store the message length. The maximum length of the message is $2^{8 \times \text{MLen}}$. Valid values are 2 to 8 bytes. MLen = 1 is reserved.						
Nonce length	2 N	The length of the Nonce field (Nlen). The length must be 15-MLen bytes.						
Nonce	n B	The Nonce value.						
Delimiter	1 A	Value ':'.						
Authentication Data Length	6 N	The length of the Authentication Data field (ALen). Zero if not required.						
Authentication Data	n B	The Authentication Data.						
Delimiter	1 A	Value ':'.						
For all versions, the following fields must be present:								
Encrypted Message Data length	4 N or 6 N	The length of the Encrypted Message Data. If Version is not present or = '1', this field consists of 4 digits. If Version = '2' or '3', this field consists of 6 digits.						
Encrypted Message Data	n B	The encrypted message data. If Version = '1' and '2', the Message Data is encrypted under the MS_KEY_CONF session key using AES in Counter (CTR) mode. If Version = '3', the Message Data is encrypted under the Transport Key using CCM. (Note the MAC is included in the Encrypted Message Data).						
MAC over Encrypted Message Data	8 B	The MAC using AES and MAC Algorithm 1 in ISO/IEC 9797-1 with padding method 2 over the Encrypted Message Data using the MS_KEY_MAC session key.						
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.						
Message Trailer	n A	Optional. Maximum length 32 characters.						

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'IX'.
Error Code	2 A	<p>'00': No error '01': MAC verification failed '06': Invalid message counter '80': Invalid Message Data length 'A1': Invalid LMK scheme 'D4': MS_KEY_CONF – key block error 'D5': MS_KEY_MAC – key block error 'D6': Invalid Version value 'D7': Message length exceeds 32K 'E1': Invalid cipher mode 'E2': Invalid MAC length 'E3': Invalid Number of bytes to encode message length value 'E4': Invalid Nonce length 'E5': Invalid Authentication Data length 'E6': Invalid Encrypted Message Data Length 'E7': Invalid key length Or a standard error code.</p>
If Error Code = 'D4' or 'D5', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
If Error Code = '00', the following 2 fields will be present:		
Message Data Length	4 N or 6 N	<p>The length of the Message Data field If Version is not present or = '1', this field consists of 4 digits. If Version field = '2' or '3', this field consists of 6 digits.</p>
Message Data	n B	The plaintext Message Data.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

10.6 JSON Web Token (JWT) Commands

The HSM provides the following host commands to support the encoding/decoding of a JSON Web Token (JWT) using JSON Web Signature and JSON Web Encryption.

Function	Command	Page
<i>JWT Encode</i>	JW (JX)	631
<i>JWT Decode</i>	JY (JZ)	635

JWT Encode

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: This command allows the building of a JSON Web Token (JWT) that is encoded in a JSON Web Encryption (JWE) block.

For JWE, the command allows building a payload containing plaintext that is encrypted and MAC protected to form a JWE encoded blob with compact serialization format (where || denotes concatenation):

```
BASE64URL (UTF8 (JWE Protected Header)) || '.' || BASE64URL (JWE Encrypted Key) || '.' ||
BASE64URL (JWE Initialization Vector) || '.' || BASE64URL (JWE Ciphertext) || '.' || BASE64URL
(JWE Authentication Tag)
```

For JWS, the command allows signing of message payloads to form a JWS encoded blob with compact serialization format (where || denotes concatenation):

```
BASE64URL (UTF8 (JWS Protected Header)) || '.' || BASE64URL (JWS Payload) || '.' ||
BASE64URL (JWS Signature)
```

For JWE, payloads may be plaintext JWTs. Encoding of keys in JWK format is not supported.

The following JWE Key Wrap mechanisms are currently supported:

```
"alg": "A128KW", "A192KW", "A256KW"
"alg": "A128GCMKW", "A192GCMKW", "A256GCMKW"
```

The following JWE Encryption mechanisms are currently supported:

```
"enc": "A128GCM", "A192GCM", "A256GCM"
"enc": "A128CBC-HS256", "A192CBC-HS384", "A256CBC-HS512"
```

The following JWE Key Wrap mechanisms are NOT currently supported:

```
"alg": "PBES2-HS256+A128KW", "PBES2-HS384+A192KW", "PBES2-HS512+A256KW"
"alg": "ECDH_ES_A128KW", "ECDH_ES_A192KW", "ECDH_ES_A256KW"
"alg": "dir"
"alg": "ECDH_ES",
"alg": "RSA1_5", "RSA_OAEP", "RSA_OAEP_256"
```

For JWS, payloads may be signed using RSA private keys.

The following JWS Signing mechanisms are currently supported:

```
"alg": "RS256", "RS384", "RS512"
"alg": "PS256", "PS384", "PS512"
```

Field	Length & Type	Details												
COMMAND MESSAGE														
Message Header	m A	Subsequently returned to the Host unchanged.												
Command Code	2 A	Value 'JW'.												
Message Format	1 N	The format of the JWT. Valid values are: '0': JWE in Compact Serialisation '1': JWS in Compact Serialisation												
Header Delimiter	1 A	Value '='. Optional. If present, the following two fields must be present.												
If Header Delimiter = '=', the following 2 fields apply:														
Protected Header Length	4 N	The length of the JWE/JWS Protected Header.												
Protected Header	n A	The JWE/JWS Protected Header in JSON format.												
If Message Format = '0', the following 3 fields apply:														
Encryption Mode	1 N	Only present if Message Format = '0': The cipher used to encrypt and MAC protect the message payload. Valid values are: '0': AES CBC encryption with HMAC SHA2 '1': AES GCM authenticated encryption												
Encryption IV Flag	1 N	Only present if Message Format = '0': Valid values are: '0': Generate random IV with command												
CEK Flag	1 N	Only present if Message Format = '0': Content Encryption Key (CEK) Flag. Valid values are '1': Generate a random CEK within command												
If Message Format = '0' and CEK Flag is '1', the following 3 fields apply:														
CEK Key Length	2 N	The length in bytes for the ephemeral key CEK. Valid values are 16, 24 or 32 bytes.												
Key Wrap Mode	1 N	The cipher for wrapping the Content Encryption Key (CEK). Valid values are: '0': AES key wrap with supplied transport key '1': AES GCM key wrapping with supplied transport key												
Wrapping Key	'S' + n A	If Key Wrap Mode is '0', the wrapping key should comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode Of Use</th> </tr> </thead> <tbody> <tr> <td>'K0'</td> <td>'A'</td> <td>'B', 'E', 'D'</td> </tr> </tbody> </table> If Key Wrap Mode is '1', the wrapping key should comply with: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode Of Use</th> </tr> </thead> <tbody> <tr> <td>'24'</td> <td>'A'</td> <td>'B', 'E', 'D'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode Of Use	'K0'	'A'	'B', 'E', 'D'	Key Usage	Algorithm	Mode Of Use	'24'	'A'	'B', 'E', 'D'
Key Usage	Algorithm	Mode Of Use												
'K0'	'A'	'B', 'E', 'D'												
Key Usage	Algorithm	Mode Of Use												
'24'	'A'	'B', 'E', 'D'												
If Message Format = '1', the following 4 fields apply:														
Signature Identifier	1 N	Identifier of the signature algorithm used to sign the message. Valid values are: '1': RSA												
Pad Mode Identifier	2 N	Identifier of the padding mode used in signature generation. '01': PKCS#1 v1.5 method (EMSA-PKCS1-v1_5) '04': PKCS#1 v2.1 method (EMSA-PSS)												
Hash Identifier	2 N	Identifier of the hash algorithm used to hash the message. Valid values are: '06': SHA-256 '07': SHA-384 '08': SHA-512												
Signing Key	'S' + n B	The key used to sign the data. The 'Signing Key' must comply with the following: <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode Of Use</th> </tr> </thead> <tbody> <tr> <td>'03'</td> <td>'R'</td> <td>'S', 'N'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode Of Use	'03'	'R'	'S', 'N'						
Key Usage	Algorithm	Mode Of Use												
'03'	'R'	'S', 'N'												

Message Data Item Count	2 N	The number of Message Data Items to load into a single message payload.
The following 4 fields must be repeated for each Message Data Item:		
Message Data Item Type	2 N	'00': Plaintext JWT.
Message Data Item Length	6 N	The length in bytes of the Message Data Item field.
Message Data Item	n A	The plaintext data.
Message Data Item Delimiter	1 A	Mandatory Delimiter. Value ';' (semi-colon).
All Message Data Item Delimiter	1 A	Mandatory Delimiter. Value ':' (colon).
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by licence; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'JX'.
Error Code	2 N	<p>'00': No error '85': Invalid Mask generation function '86': Invalid OAEP MGF Hash function '87': OAEP parameter error 'D1': Invalid Message Format 'D2': Invalid Message Data Item 'D3': Invalid encryption Mode 'D4': Invalid JSON format in header 'D5': Invalid CEK generation flag 'D6': Invalid key wrap mode 'D7': Wrapping key block error 'D8': Public key block error 'D9': Invalid Message Data Item length 'DA': Message Data Item key block error 'DB': Invalid CEK key length 'DC': Public key length error 'DD': Key not exportable 'DE': Maximum message size reached 'DF': Invalid Pad Mode Identifier 'E0': CEK key block error 'E1': Invalid Message Data Item Count 'E2': Invalid Encryption IV Flag 'E3': Invalid Signature Identifier 'E4': Invalid Hash Identifier 'E5': Signing Key block error 'E6': Invalid CEK flag 'E7': Invalid Encryption IV 'E8': Invalid Signing Key Usage for selected hash algorithm 'E9': Invalid Protected Header Length or a standard error code.</p>
If Error Code is 'D7', 'D8', 'DA' or 'E5', the following field will be present:		
Additional Error Code	2 A	The key block specific error code.
If Error Code is 'D2' or 'D9', the following field will be present:		
Additional Error Code	2 N	The number of the Message Data item in error.
If Error Code is '00', the following field will be present:		
JWT Length	6 N	The length of the JWT
JWT	n A	<p>If Message Format is '0', the JWT in JWE format: BASE64URL(UTF8(JWE Protected Header)) '.' BASE64URL(JWE Encrypted Key) '.' BASE64URL(JWE Initialization Vector) '.' BASE64URL(JWE Ciphertext) '.' BASE64URL(JWE Authentication Tag)</p> <p>If Message Format is '1', the JWT in JWS format: BASE64URL (UTF8 (JWS Protected Header)) '.' BASE64URL (JWS Payload) '.' BASE64URL (JWS Signature)</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

JWT Decode

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: This command supports the decoding of a JSON Web Token (JWT) in JWE format returning the plaintext message.

The JWE encoded blob in compact serialization format has the following format (where || denotes concatenation):

BASE64URL (UTF8 (JWE Protected Header)) || '.' || BASE64URL (JWE Encrypted Key) || '.' ||
BASE64URL (JWE Initialization Vector) || '.' || BASE64URL (JWE Ciphertext) || '.' || BASE64URL
(JWE Authentication Tag)

Prior to calling this command, the JWE/JWS Protected header will need to be decoded from base 64 encoded binary to string format in order to query the "alg" field to determine what unwrapping key needs to be provided in the command.

The following JWE mechanisms are supported:

```
"alg": "A128GCMKW", "A192GCMKW", "A256GCMKW"
"alg": "A128KW", "A192KW", "A256KW"
```

The following JWE Encryption mechanisms supported:

```
"enc": "A128GCM", "A192GCM", "A256GCM"
"enc": "A128CBC-HS256", "A192CBC-HS384", "A256CBC-HS512"
```

The following JWE Key wrap mechanisms NOT supported:

```
"alg": "PBES2-HS256+A128KW", "PBES2-HS384+A192KW", "PBES2-HS512+A256KW"
```

For JWS, payloads may be signed using RSA private keys.

The following JWS Signing mechanisms supported:

```
"alg": "RS256", "RS384", "RS512"
"alg": "PS256", "PS384", "PS512"
```

Field	Length & Type	Details												
COMMAND MESSAGE														
Message Header	m A	Subsequently returned to the Host unchanged.												
Command Code	2 A	Value 'JY'.												
Message Format	1 N	The format of the JWT. Valid values are: '0': JWE in Compact Serialisation '1': JWS in Compact Serialisation												
Message Data Length	6 N	The length of the Message Data.												
Message Data	n A	The JWT in Message Format.												
Delimiter	1 A	Value ';'.												
If Message Format = '0', the following field applies:														
Unwrap Key	'S' + n A	<p>The key to unwrap the JWE Encrypted Key. If 'alg' is A128/192/256GCMKW, the unwrap key should comply with:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode Of Use</th> </tr> </thead> <tbody> <tr> <td>'24'</td> <td>'A'</td> <td>'B', 'D', 'E'</td> </tr> </tbody> </table> <p>If 'alg' is A128/192/256KW, the unwrap key should comply with:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode Of Use</th> </tr> </thead> <tbody> <tr> <td>'K0'</td> <td>'A'</td> <td>'B', 'D', 'E'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode Of Use	'24'	'A'	'B', 'D', 'E'	Key Usage	Algorithm	Mode Of Use	'K0'	'A'	'B', 'D', 'E'
Key Usage	Algorithm	Mode Of Use												
'24'	'A'	'B', 'D', 'E'												
Key Usage	Algorithm	Mode Of Use												
'K0'	'A'	'B', 'D', 'E'												
If Message Format = '1', the following field applies:														
Signature Validation Key	'S' + n B	<p>The key to validate the JWS Encrypted Key. If 'alg' is RS256, RS384, RS512, PS256, PS384 or PS512, the signature validation key should comply with:</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Key Usage</th> <th>Algorithm</th> <th>Mode Of Use</th> </tr> </thead> <tbody> <tr> <td>'02'</td> <td>'R'</td> <td>'B', 'N', 'V'</td> </tr> </tbody> </table>	Key Usage	Algorithm	Mode Of Use	'02'	'R'	'B', 'N', 'V'						
Key Usage	Algorithm	Mode Of Use												
'02'	'R'	'B', 'N', 'V'												
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.												
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by licence; must be present if the above Delimiter is present.												
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.												
Message Trailer	n A	Optional. Maximum length 32 characters.												

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'JZ'.
Error Code	2 N	<p>'00': No error</p> <p>'D1': Invalid Message Format value</p> <p>'D2': Invalid Message Data length</p> <p>'D3': Message Data does not conform to Message Format</p> <p>'D4': Invalid JSON format in JWE Header</p> <p>'D5': Missing 'enc' field in JWE Header</p> <p>'D6': Missing 'alg' field in JWE Header</p> <p>'D7': Invalid 'alg' value</p> <p>'D8': Invalid 'enc' value</p> <p>'D9': Invalid 'cty' value</p> <p>'DA': Invalid 'kty' value</p> <p>'DB': Public key block error</p> <p>'DC': Invalid public key length</p> <p>'DD': Private key block error</p> <p>'DE': CEK key block error</p> <p>'DF': Unwrap key block error</p> <p>'E0': Invalid unwrap key length</p> <p>'E1': Invalid JWE Initialisation Vector length</p> <p>'E2': Missing tag or iv fields in header</p> <p>'E3': Unwrap key verification error</p> <p>'E4': Invalid CEK length</p> <p>'E5': Invalid PKCS format</p> <p>'E6': JWEAuthenticationTag verification error</p> <p>'E7': Invalid JSON or missing field in decrypted message.</p> <p>'E8': Validation Key block error</p> <p>or a standard error code.</p>
If Error Code is 'DB', 'DD', 'DE' or 'DF', the following fields will be present:		
Additional Error Code	2 A	The key block specific error code.
If Error Code is '00', the following fields will be present:		
Message Length	6 N	The length of the Message.
Message	n A	The decrypted JWT message.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

11 AS2805 Transaction Processing

11.1 AS2805 Commands

This document specifies the functions to be provided by a payShield 10K HSM to support the Australian AS2805 Standards. This document also provides the functionality to support the Australian Payments Clearing Association (APCA) Security Control Module specifications.

PIN Block 46 in *AS2805 Appendix K – AS2805.3 PIN block formats* is applicable to standard HSM PIN translate and verify function calls. The standard HSM function calls used are CA, CC, DA, DC, EA and EC.

A comparison guide between the APCA specifications and the Thales equivalent functions is provided in *AS2805 Appendix S – APCA Functional Specification Comparison Guide*. This is not a definitive guide but seeks to provide an equivalent where there is no direct comparison.

The payShield 10K provides the following host commands to support AS2805 operations:

Function	Command	Page
Generate a PIN Pad Acquirer Security Number	PK (PL)	640
Translate a PIN Block to Encryption under a Zone PIN Key	PO (PP)	642
Generate a Message Authentication Code AS2805.4 – 1985	PQ (PR)	644
Generate a Message Authentication Code (large messages)	C2 (C3)	646
Validate a Message Authentication Code AS2805.4 -1985	PS (PT)	648
Verify a Message Authentication Code (large messages)	C4 (C5)	650
Encrypt Data	PU (PV)	652
Decrypt Data	PW (PX)	654
Translate a PIN Block to Encryption under a PIN Encryption Key	D4 (D5)	656
Generate a KEKs Validation Request	E0 (E1)	658
Generate a KEKr Validation Response	E2 (E3)	660
Verify a PIN Pad Proof of End Point	E4 (E5)	662
Verify a Terminal PIN using the IBM Method (AS2805 6.4)	F0 (F1)	664
Verify a Terminal PIN using the VISA Method (AS2805 6.4)	F2 (F3)	666
Calculate KMACI	F4 (F5)	668
Generate a Random Number	C6 (C7)	670
Generate a PIN Pad Authentication Code	D0 (D1)	671
Encrypt a CPAT Authentication Value	D8 (D9)	672
Verify a PIN Pad Authentication Code	D2 (D3)	673
Generate a PIN Pad Proof of Endpoint (POEP)	E6 (E7)	674
Translate a PPASN from old to new LMK	QI (QJ)	675
Verify and Generate an IBM PIN Offset (of a customer selected PIN)	PY (PZ)	676
Verify and Generate a VISA PVV (of a customer selected PIN)	P0 (P1)	679

<i>Generate a VISA PVV (of a customer selected PIN)</i>	P2 (P3)	682
<i>Generate a Proof of Host value</i>	P4 (P5)	685
<i>Calculate a RSA Public Key Verification Code</i>	H2 (H3)	686

Generate a PIN Pad Acquirer Security Number

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate a PIN Pad Acquirer Security Number (PPASN) and return it encrypted under an Acquirer Key (KIA) and Variant 8 of LMK pair 14-15.

Notes: The PPASN is not a key and so will not be adjusted for odd parity.
If KIA is double length (1 A + 32 H) then output eKIAV88(PPASN) as per AS2805.6.4 § 7.2.4

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'PK'
Acquirer Key	16 H or 1 A + 32 H	KIA, encrypted under either Variant 1 or Variant 6 of LMK pair 14-15.
PIN Pad Serial Number	16 H	Optional PIN Pad Serial Number
Delimiter	1 A	Optional: If present the following field must be present. Value ';'
Acquirer Key flag	1 N	Optional field, present if delimiter is present. 1 = KIA under Variant 1 of LMK pair 14-15 2 = KIA under Variant 6 of LMK pair 14-15
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'PL'
Error Code	2 N	'00': No errors '10': KIA parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index
PPASN (LMK)	16 H	PPASN, encrypted under Variant 8 of LMK pair 14-15
PPASN (KIA)	16 H	PPASN, encrypted under the KIA. Variant 88 applied when 1 A + 32 H key used in input.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate a PIN Block to Encryption under a Zone PIN Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To translate a PIN block from encryption under a PIN Encryption Key (KPE) to encryption under a Zone PIN Key (ZPK).

Notes: The KPE is derived from a Terminal PIN Key (TPK) and two other values, the Systems Trace Audit Number (STAN) and the transaction amount. The method of derivation of the KPE varies between single and double length TPK. These are defined in AS2805 Appendix J – Derivation of the PIN Encryption Key.

The PIN block formats supported by the HSM are either given in Ref.2, Chapter 3. or a "zero" PIN block. The HSM will identify the "zero" PIN block type and translate it accordingly.

"Zero" PIN block defined in AS2805 Appendix K – AS2805.3 PIN block formats.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'PO'
Zone PIN Key	16 H or 1 A + 32 H or 1 A + 48 H	ZPK, encrypted under LMK pair 06-07
Terminal PIN Key	16 H or 1 A + 32 H	TPK, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
STAN	6 N	Systems Trace Audit Number
Transaction Amount	12 N	Transaction amount
Incoming PIN Block Format Code	2 N	A valid PIN block format code
Outgoing PIN Block Format Code	2 N	A valid PIN block format code
Incoming PIN Block	16 H	PIN block, encrypted under KPE
Primary Account Number (PAN)	12 N	Primary Account number, used in PIN Block Format 01 or 04
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'PP'
Error Code	2 N	<p>'00': No errors '10': TPK parity error '11': ZPK parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '20': PIN block error '21': Invalid user storage index '23': Invalid PIN block format code '24': PIN length error '88': Warning AS2805.3 "zero" PIN block received</p>
Outgoing PIN Block	16 H	PIN block, encrypted under the ZPK
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a Message Authentication Code AS2805.4 – 1985

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate a Message Authentication Code (MAC) using either a Zone Authentication Key (ZAK) or a Terminal Authentication Key (TAK).

Notes: The method of generating the MAC is defined in AS2805.4 (1985).

The HSM input and output buffers can support 2K bytes of data. It is recommended that the Authentication Data field in the command message is no greater than 1800 bytes.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'PQ'
Key Flag	1 N	Flag to indicate which authentication key is used '0': ZAK, encrypted under LMK pair 26-27 '1': TAK, encrypted under LMK pair 16-17
Authentication Key	16 H	ZAK or TAK, encrypted under relevant LMK pair
Length	3 H	Number of characters or bytes of data to be authenticated.
Authentication Data	n B	Data to be authenticated.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'PR'
Error Code	2 N	'00': No errors '10': ZAK or TAK parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '80': Invalid data length
MAC	8 H	MAC, calculated on the data, using the given key
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a Message Authentication Code (large messages)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate a MAB for a large message using either a TAK or a ZAK. This command supports ANSI X9.9, X9.19, AS2805.4.1 (2001) standards.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'C2'
Message Block Number	1 N	Message block processing number: '0': Only Block '1': First Block '2': A Middle Block '3': Last Block
Key Type	1 N	Key type: '0': TAK (Terminal Authentication Key) '1': ZAK (Zone Authentication Key) '2': TAKs (Send Terminal Authentication Key) '3': ZAKs (Send Zone Authentication Key)
MAC generation Mode	1 N	Mode: '0': X9.9 '1': X9.19 '2': AS2805.4.1 (2001) MAB output '3': AS2805.4.1 (2001) MAC output
Message Type	1 N	Message Type '0': Message data is binary '1': Message data is expanded Hex
Key	16 H or 1 A + 32 H or 1 A + 48 H	Key, encrypted under appropriate LMK pair TAK under LMK pair 16 – 17 ZAK under LMK pair 26 – 27 TAKs under LMK pair 16 – 17 variant 1 ZAKs under LMK pair 26 – 27 variant 1
IV	16 H	Initialization value, present only when message block number is 2 or 3. Encrypted under LMK pair 16-17 variant 3.
Message Length	4 H	Length of Message to be MAC'd.
Message Block	n H	The message block in binary format.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'C3'
Error Code	2 N	<p>'00': No errors '03': Invalid Message Type Code '04': Invalid Key Type Code '05': Invalid Message Block Number '06': Invalid MAC generation Mode '07': Invalid key length '10': KEY parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '80': Incorrect input data length</p>
MAB / MAC	8 H or 16 H	<p>Used as IV for next block when message block number is 1 or 2. Encrypted under LMK pair 16-17 variant 3. Used as message authenticator when message block is 0 or 3 If MAC generation mode = 3 output is MAC (8H)</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Validate a Message Authentication Code AS2805.4 -1985

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To validate a Message Authentication Code (MAC) using either a Zone Authentication Key (ZAK) or a Terminal Authentication Key (TAK).

Notes: The method of generating the MAC is defined in AS2805.4 (1985).

The input and output buffers can support 2K bytes of data. It is recommended that the Authentication Data field in the command message is no greater than 1800 bytes.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'PS'
Key Flag	1 N	Flag to indicate which authentication key is used '0': ZAK, encrypted under LMK pair 26-27 '1': TAK, encrypted under LMK pair 16-17
Authentication Key	16 H	ZAK or TAK, encrypted under relevant LMK pair
MAC	8 H	MAC, for validation
Length	3 H	Number of characters or bytes.
Authentication Data	n B	Data to be authenticated.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'PT'
Error Code	2 N	<p>'00': No errors '01': MAC validation failure '10': ZAK or TAK parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '80': Invalid data length</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a Message Authentication Code (large messages)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To verify a MAC for a large message using either a TAK or a ZAK. This command supports ANSI X9.9, X9.19, AS2805.4.1 (2001) standards.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'C4'
Message Block Number	1 N	Message block processing number: '0': Only Block '1': First Block '2': A Middle Block '3': Last Block
Key Type	1 N	Key type: '0': TAK (Terminal Authentication Key) '1': ZAK (Zone Authentication Key) '2': TAKr (Receive Terminal Authentication Key) '3': ZAKr (Receive Zone Authentication Key)
MAC verification Mode	1 N	Mode: '0': X9.9 '1': X9.19 '2': AS2805.4.1 (2001)
Message Type	1 N	Message Type '0': Message data is binary '1': Message data is expanded Hex
Key	16 H or 1 A + 32 H or 1 A + 48 H	Key, encrypted under appropriate LMK pair TAK under LMK pair 16 – 17 ZAK under LMK pair 26 – 27 TAKr under LMK pair 16 – 17 variant 2 ZAKr under LMK pair 26 – 27 variant 2
IV	16 H	Initialization value, present only when message block number is 2 or 3. Encrypted under LMK pair 16-17 variant 3.
MAC	8 H	MAC for verification, present only when message block number is either 0 or 3
Message Length	4 H	Length of Message to be MAC'd
Message Block	n B	The message block either in binary format.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'C5'
Error Code	2 N	<p>'00': No errors '01': MAC verification failure '03': Invalid Message Type Code '04': Invalid Key Type Code '05': Invalid Message Block Number '06': Invalid MAC Verification Mode '07': Invalid key length '10': KEY parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '80': Incorrect input data length</p>
MAB	16 H	MAB encrypted under LMK pair 16-17 variant 3. Only output if message block number is 1 or 2. Used as IV for next block.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Encrypt Data

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To encrypt a block of data, using either a Zone Encryption Key (ZEK) or a Terminal Encryption Key (TEK).

Notes: The modes of encryption supported by this command are Electronic Codebook (ECB), Cipher Block Chaining (CBC), 8-bit Cipher Feedback (CFB-8), and OFB (8 Bit or 8 Byte) - see AS2805.5.2 (Ref.8.2).

The input and output buffers can support 2K bytes of data. It is recommended that the Plaintext Data field in the command message is no greater than 1800 bytes.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'PU'
Key Flag	1 N	Flag to indicate which encryption key is used '0': ZEK, encrypted under LMK pair 30-31 '1': TEK, encrypted under LMK pair 32-33 '2': ZEKs, encrypted under LMK pair 30-31 variant 1 '3': TEKs, encrypted under LMK pair 32-33 variant 1
Encryption Key	16 H or 1 A + 32 H or 1 A + 48 H	ZEK or TEK, encrypted under relevant LMK pair
Encryption Mode	1 N	Flag to indicate the mode of encryption '0': ECB mode of encryption '1': CBC mode of encryption '2': CFB-8 mode of encryption '3': OFB mode of encryption
Initialization Value	16 H	Initialization value, used with the CBC, CFB-8 or OFB modes of encryption
Plaintext Value (j)	1 N	Only used with OFB mode, value of either 1 for 1 byte (8bits) feedback or 8 for 8 byte (64bits) feedback
Length	3 H	Length (in bytes) of data to be encrypted
Plaintext Data	n B	Data to be encrypted.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'PV'
Error Code	2 N	'00': No errors '10': ZEK or TEK parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '80': Invalid data length
Encrypted Data	n B	Encrypted data.
OCV	16 H	Output Chaining Value, only used when OFB mode is used
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Decrypt Data

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To decrypt a block of data, using either a Zone Encryption Key (ZEK) or a Terminal Encryption Key (TEK).

Notes: The modes of encryption supported by this command are Electronic Codebook (ECB), Cipher Block Chaining (CBC) or 8-bit Cipher Feedback (CFB-8) - see AS2805.5.2 (Ref.8.2). The HSM input and output buffers can support 2K bytes of data. It is recommended that the Encrypted Data field in the command message is no greater than 1800 bytes.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'PW'
Key Flag	1 N	Flag to indicate which encryption key is used '0': ZEK, encrypted under LMK pair 30-31 '1': TEK, encrypted under LMK pair 32-33 '2': ZEKr, encrypted under LMK pair 30-31 Variant 2 '3': TEKr, encrypted under LMK pair 32-33 Variant 2
Encryption Key	16 H or 1 A + 32 H or 1 A + 48 H	ZEK or TEK, encrypted under relevant LMK pair
Encryption Mode	1 N	Flag to indicate the mode of encryption '0': ECB mode of encryption '1': CBC mode of encryption '2': CFB-8 mode of encryption '3': OFB mode of encryption
Initialization Value	16 H	Initialization value, used with the CBC, CFB-8 or OFB modes of encryption
Plaintext Value (j)	1 N	Only used with OFB mode, value of either 1 for 1 byte (8bits) feedback or 8 for 8 byte (64bits) feedback
Length	3 H	Length (in bytes) of data to be decrypted
Encrypted Data	n B	Data to be decrypted.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'PX'
Error Code	2 N	'00': No errors '10': ZEK or TEK parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '80': Invalid data length
Plaintext Data	n B	Plaintext data.
OCV	16 H	Output Chaining Value, only used when OFB mode is used
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate a PIN Block to Encryption under a PIN Encryption Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To translate a PIN Block from encryption under a Terminal PIN Key (TPK) to encryption under a PIN Encryption Key (KPE).

Notes: The input PIN block will be either a standard AS2805 (ANSI X9.8) PIN block or a zero PIN block. The HSM will identify the PIN block type and translate it accordingly.
This command supports Variant LMKs only.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'D4'
Terminal PIN Key	16 H or 1 A + 32 H or 1 A + 48 H	TPK, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
PIN Encryption Key	16 H or 1 A + 32 H or 1 A + 48 H	KPE, encrypted under LMK pair 06-07
PIN Block	16 H	PIN block, encrypted under TPK
Primary Account Number (PAN)	12 N	Rightmost 12 digits of the Primary Account Number (PAN), excluding the check digit.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'D5'
Error Code	2 N	<p>'00': No errors '10': KTP parity error '11': KPE parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '20': PIN block error '21': Invalid user storage index '24': PIN length error '88': Warning: AS2805.3 "zero" PIN block received</p>
PIN Block	16 H	PIN block, encrypted under the KPE
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a KEKs Validation Request

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

- Function: To generate a random key (KR) and encrypt it with a variant of a double length Key Encrypting Key (KEKs). In addition, KR is inverted (to form KRR) and the result encrypted with another variant of the KEKs.
- Notes: The definition of the KEKs variants is given in AS2805 Appendix D – Key Encrypting Key Variants.
If no key scheme flags are supplied, the HSM generates a single length KR & KRR, and the single length KEKs variants are used. If key scheme flags are used the HSM generates the appropriate length KR & KRR as per the scheme and appropriate KEKs variants for the length of KR are used.
If the Key type flag is used, the key scheme flags must also be present.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'E0'
KEKs / Zone Master Key	32 H or 1 A + 32 H or 1 A + 48 H	KEKs, encrypted under LMK pair 04-05 variant 4 or ZMK, encrypted under LMK pair 04-05
Delimiter	1 A	Optional: If present the following three fields must be present. Value ';'
Key Scheme KEKs / ZMK	1 A	Optional. Key Scheme for encrypting keys under KEKs / ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Delimiter	1 A	Optional: If present the following field must be present. Value ';'
Flag	1 N	Optional flag to indicate if KEKs or ZMK is used. 1 = KEKs; 2 = ZMK ONLY AVAILABLE IF PRECEDING KEY SCHEME IS USED
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'E1'
Error Code	2 N	'00': No errors '10': KEKs parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '26': Invalid Key Scheme '27': Incompatible key length '28': Invalid key type
KRs	16 H or 1 A + 32 H or 1 A + 48 H	KRs, encrypted with variant 7 of KEKs or variant 7 of ZMK (see <i>AS2805 Appendix D – Key Encrypting Key Variants</i>)
KRr	16 H or 1 A + 32 H or 1 A + 48 H	KRr (i.e. inverted KR), encrypted with variant 8 of KEKs or variant 8 of ZMK (see <i>AS2805 Appendix D – Key Encrypting Key Variants</i>)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a KEKr Validation Response

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To receive a random key (KRs) encrypted under a variant of a double length Key Encrypting Key (KEKr), compute from KRs another value, denoted KRr and encrypt it under another variant of the KEKr

Notes: The definition of the KEKr variants is given in AS2805 Appendix D – Key Encrypting Key Variants.

If no key scheme flags are supplied, the HSM will use the single length KEKr variant for the input KRs and output KRr, regardless of length of the KRs. If key scheme flags are supplied the HSM uses the appropriate variant of KEKr, depending on length for the input KRs and output KRr.

If the Key type flag is used, the key scheme flags must also be used.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'E2'
KEKr / Zone Master Key	32 H or 1 A + 32 H or 1 A + 48 H 16 H or 1 A + 32 H or 1 A + 48 H	KEKr, encrypted under LMK pair 04-05 variant 3 or ZMK, encrypted under LMK pair 04-05 KRs, encrypted with variant 7 of KEKr or variant 7 of ZMK (see <i>AS2805 Appendix D – Key Encrypting Key Variants</i>)
KRs	1 A	Optional: If present the following three fields must be present. Value ':'
Delimiter	1 A	Optional. Key Scheme for encrypting keys under KEKr
Key Scheme KEKr	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Scheme LMK	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Key Check Value type	1 A	Optional: If present the following field must be present. Value ':'
Delimiter	1 A	Optional flag to indicate if KEKr or ZMK is used. 1 = KEKr; 2 = ZMK
Flag	1 N	ONLY AVAILABLE IF PRECEDING KEY SCHEME IS USED
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'E3'
Error Code	2 N	'00': No errors '10': KEKr parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '26': Invalid Key Scheme '27': Incompatible key length '28': Invalid key type
KRr	16 H or 1 A + 32 H or 1 A + 48 H	KRr (i.e. inverted KRs, encrypted with variant 8 of KEKr or variant 8 of ZMK (see <i>AS2805 Appendix D – Key Encrypting Key Variants</i>)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a PIN Pad Proof of End Point

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To verify a PIN Pad Proof of End point (POEP).

Notes: The proof of end point (POEP) is generated by the PIN pad by encrypting the PPASN (PIN Pad Acquirer Secret Number) with one of the Terminal Master Keys (known as KEK1 or KEK2 in AS2805 Part 6.4) or a Terminal Encryption Key. Only the left 32 bits is used for the POEP. This command will validate a proof of endpoint provided by the PIN Pad.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'E4'
Flag	1 N	Flag to indicate which TMK is used '1' if TMK1 is used '2' if TMK2 is used '3' if TEKr is used
Terminal Master Key or Terminal Encryption Key	32 H or 1 A + 32 H or 1 A + 48 H	TMK, encrypted under a Variant of LMK pair 14-15 (Variant 1 if Flag = 1; Variant 2 if Flag = 2). TEKr, encrypted under LMK pair 32-33 variant 2
PPASN	16 H	PIN Pad Acquirer Secret Number encrypted under Variant 8 of LMK pair 14-15
POEP	8 H	Proof of end point to be validated
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

payShield 10K Core Host Commands

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'E5'
Error Code	2 N	<p>'00': No errors '01': POEP does not Verify '10': TMK parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '88': Warning AS2805.3 "zero" PIN block received</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a Terminal PIN using the IBM Method (AS2805 6.4)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To verify a PIN from a terminal using the IBM 3624 method.

Notes: The PIN block shall be as specified in AS2805.3. The KPE shall be calculated as specified in AS2805.6.4 (Refer to *AS2805 Appendix J – Derivation of the PIN Encryption Key*)
The decimalization table can be stored in user storage and referenced in the same way as keys. The decimalization table of 16 digits must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, Error Code 25 is returned.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'F0'
TPK	16 H or 1 A + 32 H	The TPK under which the PIN block is encrypted; encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
PVK	16 H or 1 A + 32 H or 1 A + 48 H	PVK encrypted under LMK pair 14-15 variant 0
STAN	6 N	Systems Trace Audit Number
Transaction Amount	12 N	Transaction Amount
PIN block	16 H	The PIN block encrypted under the KPE
PIN block format code	2 N	One of the valid format codes.
Check length	2 N	The minimum PIN length.
Account number	12 N	The 12 right-most digits of the PAN, excluding the check digit.
Decimalization table	16 N or 16 H or 'K' + 3 H	16 N when using Plaintext decimalization tables. 16 H when using Encrypted decimalization tables. 'K' + 3 H to reference a decimalization table held in the HSM's User Storage Area.
PIN validation data	12A	User-defined data consisting of hexadecimal characters and the character N, which indicates to the HSM where to insert the last 5 digits of the PAN.
Offset	12H	IBM offset value, left-justified and padded with F.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

payShield 10K Core Host Commands

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'F1'
Error Code	2 N	<p>'00': No errors. '01': Warning: Verification failure. '02': Warning: PVK not single length '06': Invalid offset length '10': TPK parity error. '11': PVK parity error. '12': No keys or table loaded in user storage. '13': LMK error; report to supervisor. '15': Error in input data. '20': PIN block error. '21': Invalid user storage index. '23': Invalid PIN block format code. '24': PIN is fewer than 4 or more than 12 digits. '25': Decimalization table error. '88': Warning: AS2805.3 "zero" PIN block received</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a Terminal PIN using the VISA Method (AS2805 6.4)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To verify a PIN from a terminal using the VISA method.

Notes: The PIN block shall be as specified in AS2805.3. The KPE shall be calculated as specified in AS2805.6.4 (Refer to *AS2805 Appendix J – Derivation of the PIN Encryption Key*)

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'F2'
TPK	16 H or 1 A + 32 H	The TPK under which the PIN block is encrypted; encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
PVK pair	32 H or 1 A + 32 H or 1 A + 48 H	PVK encrypted under LMK pair 14-15 variant 0
STAN	6 N	Systems Trace Audit Number
Transaction Amount	12 N	Transaction Amount
PIN block	16 H	The PIN block encrypted under the KPE
PIN block format code	2 N	One of the valid format codes.
Account number	12 N	The 12 right-most digits of the PAN, excluding the check digit.
PVKI	1 N	The PVKI (should be between 0 and 6).
PVV	4 N	The PIN Verification Value
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'F3'
Error Code	2 N	<p>'00': No errors. '01': Verification failure. '10': TPK parity error. '11': PVK parity error. '12': No keys or table loaded in user storage. '13': LMK error; report to supervisor. '15': Error in input data. '20': PIN block does not contain valid values '21': Invalid user storage index. '23': Invalid PIN block format code. '24': PIN is fewer than 4 or more than 12 digits. '88': Warning: AS2805.3 "zero" PIN block received</p>
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Calculate KMACI

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To calculate an initial MAC key.

Notes: The key scheme flags are ignored in processing.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'F4'
KIA	16 H or 1 A + 32 H or 1 A + 48 H	The KIA encrypted under LMK pair 14-15 Variant 6
Flag	1 N	Flag to denote format of AIIC following: '1': 11 N '2': 16 H '3': 32 H
AIIC	11 N or 16 H or 32 H	The Acquirer Institution Identification Code
Delimiter	1 A	Optional: If present the following three fields must be present. Value ','
Key Scheme ZMK	1 A	Optional. Key Scheme for encrypting keys under ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'F5'
Error Code	2 N	'00': No errors. '10': KIA parity error. '12': No keys or table loaded in user storage. '13': LMK error; report to supervisor. '15': Error in input data. '21': Invalid user storage index. '26': Invalid Key Scheme '27': Incompatible key length '28': Invalid key type
KMACI	16 H or 1 A + 32 H	The KMACI encrypted under LMK pair 16-17
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a Random Number

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input checked="" type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate a random 64 bit number.

Notes:

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'C6'
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'C7'
Error Code	2 N	'00': No errors
Random Number	16 H	Random Number
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a PIN Pad Authentication Code

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate a PIN Pad Authentication Code (PPAC).

Notes: The PPAC is formed by encrypting the PIN Pad Serial Number (PPSN) with the acquirer Master Key Encrypting Key (KMA) and using the leftmost 32 bits of the result as the PPAC.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'D0'
KMA	16 H or 1 A + 32 H or 1 A + 48 H	KMA, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
PPSN	16 N	PIN Pad Serial Number
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'D1'
Error Code	2 N	'00': No errors '10': KMA parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index
PPAC	8 H	PIN Pad Authentication Code
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Encrypt a CPAT Authentication Value

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To encrypt a CPAT Authentication Value (CAV).

Notes: The CAV is encrypted with a privacy key, denoted KD, which is derived from the current value of the Transaction Key (KT), the Systems Trace Audit Number (STAN) and the Card Acceptor Terminal Identification (CATID) according to the method defined in AS2805 Appendix N – B: Derivation of Data Values for 16H and AS2805 Appendix N – E: Privacy Key Derivation for 32H key lengths.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'D8'
KT	16 H or 1 A + 32 H	KT, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
STAN	6 N	Systems Trace Audit Number
CATID	16 H	Card Acceptor Terminal Identification
CAV	16 H	CPAT Authentication Value
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'D9'
Error Code	2 N	'00': No errors '10': KT parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index
Encrypted CAV	16 H	CAV, encrypted with KD
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a PIN Pad Authentication Code

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To verify a PIN Pad Authentication Code (PPAC).

Notes: The PPAC is formed by encrypting the PIN Pad Serial Number (PPSN) with the Acquirer Master Key Encrypting Key (KMA) and using the leftmost 32 bits of the result as the PPAC.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'D2'
KMA	16 H or 1 A + 32 H or 1 A + 48 H	KMA, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
PPSN	16 N	PIN Pad Serial Number
PPAC	8 H	PIN Pad Authentication Code
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'D3'
Error Code	2 N	'00': No errors '01': PPAC Verification error '10': KMA parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a PIN Pad Proof of Endpoint (POEP)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate a PIN Pad Proof of End point (POEP).

Notes: The proof of end point (POEP) is generated by the PIN pad by encrypting the PPASN (PIN Pad Acquirer Secret Number) with one of the Terminal Master Keys (known as KEK1 or KEK2 in AS2805 Part 6.4) or a Terminal Encryption Key. Only the left 32 bits is used for the POEP.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'E6'
Flag	1 N	Flag to indicate which TMK is used '1': if TMK1 is used '2': if TMK2 is used '3': if TEKs is used
Terminal Master Key or Terminal Encryption Key	32 H or 1 A + 32 H or 1 A + 48 H	TMK, encrypted under a Variant of LMK pair 14-15 (Variant 1 if Flag = 1; Variant 2 if Flag = 2). TEKs, encrypted under LMK pair 32-33 variant 1
PPASN	16 H	PIN Pad Acquirer Secret Number encrypted under Variant 8 of LMK pair 14-15
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'E7'
Error Code	2 N	'00': No errors '01': TMK parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index
Generated POEP	8 H	Generated POEP
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate a PPASN from old to new LMK

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To translate a PPASN from encrypted under the old LMK, held in key change storage, to encryption under a new LMK.

Notes: For details of loading the old LMK into Key Change Storage see Ref 3. The PPASN is not a key so will not be checked for parity.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'QI'
PPASN	16 H	PIN PAD Acquirer Security Number encrypted under old LMK 14-15 variant 8 held in key change storage
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'QJ'
Error Code	2 N	'00': No errors '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index
PPASN	16 H	PIN PAD Acquirer Security Number encrypted under new LMK 14-15 variant 8
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify and Generate an IBM PIN Offset (of a customer selected PIN)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To Verify an IBM PIN Offset using the AS2805 6.4 key scheme, and if successful, generate the PIN offset of the customer selected PIN using the IBM 3624 method. The current and new PINs are supplied in encrypted PIN Blocks.

Notes: The PIN blocks shall be as specified in AS2805.3. The KPE's shall be calculated as specified in AS2805.6.4 (Refer to *AS2805 Appendix J – Derivation of the PIN Encryption Key*)
The decimalisation table can be stored in user storage and referenced in the same way as keys. The decimalisation table of 16 digits must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, error code 25 is returned.

Caution: The behaviour of this command is affected by the following CS (Configure Security) console command settings:

Decimalization Table: Encrypted/Plaintext [E/P]

- When set to 'E' (the default setting), the supplied decimalization table must be encrypted (using console command ED), and will consist of 16 hexadecimal digits.
- When set to 'P', the supplied decimalization table must be plaintext, and will consist of 16 decimal digits.

Decimalization Table checks enabled? [Yes/No]

- When set to 'Yes' (the default setting), the decimalization table must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, error code 25 is returned.
- When set to 'No', the decimalization table is not checked.

Enable support for variable length PIN offset? [Yes/No]

- When set to 'No' (the default setting), the length of the generated Offset is determined by the value of the Check Length parameter. This setting makes the command backward compatible with previous versions of HSM software.
- When set to 'Yes', the length of the generated Offset matches the length of the input PIN.

Enable Weak PIN checking? [Yes/No]

Check new PINs using global list of weak PINs: [Yes/No]

Check new PINs using local list of weak PINs: [Yes/No]

Check new PINs using rules: [Yes/No]

- Refer to the *payShield 10K Security Operations* manual for full details on how these settings can prevent the generation of 'weak' PINs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'PY'
TPK	32 H or 1 A + 32 H	The TPK under which the PIN block is encrypted; encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
PVK	32 H or 1 A + 32 H or 1 A + 48 H	PVK encrypted under LMK pair 14-15 variant 0
STAN	6 N	Systems Trace Audit Number
Transaction Amount	12 N	Transaction Amount
Current PIN block	16 H	The PIN block encrypted under the KPE
PIN block format code	2 N	One of the valid format codes.
Check length	2 N	The minimum PIN length.
Account number	12 N or 18 N	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the PAN, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the PAN, excluding the check digit, right-justified and padded with X'F' on the left if necessary
Old Decimalization table	16 N or 16 H or 'K' + 3 H	16 N if console CS cmd is set for Plaintext decimalisation tables. 16 H if console CS cmd is set for Encrypted decimalisation tables 'K' + 3 H if the decimalization table is held in the HSM's User Storage Area
PIN validation data	12 A or 1 A + 16 H	User-defined data consisting of hexadecimal characters and the character N, which indicates to the HSM where to insert the last 5 digits of the PAN. or User-defined data consisting of the ASCII character 'P' followed by 16 hexadecimal digits which will be used as input to the PIN generation algorithm.
Current Offset	12 H	IBM offset value, left-justified and padded with F.
New PIN block	16 H	The New PIN block encrypted under the KPE
New Decimalization table	16 N or 16 H or 'K' + 3 H	16 N if console CS cmd is set for Plaintext decimalisation tables. 16 H if console CS cmd is set for Encrypted decimalisation tables 'K' + 3 H if the decimalization table is held in the HSM's User Storage Area
Delimiter	1 A	Value '*' Only present if the following Excluded PIN fields are present
Excluded PIN Count	2 N	'00' .. '99': The number of excluded PINs listed in the following Excluded PIN Table
Excluded PIN Length	2 N	'04' .. '12' The length of each excluded PIN in the following Excluded PIN Table Only present if Excluded PIN Count > '00'
Excluded PIN Table	n N	A list of PINs to be excluded. The length of this field will be Excluded PIN Count multiplied by the Excluded PIN Length characters Only present if Excluded PIN Count > '00'
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'PZ'
Error Code	2 N	<p>'00': No errors '01': Verification failure '06': Invalid offset length '10': TPK parity error '11': PVK parity error '12': No keys or table loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '20': PIN block error '21': Invalid user storage index '23': Invalid PIN block format code '24': PIN is fewer than 4 or more than 12 digits '25': Decimalization table error '81': PIN length mismatch '86': PIN is determined to be 'weak' '88': AS2805.3 "zero" PIN block received </p>
New Offset	12 H	The new offset value; left justified and padded with 'F'
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify and Generate a VISA PVV (of a customer selected PIN)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To Verify a VISA PVV, and if successful, generate the PVV of the customer selected PIN using the VISA method. The Current & New PINs are supplied in an encrypted PIN Block.

Notes: The PIN blocks shall be as specified in AS2805.3. The KPE's shall be calculated as specified in AS2805.6.4 (Refer to *AS2805 Appendix J – Derivation of the PIN Encryption Key*)
 VISA defines the PIN Verification Key Indicator (PVKI) to be between 0 and 6. The HSM does not enforce this restriction.
 This command will optionally check the input PIN in order to exclude 'weak' PINs.
 The PIN change process requires verifying the existing PIN and creating a PVV for the new PIN.

Caution: The behavior of this command is affected by the following CS (Configure Security) console command setting:

Enable Weak PIN checking? [Yes/No]

Check new PINs using global list of weak PINs: [Yes/No]

Check new PINs using local list of weak PINs: [Yes/No]

Check new PINs using rules: [Yes/No]

- Refer to the *payShield 10K Security Operations* manual for full details on how these settings can prevent the generation of 'weak' PINs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'P0' (P-zero)
TPK	32 H or 1 A + 32 H	The TPK under which the PIN block is encrypted; encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
PVK pair	32 H or 1 A + 32 H or 1 A + 48 H	PVK encrypted under LMK pair 14-15 variant 0.
STAN	6 N	Systems Trace Audit Number
Transaction Amount	12 N	Transaction Amount
Current PIN block	16 H	The Current PIN block encrypted under the KPE
PIN block format code	2 N	One of the valid format codes.
Account number	12 N or 18 N	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the PAN, excluding the check digit, For PIN Block format 04, this is an 18 digit field consisting of the PAN, excluding the check digit, right-justified and padded with X'F on the left if necessary
PVKI	1 N	The PVKI (value 0 to 9).
Current PVV	4 N	The PIN Verification Value for the current PIN
New PIN Block	16 H	The New PIN block encrypted under the KPE
Delimiter	1 A	Value '*' Only present if the following Excluded PIN fields are present
Excluded PIN Count	2 N	'00' .. '99': The number of excluded PINs listed in the following local Excluded PIN Table
Excluded PIN Length	2 N	'04' .. '12' The length of each excluded PIN in the following local Excluded PIN Table Only present if Excluded PIN Count > '00'
Excluded PIN Table	n N	A local list of PINs to be excluded. The length of this field will be Excluded PIN Count multiplied by the Excluded PIN Length characters Only present if Excluded PIN Count > '00'
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

payShield 10K Core Host Commands

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'P1'
Error Code	2 N	<p>'00': No errors. '01': PIN Verification failure. '10': TPK parity error. '11': PVK parity error. '12': No keys or table loaded in user storage. '13': LMK error; report to supervisor. '15': Error in input data. '20': PIN block does not contain valid values '21': Invalid user storage index. '23': Invalid PIN block format code. '24': PIN is fewer than 4 or more than 12 digits. '27': PVK not double length '81': PIN length mismatch '86': PIN is determined to be 'weak' '88': Warning: AS2805.3 "zero" PIN block received </p>
New PVV	4 N	The PVV for the new PIN
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a VISA PVV (of a customer selected PIN)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Generate a 4 digit VISA PVV. The PIN (for which a PVV is required) is supplied in an encrypted PIN Block.

Notes: The PIN blocks shall be as specified in AS2805.3. The KPE's shall be calculated as specified in AS2805.6.4 (Refer to *AS2805 Appendix J – Derivation of the PIN Encryption Key*)
VISA defines the PIN Verification Key Indicator (PVKI) to be between 0 and 6. The HSM does not enforce this restriction.
This command will optionally check the input PIN in order to exclude 'weak' PINs.

Caution: The behavior of this command is affected by the following CS (Configure Security) console command setting:

Enable Weak PIN checking? [Yes/No]

Check new PINs using global list of weak PINs: [Yes/No]

Check new PINs using local list of weak PINs: [Yes/No]

Check new PINs using rules: [Yes/No]

- Refer to the *payShield 10K Security Operations* manual for full details on how these settings can prevent the generation of 'weak' PINs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'P2'
TPK	32 H or 1 A + 32 H	The TPK under which the PIN block is encrypted; encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
PVK pair	32 H or 1 A + 32 H or 1 A + 48 H	PVK encrypted under LMK pair 14-15 variant 0
STAN	6 N	Systems Trace Audit Number
Transaction Amount	12 N	Transaction Amount
PIN block	16 H	The PIN block encrypted under the KPE
PIN block format code	2 N	One of the valid format codes.
Account number	12 N or 18 N	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the PAN, excluding the check digit, For PIN Block format 04, this is an 18 digit field consisting of the PAN, excluding the check digit, right-justified and padded with X'F on the left if necessary
PVKI	1 N	The PVKI (value 0 to 9).
Delimiter	1 A	Value '*' Only present if the following Excluded PIN fields are present
Excluded PIN Count	2 N	'00' .. '99': The number of excluded PINs listed in the following Excluded PIN Table
Excluded PIN Length	2 N	'04' .. '12' The length of each excluded PIN in the following Excluded PIN Table Only present if Excluded PIN Count > '00'
Excluded PIN Table	n N	A list of PINs to be excluded. The length of this field will be Excluded PIN Count multiplied by the Excluded PIN Length characters Only present if Excluded PIN Count > '00'
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'P3'
Error Code	2 N	<p>'00': No errors. '10': TPK parity error. '11': PVK parity error. '12': No keys or table loaded in user storage. '13': LMK error; report to supervisor. '15': Error in input data. '20': PIN block does not contain valid values '21': Invalid user storage index. '23': Invalid PIN block format code. '24': PIN is fewer than 4 or more than 12 digits. '27': PVK not double length '81': PIN length mismatch '86': PIN is determined to be 'weak' '88': AS2805.3 "zero" PIN block received </p>
PVV	4 N	The PVV for the PIN
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a Proof of Host value

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To generate a value for the host to send to the PIN pad to prove the host is the bona fide host for the terminal. As per AS2805 6.4 terminal key management.

Notes: The One Way Function is as specified in AS2805.5.4. (Refer to *AS2805 Appendix N – A: One-way Function*.)

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'P4'
Terminal Master Key 1	1 A + 32 H or 1 A + 48 H	TMK1, encrypted under Variant 1 of LMK pair 14-15
PPASN (LMK)	16 H	PPASN, encrypted under Variant 8 of LMK pair 14-15
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'P5'
Error Code	2 N	'00': No errors. '10': TMK1 parity error. '12': No keys or table loaded in user storage. '13': LMK error; report to supervisor. '15': Error in input data.
Host Proof	8 H	The value for host proof of endpoint
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Calculate a RSA Public Key Verification Code

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: Calculate a Public Key Verification Code.

Notes:

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'H2'
Public Key Encoding	2 N	Encoding rules for Public Key
Public Key	n B	Public key, encoded appropriately
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'H3'
Error Code	2 N	'00': No errors. '03': Invalid public key encoding type. '04': Length error. '06': Public exponent length error. '08': Supplied public exponent is even. '15': Error in input data.
PVC	16 H	The Public Key Verification Code
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

11.2 AS2805.6.2 Support

This section details all the host commands required to support the AS2805.6.2 – 2002 standard.

The Australian Standard AS2805.6.2 - 2002 (Ref.8) on transaction key management supersedes the earlier (1988) standard (Ref.3). The main difference between the two standards is that the 2002 version of the standard specifies the use of double length keys, whereas the 1988 standard uses single length keys only.

The standard firmware for the Thales payShield 10K has a number of functions to support the 1988 standard (see Ref.1, Chapter 28, and Ref.4).

This section specifies functions for the payShield 10K to support the 2002 standard. In order to maintain backwards compatibility with existing applications, these commands have been written to permit both single length key (1988 standard) and double length key (2002 standard) processing. Where the 2002 standard processing requirements necessitate additional fields, these have been included as optional fields at the end of each command.

The AS2805.6.2 transaction key management scheme is based on each terminal having a key (the Terminal Key (TK)) that is updated automatically with each transaction. The update is based on the current TK and Message Authentication Code (MAC) Residues of the current transaction. The MAC Residue is calculated using a MAC Key, derived from the current TK and the Primary Account Number (PAN) of the current debit or credit card. Similarly, a PIN Encryption Key is derived from the TK and the card data.

Thus, the current TK at a terminal is a function of the initial TK at that terminal and all previous cards and transaction details at that terminal.

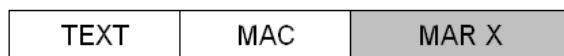
The Acquirer system maintains a database of current TKs for all the terminals it supports, and updates each TK as described above.

Details of all processing primitives used during a transaction are given in the Appendices at the end of this document. Specifically AS2805 Appendix N – AS 2805.6.2 Support Appendices, under the following headings:

- One-Way Function (OWF)
- Derivation of Data Values
- MAC Key Derivation
- PIN Encipherment Key Derivation
- Privacy Key Derivation
- Terminal Key Update
- MAC and MAC Residue (MAR) Calculation
- Authentication Parameter (AP)

The following diagram shows a transaction flow, between a terminal and the Acquirer. The transaction is initiated from the terminal. The shaded fields are not transmitted, but where they precede the MAC they form part of the data used to calculate the MAC.

Request Message:



Response Message:



Optional Completion Confirmation Message:



Optional Completion Response Message:



The Authentication Parameter (AP) is calculated from card data, including discretionary data (possibly non-transmitted), certain transaction details and the terminal identifier. In the most secure version of the scheme, where the discretionary data is not transmitted, only the Card Issuer can calculate the AP. Thus, the inclusion of the AP in the MAC calculation for the Response Message is "proof" of the Card Issuer's involvement in the transaction.

If the discretionary card data is transmitted in the Request Message then the AP may be calculated by the Acquirer.

The payShield 10K provides the following host commands to support AS2805 operations:

Function	Command	Page
<i>Verify a Transaction Request, without PIN</i>	RE (RF)	692
<i>Verify a Transaction Request, with PIN, when CD Field Available</i>	RG (RH)	694
<i>Verify a Transaction Request, with PIN, when CD Field not Available (when selected Transaction Key Scheme is Australian)</i>	RI (RJ)	696
<i>Verify a Transaction Request, with PIN, when CD Field not Available (when selected Transaction Key Scheme is Racal)</i>	HI (HJ)	698
<i>Generate Transaction Response, with Auth Para Generated by Acquirer (when selected Transaction Key Scheme is Australian)</i>	RK (RL)	699
<i>Generate Transaction Response, with Auth Para Generated by Acquirer (when selected Transaction Key Scheme is Racal)</i>	HK (HL)	701
<i>Generate Transaction Response with Auth Para Generated by Card Issuer (when selected Transaction Key Scheme is Australian)</i>	RM (RN)	702
<i>Generate Transaction Response with Auth Para Generated by Card Issuer (when selected Transaction Key Scheme is Racal)</i>	HM (HN)	704
<i>Translate a PIN from PEK to ZPK Encryption (when selected Transaction Key Scheme is Australian)</i>	RO (RP)	705
<i>Translate a PIN from PEK to ZPK Encryption (when selected Transaction Key Scheme is Racal)</i>	HO (HP)	707
<i>Verify a Transaction Completion Confirmation (when selected Transaction Key Scheme is Australian)</i>	RQ (RR)	708
<i>Verify a Transaction Completion Confirmation (when selected Transaction Key Scheme is Racal)</i>	HQ (HR)	710
<i>Generate a Transaction Completion Response (when selected Transaction Key Scheme is Australian)</i>	RS (RT)	711
<i>Generate a Transaction Completion Response (when selected Transaction Key Scheme is Racal)</i>	HS (HT)	713
<i>Verify a PIN at Card Issuer using IBM Method</i>	QQ (QR)	714
<i>Verify a PIN at Card Issuer using the Diebold Method</i>	QS (QT)	716
<i>Verify a PIN at Card Issuer using Visa Method</i>	QU (QV)	718
<i>Verify a PIN at Card Issuer using the Comparison Method</i>	QW (QX)	720
<i>Generate Auth Para at the Card Issuer (when selected Transaction Key Scheme is Australian)</i>	RU (RV)	722
<i>Generate Auth Para at the Card Issuer (when selected Transaction Key Scheme is Racal)</i>	HU (HV)	724
<i>Generate an Initial Terminal Key (when selected Transaction Key Scheme is Australian)</i>	RW (RX)	725
<i>Generate an Initial Terminal Key (when selected Transaction Key Scheme is Racal)</i>	HW (HX)	726
<i>Data Encryption Using a Derived Privacy Key</i>	QM (QN)	727
<i>Data Decryption Using a Derived Privacy Key</i>	QO (QP)	729

The commands specified in this section fall, naturally, into five categories:

Transaction with no PIN and AP Generated by the Acquirer

In this case, the sequence of commands is:

Command	Description	Notes
'RE'	Verify Transaction Request, without PIN	Acquirer function
'RK'	Generate Transaction Response when AP Generated by the Acquirer	Acquirer function
'RQ'	Verify Transaction Completion Confirmation Request	Acquirer function (optional)
'RS'	Generate Transaction Completion Response	Acquirer function (only if previous command ('RQ') is required)

Transaction with no PIN and AP Generated by the Issuer

In this case, the sequence of commands is:

Command	Description	Notes
'RE'	Verify Transaction Request, without PIN	Acquirer function
'RU'	Generate AP at Card Issuer	Issuer function
'RM'	Generate Transaction Response when AP Generated by the Issuer	Acquirer function
'RQ'	Verify Transaction Completion Confirmation Request	Acquirer function (optional)
'RS'	Generate Transaction Completion Response	Acquirer function (only if previous command ('RQ') is required)

PIN Verification at the Acquirer

In this case, the sequence of commands is:

Command	Description	Notes
'RG'	Verify Transaction Request, with PIN, when CD Field Available	Acquirer function
'DA', 'CG', 'DC', 'BC'	PIN Verify (standard commands)	Acquirer function
'RK'	Generate Transaction Response when AP Generated by the Acquirer	Acquirer function
'RQ'	Verify Transaction Completion Confirmation Request	Acquirer function (optional)
'RS'	Generate Transaction Completion Response	Acquirer function (only if previous command ('RQ') is required)

PIN Verification at the Issuer

In this case, the sequence of commands is:

Command	Description	Notes
'RI'	Verify Transaction Request, with PIN, when CD Field not Available	Acquirer function
'RO'	Translate PIN from PEK to ZPK Encryption	Acquirer function
'QQ','QS', 'QU','QW'	PIN Verify (various methods)	Issuer function
'RM'	Generate Transaction Response when AP Generated by the Issuer	Acquirer function
'RQ'	Verify Transaction Completion Confirmation Request	Acquirer function (optional)
'RS'	Generate Transaction Completion Response	Acquirer function (only if previous command ('RQ') is required)

Other Commands

The RW command is a "new" command, in that there is no equivalent function specified in Ref.1. The QM & QO commands are required to satisfy the requirement to encipher track 2 data in terminals supporting AS2805.6.2 functionality

Command	Description	Notes
'RW'	Generate Initial Terminal Key	Acquirer function
'QM'	Data Encryption Using a Derived Privacy Key	Acquirer function
'QO'	Data Decryption Using a Derived Privacy Key	Acquirer function

Verify a Transaction Request, without PIN

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To verify a transaction Request Message, without PIN, and return the MAC Residue (MARX) for subsequent inclusion in the MAC calculation for the Response Message.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RE'
TK	16 H or 1 A + 32 H	Single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
AB Field	16 H	AB field, as defined in AS2805.6.2
Message Length	3 H	Length (in bytes) of the next field; max value X'320
Message Text	n B	Message text; the last 64 bits (8 bytes) contain the MAC field, of which the leftmost 4, 6 or 8 bytes contain the MAC (depends on value of optional MAC Length field)
Delimiter	1 A	Optional field; present only if MAC Length field is present; value = ':'
MAC Length	1 N	Optional field; if field not present then value 0 is assumed: '0': 32-bit MAC (single or double length TK) '1': 48-bit MAC (double length TK only) '2': 64-bit MAC (double length TK only)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

payShield 10K Core Host Commands

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RF'
Error Code	2 N	<p>'00': No errors '01': MAC verification failure '10': Terminal Key parity error '12': No keys loaded in user storage '13': LMK error – report to Supervisor '15': Error in input data '21': Invalid user storage index '65': Transaction Key Scheme set to None '80': Message length error '90': Communications link parity error '91': Communications link LRC error '92': Data length error</p>
MARX	8 H or 16 H	Encrypted MAC Residue (X) for use in the transaction response message: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a Transaction Request, with PIN, when CD Field Available

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To verify a transaction Request Message, with PIN, and return the encrypted derived Terminal PIN Key (TPK), the PIN block encrypted under the TPK and the MAC Residue (MARX) for subsequent inclusion in the MAC calculation for the Response Message.

Notes: The output encrypted TPK and PIN block can be used by the Acquirer to verify the PIN using a standard PIN verification command ('DA', 'CG', 'DC' or 'BC').
The PIN Block Pointer field represents the position of the first byte of the PIN block (8 bytes) in the binary representation of the Message Text (it is therefore independent of the communication protocol).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RG'
TK	16 H or 1 A + 32 H	Single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
AB Field	16 H	AB field, as defined in AS2805.6.2
CD Field	16 H	CD field, as defined in AS2805.6.2
PIN Block Pointer	3 H	Pointer to first byte of encrypted PIN block in binary message text; value X'000 to X'310
Message Length	3 H	Length (in bytes) of the next field; max value X'320
Message Text	n B	Message text; the last 64 bits (8 bytes) contain the MAC field, of which the leftmost 4, 6 or 8 bytes contain the MAC (depends on value of optional MAC Length field)
Delimiter	1 A	Optional field; present only if MAC Length field is present; value = ':'
MAC Length	1 N	Optional field; if field not present then value 0 is assumed: 0 = 32-bit MAC (single or double length TK) 1 = 48-bit MAC (double length TK only) 2 = 64-bit MAC (double length TK only)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RH'
Error Code	2 N	<p>'00': No errors '01': MAC verification failure '10': Terminal Key parity error '12': No keys loaded in user storage '13': LMK error – report to Supervisor '15': Error in input data '20': PIN block error '21': Invalid user storage index '65': Transaction Key Scheme set to None '80': Message length error '88': Warning: AS2805.3 "zero" PIN block received '90': Communications link parity error '91': Communications link LRC error '92': Data length error</p>
TPK	16 H or 1 A + 32 H	Derived Terminal PIN Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
PIN Block	16 H	PIN block, encrypted under the derived TPK
MARX	8 H or 16 H	Encrypted MAC Residue (X) for use in the transaction response message: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a Transaction Request, with PIN, when CD Field not Available (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To verify a transaction Request Message, with PIN, and return the encrypted PIN Encipherment Key (PEK), for use in the 'RO' command, and the MAC Residue (MARX) for subsequent inclusion in the MAC calculation for the Response Message.

Notes: This command is only available if Transaction Key Scheme has been set to Australian (using the CS Console command or payShield Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HI Host command can be used, which provides exactly the same functionality as the RI Host command described below.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RI'
TK	16 H or 1 A + 32 H	Single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
AB Field	16 H	AB field, as defined in AS2805.6.2
Message Length	3 H	Length (in bytes) of the next field; max value X'320
Message Text	n B	Message text; the last 64 bits (8 bytes) contain the MAC field, of which the leftmost 4, 6 or 8 bytes contain the MAC (depends on value of optional MAC Length field)
Delimiter	1 A	Optional field; present only if MAC Length field is present; value = ':'
MAC Length	1 N	Optional field; if field not present then value 0 is assumed: '0': 32-bit MAC (single or double length TK) '1': 48-bit MAC (double length TK only) '2': 64-bit MAC (double length TK only)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RJ'
Error Code	2 N	<p>'00': No errors '01': MAC verification failure '10': Terminal Key parity error '12': No keys loaded in user storage '13': LMK error – report to Supervisor '15': Error in input data '21': Invalid user storage index '65': Transaction Key Scheme set to None '80': Message length error '88': Warning: AS2805.3 "zero" PIN block received '90': Communications link parity error '91': Communications link LRC error '92': Data length error</p>
PEK	16 H or 1 A + 32 H	PIN Encipherment Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y" (for use with the "RO" command)
MARX	8 H or 16 H	Encrypted MAC Residue (X) for use in the transaction response message: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a Transaction Request, with PIN, when CD Field not Available (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To verify a transaction Request Message, with PIN, and return the encrypted PIN Encipherment Key (PEK), for use in the 'RO' command, and the MAC Residue (MARX) for subsequent inclusion in the MAC calculation for the Response Message.

Notes: This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or payShield Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RI command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RI Host command described in this manual, except that:

Command Code = HI

Response Code = HJ

If Transaction Key Scheme has been set to Australian, then the RI Host command (as described in this manual) must be used.

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command	Use the Hx variant of the command
You want to process Australian Transaction Key commands	Use the Hx variant of the command	Use the Rx variant of the command

Generate Transaction Response, with Auth Para Generated by Acquirer (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate a transaction Response Message (when Auth Para is generated by the Acquirer) and to update the Terminal Key.

- Notes:
- a) This command is only available if Transaction Key Scheme has been set to Australian (using the CS Console command or payShield Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HK Host command can be used, which provides exactly the same functionality as the RK Host command described below.
 - b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')
 - c) The AT, STAN and CATID Pointer fields represent the position of the first byte of each of the relevant data items in the binary representation of the Message Text (they are therefore independent of the communication protocol). Note that the AT is 6 bytes (12 digits) in length, the STAN is 3 bytes (6 digits) and the CATID is 8 bytes (16 digits).
 - d) This function can also be used to generate a MAC and update the Terminal Key for an Administration Response Message. In this case the AP Include Flag should be set to 'E'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RK'
TK	16 H or 1 A + 32 H	Single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
AB Field	16 H	AB field, as defined in AS2805.6.2
MARX	8 H or 16 H	Encrypted MAC Residue (X) from the transaction request: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
AP Include Flag	1 A	Flag to indicate whether to include Auth Para in the MAC calculation; 'I' = include and pad to Thales standard 'E' = exclude and pad to Thales standard 'H' = include and pad to AS2805 standard 'F' = exclude and pad to AS2805 standard
CD Field	16 H	CD field, as defined in AS2805.6.2; only present if AP Include Flag = 'I' or 'H'.
AT Pointer	3 H	Pointer to first byte of transaction amount in binary message text; value X'000 to X'31A only present if AP Include Flag = 'I' or 'H'.
STAN Pointer	3 H	Pointer to first byte of systems trace audit number in binary message text; value X'000 to X'31D; only present if AP Include Flag = 'I' or 'H'.
CATID Pointer	3 H	Pointer to first byte of card acceptor terminal identification in binary message text; value X'000 to X'318; only present if AP Include Flag = 'I' or 'H'.
Message Length	3 H	X'001 to X'320 indicating the length of the next field.
Message Text	n B	1 to 800 bytes of message.

Field	Length & Type	Details
Parity Flag	1 N	Optional field; specifies the parity to apply to the new TK. If field not present, then odd parity is enforced. '0': Enforce odd parity '1': No parity
Delimiter	1 A	Optional field; present only if MAC Length field is present; value = ':'
MAC Length	1 N	Optional field; if field not present then value 0 is assumed: '0': 32-bit MAC (single or double length TK) '1': 48-bit MAC (double length TK only) '2': 64-bit MAC (double length TK only)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RL'
Error Code	2 N	'00': No errors '10': Terminal Key parity error '12': No keys loaded in user storage '13': LMK error – report to Supervisor '15': Error in input data '20': PIN block error '21': Invalid user storage index '65': Transaction Key Scheme set to None '80': Message length error '90': Communications link parity error '91': Communications link LRC error '92': Data length error
MARY	8 H or 16 H	Encrypted MAC Residue (Y) from the transaction response: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
MAC	8 H, 12 H or 16 H	MAC (length dependent on value of MAC Length field)
New TK	16 H or 1 A + 32 H	New single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Transaction Response, with Auth Para Generated by Acquirer (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate a transaction Response Message (when Auth Para is generated by the Acquirer) and to update the Terminal Key.

Notes: a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or payShield Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RK command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RK Host command described in this manual, except that:

Command Code = HK

Response Code = HL

If Transaction Key Scheme has been set to Australian, then the RK Host command (as described in this manual) must be used. (With this setting, the HK command code is as described in this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command	Use the Hx variant of the command
You want to process Australian Transaction Key commands	Use the Hx variant of the command	Use the Rx variant of the command

b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')

c) The AT, STAN and CATID Pointer fields represent the position of the first byte of each of the relevant data items in the binary representation of the Message Text (they are therefore independent of the communication protocol). Note that the AT is 6 bytes (12 digits) in length, the STAN is 3 bytes (6 digits) and the CATID is 8 bytes (16 digits).

d) This function can also be used to generate a MAC and update the Terminal Key for an Administration Response Message. In this case the AP Include Flag should be set to 'E'.

Generate Transaction Response with Auth Para Generated by Card Issuer (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate a transaction Response Message (when Auth Para has been generated by the Card issuer) and to update the Terminal Key.

Notes:

- a) This command is only available if Transaction Key Scheme has been set to Australian (using the CS Console command or payShield Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HM Host command can be used, which provides exactly the same functionality as the RM Host command described below.
- b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RM'
TK	16 H or 1 A + 32 H	Single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
AB Field	16 H	AB field, as defined in AS2805.6.2
MARX	8 H or 16 H	Encrypted MAC Residue (X) from the transaction request: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
AP Include Flag	1 A	Flag to indicate whether to include Auth Para in the MAC calculation; Value 'I' = include, 'E' = exclude; must have value 'I' for double length TK
ZPK	16 H or 1 A + 32 H or 1 A + 48 H	Zone PIN Key, encrypted under LMK pair 06-07; only present if AP Include Flag = 'I'
Auth Para	16 H	Auth Para, encrypted under variant 1 of the ZPK; only present if AP Include Flag = 'I';
Message Length	3 H	Length (in bytes) of the next field; max value X'320
Message Text	n B	Message text (maximum length = 800 bytes)
Delimiter	1 A	Optional field; present only if MAC Length field is present; value = ':';
MAC Length	1 N	Optional field; if field not present then value 0 is assumed: '0': 32-bit MAC (single or double length TK) '1': 48-bit MAC (double length TK only) '2': 64-bit MAC (double length TK only)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RN'
Error Code	2 N	<p>'00': No errors '04': AP include flag error '10': Terminal Key parity error '11': ZPK parity error '12': No keys loaded in user storage '13': LMK error – report to Supervisor '15': Error in input data '21': Invalid user storage index '65': Transaction Key Scheme set to None '80': Message length error '90': Communications link parity error '91': Communications link LRC error '92': Data length error</p>
MARY	8 H or 16 H	Encrypted MAC Residue (Y) from the transaction response: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
MAC	8 H, 12 H or 16 H	MAC (length dependent on value of MAC Length field)
New TK	16 H or 1 A + 32 H	New single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Transaction Response with Auth Para Generated by Card Issuer (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate a transaction Response Message (when Auth Para has been generated by the Card issuer) and to update the Terminal Key.

Notes: a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or payShield Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RM command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RM Host command described in this manual, except that:

Command Code = HM

Response Code = HN

If Transaction Key Scheme has been set to Australian, then the RM Host command (as described in this manual) must be used. (With this setting, the HM command code is as described in the AS2805 section of this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command	Use the Hx variant of the command
You want to process Australian Transaction Key commands	Use the Hx variant of the command	Use the Rx variant of the command

b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')

Translate a PIN from PEK to ZPK Encryption (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To translate a PIN block from encryption under Card Key and a PIN Encipherment Key (PEK) to encryption under Card Key and a Zone PIN Key (ZPK).

- Notes:
- a) This command is only available if Transaction Key Scheme has been set to Australian (using the CS Console command or payShield Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HO Host command can be used, which provides exactly the same functionality as the RO Host command described below.
 - b) This command is used, by the Acquirer, with the 'RI' command. In this case, the Acquirer has no access to the CD field and hence is unable to calculate Card Key.
 - c) This command is essentially a standard PIN translation command, with the exception that no PIN block validation occurs. The processing described is independent of the AS2805.6.2 standard(s).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RO'
PEK	16 H or 1 A + 32 H	PIN Encipherment Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y". (as returned from the 'RI' command)
ZPK	16 H or 1 A + 32 H or 1 A + 48 H	Zone PIN Key, encrypted under LMK pair 06-07
PIN Block	16 H	PIN block, doubly encrypted with Card Key and PEK
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RP'
Error Code	2 N	'00': No errors '10': PEK parity error '11': ZPK parity error '12': No keys loaded in user storage '13': LMK error – report to Supervisor '15': Error in input data '21': Invalid user storage index '65': Transaction Key Scheme set to None
PIN Block	16 H	PIN block, doubly encrypted with Card Key and ZPK
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate a PIN from PEK to ZPK Encryption (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To translate a PIN block from encryption under Card Key and a PIN Encipherment Key (PEK) to encryption under Card Key and a Zone PIN Key (ZPK).

Notes: a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or payShield Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RO command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RO Host command described in this manual, except that:

Command Code = HO

Response Code = HP

If Transaction Key Scheme has been set to Australian, then the RO Host command (as described in this manual) must be used. (With this setting, the HO command code is as described in the AS2805 section of this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command	Use the Hx variant of the command
You want to process Australian Transaction Key commands	Use the Hx variant of the command	Use the Rx variant of the command

- b) This command is used, by the Acquirer, with the 'RI' command. In this case, the Acquirer has no access to the CD field and hence is unable to calculate Card Key.
- c) This command is essentially a standard PIN translation command, with the exception that no PIN block validation occurs. The processing described is independent of the AS2805.6.2 standard(s).

Verify a Transaction Completion Confirmation (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To verify a transaction Completion Confirmation Message and return the MAC Residue (MARZ) for subsequent inclusion in the MAC calculation for the Completion Response Message.

- Notes:**
- a) This command is only available if Transaction Key Scheme has been set to Australian (using the CS Console command or payShield Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HQ Host command can be used, which provides exactly the same functionality as the RQ Host command described below.
 - b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RQ'
TK	16 H or 1 A + 32 H	Single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
AB Field	16 H	AB field, as defined in AS2805.6.2
MARY	8 H or 16 H	Encrypted MAC Residue (Y) from the transaction response: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
Message Length	3 H	Length (in bytes) of the next field; max value X'320
Message Text	n B	Message text; the last 64 bits (8 bytes) contain the MAC field, of which the leftmost 4, 6 or 8 bytes contain the MAC (depends on value of optional MAC Length field)
Delimiter	1 A	Optional field; present only if MAC Length field is present; value = ','
MAC Length	1 N	Optional field; if field not present then value 0 is assumed: '0': 32-bit MAC (single or double length TK) '1': 48-bit MAC (double length TK only) '2': 64-bit MAC (double length TK only)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RR'
Error Code	2 N	<p>'00': No errors '01': MAC verification failure '10': Terminal Key parity error '12': No keys loaded in user storage '13': LMK error – report to Supervisor '15': Error in input data '21': Invalid user storage index '80': Message length error '65': Transaction Key Scheme set to None '90': Communications link parity error '91': Communications link LRC error '92': Data length error</p>
MARZ	8 H or 16 H	Encrypted MAC Residue (Z) for use in the completion response message: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a Transaction Completion Confirmation (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To verify a transaction Completion Confirmation Message and return the MAC Residue (MARZ) for subsequent inclusion in the MAC calculation for the Completion Response Message.

Notes: a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or payShield Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RQ command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RQ Host command described in this manual, except that:

Command Code = HQ

Response Code = HR

If Transaction Key Scheme has been set to Australian, then the RQ Host command (as described in this manual) must be used. (With this setting, the HQ command code is as described in the AS2805 section of this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command	Use the Hx variant of the command
You want to process Australian Transaction Key commands	Use the Hx variant of the command	Use the Rx variant of the command

b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')

Generate a Transaction Completion Response (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate a transaction Completion Response Message.

- Notes:
- a) This command is only available if Transaction Key Scheme has been set to Australian (using the CS Console command or payShield Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HS Host command can be used, which provides exactly the same functionality as the RS Host command described below.
 - b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RS'
TK	16 H or 1 A + 32 H	Single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
AB Field	16 H	AB field, as defined in AS2805.6.2
MARZ	8 H or 16 H	Encrypted MAC Residue (Z) from the transaction completion confirmation request: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
Message Length	3 H	Length (in bytes) of the next field; max value X'320
Message Text	n B	Message text (maximum length = 800 bytes)
Delimiter	1 A	Optional field; present only if MAC Length field is present; value = ':'
MAC Length	1 N	Optional field; if field not present then value 0 is assumed: '0': 32-bit MAC (single or double length TK) '1': 48-bit MAC (double length TK only) '2': 64-bit MAC (double length TK only)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RT'
Error Code	2 N	<p>'00': No errors '10': Terminal Key parity error '12': No keys loaded in user storage '13': LMK error – report to Supervisor '15': Error in input data '21': Invalid user storage index '65': Transaction Key Scheme set to None '80': Message length error '90': Communications link parity error '91': Communications link LRC error '92': Data length error</p>
MAC	8 H, 12 H or 16 H	MAC (length dependent on value of MAC Length field)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a Transaction Completion Response (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate a transaction Completion Response Message.

Notes: a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or payShield Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RS command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RS Host command described in this manual, except that:

Command Code = HS

Response Code = HT

If Transaction Key Scheme has been set to Australian, then the RS Host command (as described in this manual) must be used. (With this setting, the HS command code is as described in the AS2805 section of this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command	Use the Hx variant of the command
You want to process Australian Transaction Key commands	Use the Hx variant of the command	Use the Rx variant of the command

b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI').

Verify a PIN at Card Issuer using IBM Method

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To verify a PIN at the Card Issuer, using the IBM 3624 method and return Auth Para.

Notes: The PIN block input to this command is doubly encrypted with Card Key and a Zone PIN Key (ZPK).

The input fields for this command are identical to those for the original 'QQ' command, as defined in the 40-1018-02 specification (Ref.4). Thus, an optional field ("Processing Flag") has been included. If the field is not present then the original processing occurs. If the field is present then either the original processing or the new processing described in this document occurs, depending on the value of the field.

If a double or triple length PVK is used in this command then processing will continue as normal, but a different error code ('02') will be returned.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'QQ'
ZPK(S)	16 H or 1 A + 32 H or 1 A + 48 H	Source Zone PIN Key, encrypted under LMK pair 06-07
ZPK(D)	16 H or 1 A + 32 H or 1 A + 48 H	Destination Zone PIN Key, encrypted under LMK pair 06-07
PVK	16 H or 1 A + 32 H or 1 A + 48 H	PIN Verification Key, encrypted under LMK pair 14-15 variant 0
AB Field	16 H	AB field, as defined in AS2805.6.2
CD Field	16 H	CD field, as defined in AS2805.6.2
STAN	6 N	Systems trace audit number
CATID	16 H	Card acceptor terminal identification
AT	12 H	Transaction amount
Maximum PIN Length	2 N	Value = 12
PIN Block	16 H	PIN block, doubly encrypted with Card Key and ZPK(S)
PIN Block Format Code	2 N	Valid formats are: 01, 05 & 46
Check Length	2 N	Minimum PIN length
Primary Account Number (PAN)	12 N	Rightmost 12 digits of the card PAN, excluding the check digit
Decimalization Table	16 N or 16 H or 'K' + 3 H	16 N if console CS cmd is set for Plaintext decimalisation tables. 16 H if console CS cmd is set for Encrypted decimalisation tables. 'K' + 3 H if the decimalization table is held in the HSM's User Storage Area
PIN Validation Data	16 H	The 16 character field used as input to the IBM PIN verification algorithm

payShield 10K Core Host Commands

Field	Length & Type	Details
Offset	12 H	PIN offset, left justified and padded with X'F
Delimiter	1 A	Optional field, if present then the following field is present. value = ':'
Processing Flag	1 N	Optional field; if not present then value = 0 is assumed; values: '0': old processing (1988 standard) '1': new processing (2002 standard)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'QR'
Error Code	2 N	'00': No errors '01': PIN verification failure '02': Warning – PVK not single length (PIN OK) '10': ZPK(S) parity error '11': ZPK(D) or PVK parity error '12': No keys loaded in user storage '13': LMK error – report to Supervisor '15': Error in input data '20': PIN block error '21': Invalid user storage index '23': Invalid PIN block format code '24': PIN length error '25': Invalid decimalization table '65': Transaction Key Scheme set to None
Auth Para	16 H	Auth Para, encrypted under variant 1 of ZPK(D)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a PIN at Card Issuer using the Diebold Method

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To verify a PIN at the Card Issuer, using the Diebold method and return Auth Para.

Notes: The PIN block input to this command is doubly encrypted with Card Key and a Zone PIN Key (ZPK).

The input fields for this command are identical to those for the original 'QS' command, as defined in the 40-1018-02 specification (Ref.9). Thus, an optional field ("Processing Flag") has been included. If the field is not present then the original processing occurs. If the field is present then either the original processing or the new processing described in this document occurs, depending on the value of the field.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'QS'
ZPK(S)	16 H or 1 A + 32 H or 1 A + 48 H	Source Zone PIN Key, encrypted under LMK pair 06-07
ZPK(D)	16 H or 1 A + 32 H or 1 A + 48 H	Destination Zone PIN Key, encrypted under LMK pair 06-07
AB Field	16 H	AB field, as defined in AS2805.6.2
CD Field	16 H	CD field, as defined in AS2805.6.2
STAN	6 N	Systems trace audit number
CATID	16 H	Card acceptor terminal identification
AT	12 H	Transaction amount
Index Flag	1 A	Value 'K'
Index Pointer	3 N	Index to stored Diebold table
Algorithm Number	2 N	Diebold algorithm required
PIN Block	16 H	PIN block, doubly encrypted with Card Key and ZPK(S)
PIN Block Format Code	2 N	Valid formats are: 01, 05 & 46
Primary Account Number (PAN)	12 N	Rightmost 12 digits of the card PAN, excluding the check digit
PIN Validation Data	20 H	The 20 character field used as input to the PIN verification algorithm
Offset	4 N	PIN offset
Delimiter	1 A	Optional field, if present then the following field is present. value = ','
Processing Flag	1 N	Optional field; if not present then value = 0 is assumed; values: '0': old processing (1988 standard) '1': new processing (see this document)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'QT'
Error Code	2 N	<p>'00': No errors '01': PIN verification failure '10': ZPK(S) parity error '11': ZPK(D) or PVK parity error '12': No keys loaded in user storage '13': LMK error – report to Supervisor '15': Error in input data '20': PIN block error '21': Invalid user storage index '23': Invalid PIN block format code '24': PIN length error '65': Transaction Key Scheme set to None</p>
Auth Para	16 H	Auth Para, encrypted under variant 1 of ZPK(D)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a PIN at Card Issuer using Visa Method

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To verify a PIN at the Card Issuer, using the Visa method and return Auth Para.

Notes: The PIN block input to this command is doubly encrypted with Card Key and a Zone PIN Key (ZPK).

The input fields for this command are identical to those for the original 'QU' command, as defined in the 40-1018-02 specification (Ref.4). Thus, an optional field ("Processing Flag") has been included. If the field is not present then the original processing occurs. If the field is present then either the original processing or the new processing described in this document occurs, depending on the value of the field.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'QU'
ZPK(S)	16 H or 1 A + 32 H or 1 A + 48 H	Source Zone PIN Key, encrypted under LMK pair 06-07
ZPK(D)	16 H or 1 A + 32 H or 1 A + 48 H	Destination Zone PIN Key, encrypted under LMK pair 06-07
PVK	32 H or 1 A + 32 H	PIN Verification Key, encrypted under LMK pair 14-15 variant 0
AB Field	16 H	AB field, as defined in AS2805.6.2
CD Field	16 H	CD field, as defined in AS2805.6.2
STAN	6 N	Systems trace audit number
CATID	16 H	Card acceptor terminal identification
AT	12 H	Transaction amount
PIN Block	16 H	PIN block, doubly encrypted with Card Key and ZPK(S)
PIN Block Format Code	2 N	Valid formats are: 01, 05 & 46
Primary Account Number (PAN)	12 N	Rightmost 12 digits of the card PAN, excluding the check digit
PVKI	1 N	PVK indicator; value 0 to 6
PVV	4 N	PIN verification value
Delimiter	1 A	Optional field, if present then the following field is present. value = ':';
Processing Flag	1 N	Optional field; if not present then value = 0 is assumed; values: '0': old processing (1988 standard) '1': new processing (see this document)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'QV'
Error Code	2 N	<p>'00': No errors '01': PIN verification failure '10': ZPK(S) parity error '11': ZPK(D) or PVK parity error '12': No keys loaded in user storage '13': LMK error – report to Supervisor '15': Error in input data '20': PIN block error '21': Invalid user storage index '23': Invalid PIN block format code '24': PIN length error '27': PVK not double length '65': Transaction Key Scheme set to None</p>
Auth Para	16 H	Auth Para, encrypted under variant 1 of ZPK(D)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a PIN at Card Issuer using the Comparison Method

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To verify a PIN at the Card Issuer, using the Comparison method and return Auth Para.

Notes: The PIN block input to this command is doubly encrypted with Card Key and a Zone PIN Key (ZPK).

The input fields for this command are identical to those for the original 'QW' command, as defined in the 40-1018-02 specification (Ref.4). Thus, an optional field ("Processing Flag") has been included. If the field is not present then the original processing occurs. If the field is present then either the original processing or the new processing described in this document occurs, depending on the value of the field.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'QW'
ZPK(S)	16 H or 1 A + 32 H or 1 A + 48 H 16 H or 1 A + 32 H or 1 A + 48 H	Source Zone PIN Key, encrypted under LMK pair 06-07
ZPK(D)	16 H or 1 A + 32 H or 1 A + 48 H	Destination Zone PIN Key, encrypted under LMK pair 06-07
AB Field	16 H	AB field, as defined in AS2805.6.2
CD Field	16 H	CD field, as defined in AS2805.6.2
STAN	6 N	Systems trace audit number
CATID	16 H	Card acceptor terminal identification
AT	12 H	Transaction amount
PIN Block	16 H	PIN block, doubly encrypted with Card Key and ZPK(S)
PIN Block Format Code	2 N	Valid formats are: 01, 05 & 46
Primary Account Number (PAN)	12 N	Rightmost 12 digits of the card PAN, excluding the check digit
Encrypted PIN	L N	PIN, encrypted using the PAN and LMK pair 02-03, stored on host database
Delimiter	1 A	Optional field, if present then the following field is present. value = ;
Processing Flag	1 N	Optional field; if not present then value = 0 is assumed; values: '0': old processing (1988 standard) '1': new processing (see this document)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'QX'
Error Code	2 N	<p>'00': No errors '01': PIN verification failure '10': ZPK(S) parity error '11': ZPK(D) parity error '12': No keys loaded in user storage '13': LMK error – report to Supervisor '14': Database PIN error '15': Error in input data '20': PIN block error '21': Invalid user storage index '23': Invalid PIN block format code '24': PIN length error '65': Transaction Key Scheme set to None</p>
Auth Para	16 H	Auth Para, encrypted under variant 1 of ZPK(D)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Auth Para at the Card Issuer (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate Auth Para at the Card Issuer and return it encrypted under variant 1 of a Zone PIN Key (ZPK).

- Notes:
- a) This command is only available if Transaction Key Scheme has been set to Australian (using the CS Console command or payShield Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HU Host command can be used, which provides exactly the same functionality as the RU Host command described below.
 - b) This command allows the Card Issuer to generate Auth Para when no PIN is to be verified, but the CD fields are not known to the Acquirer.
 - c) The input fields for this command are identical to those for the original 'RU' command, as defined in the 40-1018-02 specification (Ref.4). Thus, an optional field ("Processing Flag") has been included. If the field is not present then the original processing occurs. If the field is present then either the original processing or the new processing described in this document occurs, depending on the value of the field.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RU'
ZPK	16 H or 1 A + 32 H or 1 A + 48 H	Zone PIN Key, encrypted under LMK pair 06-07
AB Field	16 H	AB field, as defined in AS2805.6.2
CD Field	16 H	CD field, as defined in AS2805.6.2
STAN	6 N	Systems trace audit number
CATID	16 H	Card acceptor terminal identification
AT	12 H	Transaction amount
Delimiter	1 A	Optional field, if present then the following field is present. value = ':'
Processing Flag	1 N	Optional field; if not present then value = 0 is assumed; values: 0 = old processing (1988 standard) 1 = new processing (see this document)
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RV'
Error Code	2 N	'00': No errors '10': ZPK parity error '12': No keys loaded in user storage '13': LMK error – report to Supervisor '15': Error in input data '21': Invalid user storage index '65': Transaction Key Scheme set to None '90': Communications link parity error '91': Communications link LRC error '92': Data length error
Auth Para	16 H	Auth Para, encrypted under LMK pair 06-07 variant 1
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Auth Para at the Card Issuer (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate Auth Para at the Card Issuer and return it encrypted under variant 1 of a Zone PIN Key (ZPK).

Notes: a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or payShield Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RU command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RU Host command described in this manual, except that:

Command Code = HU

Response Code = HV

If Transaction Key Scheme has been set to Australian, then the RU Host command (as described in this manual) must be used. (With this setting, the HU command code is as described in the AS2805 section of this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command*	Use the Hx variant of the command*
You want to process Australian Transaction Key commands	Use the Hx variant of the command*	Use the Rx variant of the command*

- b) This command allows the Card Issuer to generate Auth Para when no PIN is to be verified, but the CD fields are not known to the Acquirer.
- c) The input fields for this command are identical to those for the original 'RU' command, as defined in the 40-1018-02 specification (Ref.4). Thus, an optional field ("Processing Flag") has been included. If the field is not present then the original processing occurs. If the field is present then either the original processing or the new processing described in this document occurs, depending on the value of the field.

Generate an Initial Terminal Key (when selected Transaction Key Scheme is Australian)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate an initial double length Terminal Key (TK) and return the result encrypted under the appropriate LMK pair.

Notes:

- a) This command is only available if Transaction Key Scheme has been set to Australian (using the CS Console command or payShield Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HW Host command can be used, which provides exactly the same functionality as the RW Host command described below.
- b) This command uses a previously established double length Acquirer Initialization Key (KIA) and the Card Acceptor Terminal Identification (CATID) to generate the initial TK for the terminal.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'RW'
KIA	1 A + 32 H	Double length Acquirer Initialization Key, encrypted under LMK pair 14-15 variant 6
CATID	16 H	Card acceptor terminal identification
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'RX'
Error Code	2 N	'00': No errors '10': KIA parity error '12': No keys loaded in user storage '13': LMK error – report to Supervisor '15': Error in input data '21': Invalid user storage index '65': Transaction Key Scheme set to None
Initial TK	1 A + 32 H	Initial double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate an Initial Terminal Key (when selected Transaction Key Scheme is Racal)

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Classic & Premium	
Authorization: Not required	

Function: To generate an initial double length Terminal Key (TK) and return the result encrypted under the appropriate LMK pair.

Notes: a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or payShield Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RW command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 10K.

The structure of this command and response is identical to the RW Host command described in this manual, except that:

Command Code = HW

Response Code = HX

If Transaction Key Scheme has been set to Australian, then the RW Host command (as described in this manual) must be used. (With this setting, the HW command code is as described in the AS2805 section of this manual.)

In summary ...

	If Transaction Key Scheme = Racal	If Transaction Key Scheme = Australian
You want to process Racal Transaction Key commands	Use the Rx variant of the command*	Use the Hx variant of the command*
You want to process Australian Transaction Key commands	Use the Hx variant of the command*	Use the Rx variant of the command*

b) This command uses a previously established double length Acquirer Initialization Key (KIA) and the Card Acceptor Terminal Identification (CATID) to generate the initial TK for the terminal.

Data Encryption Using a Derived Privacy Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To encrypt a block of data, using a double length Privacy Key (KP) derived from the Terminal Key (KT), the Systems Trace Audit Number (STAN) and the Card Acceptor Terminal Identification (CATID).

Notes: The modes of encryption supported by this command are Electronic Codebook (ECB), Cipher Block Chaining (CBC), 8-bit Cipher Feedback (CFB-8), and OFB (8-bit or 8-byte) - see AS2805.5.2 (Ref.8.2).

The HSM input and output buffers can support 2K bytes of data. It is recommended that the Plaintext Data field in the command message is no greater than 1800 bytes.

The Plaintext Data field must be an exact multiple of 8 bytes. The Encrypted Data field will be the same length as the Plaintext Data field.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'QM'
TK	1 A + 32 H	Double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
STAN	6 N	Systems Trace Audit Number
CATID	16 H	Card Acceptor Terminal Identification
Encryption Mode	1 N	Flag to indicate the mode of encryption '0': ECB mode of encryption '1': CBC mode of encryption '2': CFB-8 mode of encryption '3': OFB mode of encryption
Initialization Value	16 H	Initialization value, used when Encryption Mode = 1, 2 or 3 (CBC, CFB-8 or OFB)
Plaintext Value (j)	1 N	Only used when Encryption Mode = 3 (OFB); j = 1 for 8-bit feedback or j = 8 for 8-byte (64-bit) feedback
Length	3 H	Length (in bytes) of data to be encrypted
Plaintext Data	n B	Data to be encrypted.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'QN'
Error Code	2 N	'00': No errors '10': TK parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '65': Transaction Key Scheme set to None '80': Invalid data length
Encrypted Data	n B	Encrypted data.
OCV	16 H	Output Chaining Value, only returned when Encryption Mode = 3 (OFB)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Data Decryption Using a Derived Privacy Key

Variant LMK <input checked="" type="checkbox"/>	Key Block LMK <input type="checkbox"/>
Available in package(s): Premium	
Authorization: Not required	

Function: To decrypt a block of data, using a double length Privacy Key (KP) derived from the Terminal Key (KT), the Systems Trace Audit Number (STAN) and the Card Acceptor Terminal Identification (CATID).

Notes: The modes of encryption supported by this command are Electronic Codebook (ECB), Cipher Block Chaining (CBC), 8-bit Cipher Feedback (CFB-8), and OFB (8-bit or 8-byte) - see AS2805.5.2 (Ref.8.2).

The HSM input and output buffers can support 2K bytes of data. It is recommended that the Encrypted Data field in the command message is no greater than 1800 bytes.

The Encrypted Data field must be an exact multiple of 8 bytes. The output Plaintext Data field will be the same length as the Encrypted Data field.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'QO'
TK	1 A + 32 H	Double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
STAN	6 N	Systems Trace Audit Number
CATID	16 H	Card Acceptor Terminal Identification
Encryption Mode	1 N	Flag to indicate the mode of encryption '0': ECB mode of encryption '1': CBC mode of encryption '2': CFB-8 mode of encryption '3': OFB mode of encryption
Initialization Value	16 H	Initialization value, used when Encryption Mode = 1, 2 or 3 (CBC, CFB-8 or OFB)
Plaintext Value (j)	1 N	Only used when Encryption Mode = 3 (OFB); j = 1 for 8-bit feedback or j = 8 for 8-byte (64-bit) feedback
Length	3 H	Length (in bytes) of data to be decrypted
Encrypted Data	n B	Data to be decrypted.
Delimiter	1 A	Value '%'. Optional; if present, the following field must also be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'QP'
Error Code	2 N	'00': No errors '10': TK parity error '12': No keys loaded in user storage '13': LMK error; report to supervisor '15': Error in input data '21': Invalid user storage index '65': Transaction Key Scheme set to None '80': Invalid data length
Plaintext Data	n B	Decrypted data.
OCV	16 H	Output Chaining Value, only returned when Encryption Mode = 3 (OFB)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

12 Error Codes

The standard error codes returned by the payShield 10K to the Host are listed in the table. Some error codes are specific to certain commands: these are documented in Chapter 2.

Note: Whilst the payShield 10K's host commands are backward compatible with those of the payShield 9000 and HSM 8000, the internal processing steps are occasionally different, resulting in different error codes being returned.

Note: All commands that have a data length field followed by a data field will return error 15 if the data is longer than the specified length and error 80 if the data is shorter than the specified length or if the value in the data length field is 0.

Code	Description
00	No error
01	Verification failure or warning of imported key parity error
02	Key inappropriate length for algorithm
04	Invalid key type code
05	Invalid key length flag
10	Source key parity error
11	Destination key parity error or key all zeros
12	Contents of user storage not available. Reset, power-down or overwrite
13	Invalid LMK Identifier
14	PIN encrypted under LMK pair 02-03 is invalid
15	Invalid input data (invalid format, invalid characters, or not enough data provided)
16	Console or printer not ready or not connected
17	HSM not authorized, or operation prohibited by security settings
18	Document format definition not loaded
19	Specified Diebold Table is invalid
20	PIN block does not contain valid values
21	Invalid index value, or index/block count would cause an overflow condition
22	Invalid account number
23	Invalid PIN block format code. (Use includes where the security setting to implement PCI HSM limitations on PIN Block format usage is applied, and a Host command attempts to convert a PIN Block to a disallowed format.)
24	PIN is fewer than 4 or more than 12 digits in length
25	Decimalization Table error
26	Invalid key scheme
27	Incompatible key length
28	Invalid key type
29	Key function not permitted
30	Invalid reference number

Code	Description
31	Insufficient solicitation entries for batch
32	AES not licensed
33	LMK key change storage is corrupted
39	Fraud detection
40	Invalid checksum
41	Internal hardware/software error: bad RAM, invalid error codes, etc.
42	DES failure
43	RSA Key Generation Failure
46	Invalid tag for encrypted PIN
47	Algorithm not licensed
48	Key cannot be encrypted by a 3DES LMK
49	Private key error, report to supervisor
51	Invalid message header
65	Transaction Key Scheme set to None
67	Command not licensed
68	Command has been disabled
69	PIN block format has been disabled
74	Invalid digest info syntax (no hash mode only)
75	Single length key masquerading as double or triple length key
76	RSA public key length error or RSA encrypted data length error
77	Clear data block error
78	Private key length error
79	Hash algorithm object identifier error
80	Data length error. The amount of MAC data (or other data) is greater than or less than the expected amount.
81	Invalid certificate header
82	Invalid check value length
83	Key block format error
84	Key block check value error
85	Invalid OAEP Mask Generation Function
86	Invalid OAEP MGF Hash Function
87	OAEP Parameter Error
90	Data parity error in the request message received by the HSM
A1	Incompatible LMK schemes
A2	Incompatible LMK identifiers
A3	Incompatible key block LMK identifiers
A4	Key block authentication failure
A5	Incompatible key length

Code	Description
A6	Invalid key usage
A7	Invalid algorithm
A8	Invalid mode of use
A9	Invalid key version number
AA	Invalid export field
AB	Invalid number of optional blocks
AC	Optional header block error
AD	Key status optional block error
AE	Invalid start date/time
AF	Invalid end date/time
B0	Invalid encryption mode
B1	Invalid authentication mode
B2	Miscellaneous key block error
B3	Invalid number of optional blocks
B4	Optional block data error
B5	Incompatible components
B6	Incompatible key status optional blocks
B7	Invalid change field
B8	Invalid old value
B9	Invalid new value
BA	No key status block in the key block
BB	Invalid wrapping key
BC	Repeated optional block
BD	Incompatible key types
BE	Invalid key block header ID
D3	The wrapping key has a lower security strength than the key being wrapped.

13 Card Issuing Appendices

Note 1: Compress data elements by creating bytes consisting of two digits per byte (having values in the range Hex '0'–'F'). These data elements are right justified and padded with leading hex '0's if required.

Note 2: Compress data elements by creating bytes consisting of two digits per byte (having values in the range Hex '0'–'F'). These data elements are left justified and padded with trailing hexadecimal 'F's if required.

Example: A Primary Account Number (PAN) consisting of 1234567890123 will be stored in an 8 byte field as Hex '12 34 56 78 90 12 3F FF'.

Notations: N_{CA} = Length of the Certification Authority Public Key Modulus

N_I = Length of the Issuer Public Key Modulus

N_{IC} = Length of the Card (ICC) Public Key Modulus

Card Issuing Appendix A – Self-Signed Issuer Public Key Certificate Format (Visa)

Field Name	Length & Format	Description	
Header	1 b	Hex value '22'	NOT SIGNED
Length of Issuer Public Key Modulus	1 b	Length of Issuer Public Key Modulus in Hex. (Number of bytes)	NOT SIGNED
Issuer Public Key Modulus	var b	Issuer's Public Key Modulus	NOT SIGNED
Issuer Public Key Exponent Length	1 b	Length of Issuer Public Key Exponent. (Number of bytes). Must be either hex 01 (for exponent 3) or hex 03 (for exponent 65537).	NOT SIGNED
Issuer Public Key Exponent	1 or 3 b	Issuer Public Key Exponent. Must be either 3 or 65537, that is, hex 03 or hex 01 00 01.	NOT SIGNED
Tracking Number	3 b	Tracking number from Visa Financial Institution registration form. See Note 1.	NOT SIGNED

Self-Signed Issuer Public Key Certificate

(Clear Data – Unsigned Issuer Public Key Input Extension)

Field Name	Length & Format	Description	Hashed
Header	1 b	Hex. value '23'.	Yes
Visa Service Identifier	4 b	<p>Identifies a Visa Service. The Proprietary Application Identifier Extension (PIX) is left justified and padded on the right with four hex zeros. Current valid International Service Identifiers are: Hex 1010 0000 : for Debit/Credit Hex 2010 0000 : for Electron Hex 3010 0000 : for Interlink Hex 8010 0000 : for PLUS Check with Visa regional offices for Regional/National service identifiers</p>	Yes
Certificate Format	1 b	Hex value '02'.	Yes
Issuer Identification Number	4 b	Leftmost 3-8 digits from the PAN, right padded with hexadecimal Fs. See Note 2.	Yes
Certificate Expiration Date	2 b	MMYY after which this certificate is invalid. See Note 1.	Yes
Tracking Number	3 b	Tracking number from Visa Financial Institution registration form. See Note 1.	Yes
Hash Algorithm Indicator	1 b	Identifies the hash algorithm used to produce the Hash Result.	Yes
Issuer's Public Key Algorithm Indicator	1 b	Identifies the digital signature algorithm to be used with the Issuer's Public Key.	Yes
Issuer Public Key Modulus Length	1 b	Identifies the length of the Issuer Public Key Modulus. (Number of bytes)	Yes
Issuer Public Key Exponent Length	1 b	Length e of the Issuer Public Key Exponent (Number of bytes). Either hex 01 (for exponent 3) or hex 03 (for exponent 65537).	Yes
Leftmost Digits of Issuer Public Key Modulus	var b	Leftmost $N_1 - (39 + e)$ bytes of Issuer's Public Key Modulus	Yes
Issuer Public Key Exponent	1 or 3 b	Issuer Public Key Exponent. Is either 3 or 65537, that is, hex 03 or hex 01 00 01.	Yes
Hash Result	20 b	Hash of Issuer's Public Key and its related information.	No

*Self-Signed Issuer Public Key Certificate**(Self-Signed Certificate Data)*

Card Issuing Appendix B – Self-Signed Issuer Public Key Certificate Format (Mastercard)

Field Name	Length & Format	Description		Hashed
ID of Subject Certificate (Issuer Identifier)	4 b	Leftmost 3-8 digits from the PAN, right padded with hexadecimal F. See Note 2.	NOT SIGNED	No
Issuer Public Key Index	3 b	Number, chosen by the Issuer, which uniquely identifies the Public Key. See Note 1.	NOT SIGNED	No
Subject Public Key Algorithm Indicator (Signature Identifier)	1 b	Indicates the signature algorithm to be used with the Issuer Public Key.	NOT SIGNED	No
Subject Public Key Modulus Length	1 b	Length of Issuer Public Key Modulus (equal to N_i)	NOT SIGNED	No
Subject Public Key Exponent Length	1 b	Length of Issuer Public Key Exponent. (Number of bytes). Must be either hex 01 (for exponent 3) or hex 03 (for exponent 65537).	NOT SIGNED	No
Leftmost Digits of Subject Public Key Modulus	N_i-36 b	N_i-36 most significant bytes of the Issuer Public Key Modulus	NOT SIGNED	No
Subject Public Key Modulus Remainder	36 b	36 least significant bytes of the Issuer Public Key Modulus	NOT SIGNED	Yes
Subject Public Key Exponent	1 or 3 b	Issuer Public Key Exponent. Is either 3 or 65537, that is, hex 03 or hex 01 00 01.	NOT SIGNED	Yes

Self-Signed Issuer Public Key Certificate

(Clear Data)

Field Name	Length & Format	Description	Hashed
Recovered Data Header	1 b	Hex value '6A'.	No
Certificate Format	1 b	Hex value '11'.	Yes
ID of Certificate Subject (Issuer Identifier)	4 b	Leftmost 3-8 digits from the PAN, right padded with hex. 'F'. See Note 2.	Yes
Certificate Expiry Date	2 b	MMYY after which this certificate is invalid. See Note 1.	Yes
Certificate Serial Number	3 b	Chosen by the Issuer. See Note 1.	Yes
Hash Algorithm Indicator	1 b	Identifies the hash algorithm used to produce the Hash Result.	Yes
Subject Public Key Algorithm Indicator	1 b	Identifies the digital signature algorithm to be used with the Issuer's Public Key	Yes
Subject Public Key Modulus Length	1 b	Length of the Issuer Public Key Modulus in bytes (N _i)	Yes
Subject Public Key Exponent Length	1 b	Length of the Issuer Public Key Exponent (Number of bytes). Either hex 01 (for exponent 3) or hex 03 (for exponent 65537).	Yes
Leftmost Digits of Subject Public Key Modulus	N _i -36 b	Leftmost N _i -36 bytes of Issuer's Public Key Modulus	Yes
Hash Result	20 b	Hash of Issuer Public Key and its associated information.	No
Recovered Data Trailer	1 b	Hex value 'BC'.	No

*Self-Signed Issuer Public Key Certificate**(Self-Signed Certificate)*

Card Issuing Appendix C – Self-Signed Issuer Public Key Certificate Format (American Express)

Field Name	Length & Format	Description	
Header	1 b	Hex value '22'.	NOT SIGNED
Length of Issuer Public Key Modulus	1 b	Length of Issuer Public Key in Hex. (Number of bytes)	NOT SIGNED
Issuer Public Key Modulus	var b	Issuer's Public Key Modulus	NOT SIGNED
Issuer Public Key Exponent Length	1 b	Length of Issuer Public Key Exponent. (Number of bytes). Must be either hex 01 (for exponent 3) or hex 03 (for exponent 65537).	NOT SIGNED
Issuer Public Key Exponent	1 or 3 b	Issuer Public Key Exponent. Must be either 3 or 65537, that is, hex 03 or hex 01 00 01.	NOT SIGNED
Tracking Number	3 b	Number for transmittal tracking. See Note 1.	NOT SIGNED

Self-Signed Issuer Public Key Certificate

(Clear Data – Unsigned Issuer Public Key Input Extension)

Field Name	Length & Format	Description	Hashed
Header	1 b	Hex. value '23'.	Yes
Service Identifier	4 b	American Express Product Identifier Fixed value '00 00 00 00'	Yes
Certificate Format	1 b	Hex value '02'.	Yes
Issuer Identifier (BIN)	4 b	Issuer Identification Number (left justified and padded on the right with hexadecimal 'F's). See Note 2.	Yes
Certificate Expiration Date	2 b	MMYY after which this certificate is invalid. See Note 1.	Yes
Tracking Number	3 b	Number for transmittal tracking. See Note 1	Yes
Hash Algorithm Indicator	1 b	Identifies the hash algorithm used to produce the Hash Result.	Yes
Issuer's Public Key Algorithm Indicator	1 b	Identifies the digital signature algorithm to be used with the Issuer's Public Key.	Yes
Issuer Public Key Modulus Length	1 b	Identifies the length of the Issuer Public Key Modulus. (Number of bytes)	Yes
Issuer Public Key Exponent Length	1 b	Length e of the Issuer Public Key Exponent (Number of bytes). Either hex 01 (for exponent 3) or hex 03 (for exponent 65537).	Yes
Most Significant Part of Issuer Public Key Modulus	var b	Leftmost $N_i - (39 + e)$ bytes of Issuers Public Key Modulus	Yes
Issuer Public Key Exponent	1 or 3 b	Issuer Public Key Exponent. Is either 3 or 65537, that is, hex 03 or hex 01 00 01.	Yes
Hash Result	20 b	Hash of indicated fields.	No

*Self-Signed Issuer Public Key Certificate**(Self-Signed Issuer Public Key Data)*

Card Issuing Appendix D – Issuer Public Key Certificate Format (Visa)

Field Name	Length & Format	Description		Hashed
Header	1 b	Hex. value '24'.	NOT SIGNED	No
Visa Service Identifier	4 b	Identifies a Visa Service. The Proprietary Application Identifier Extension (PIC) is left justified and padded on the right with four hex zeros. Current valid International Service Identifiers are: Hex 1010 0000 : for Debit/Credit Hex 2010 0000 : for Electron Hex 3010 0000 : for Interlink Hex 8010 0000 : for PLUS Check with Visa regional offices for Regional/National service identifiers	NOT SIGNED	No
Issuer Identification Number	4 b	Leftmost 3-8 digits from the PAN, right padded with hexadecimal Fs. See Note 2.	NOT SIGNED	No
Certificate Serial Number	3 b	Certificate Serial Number assigned by Visa CA	NOT SIGNED	No
Certificate Expiration Date	2 b	MMYY after which this certificate is invalid. See Note 1.	NOT SIGNED	No
Issuer Public Key Modulus Remainder Length	1 b	Length of Issuer Public Key Modulus (N) Remainder in hex (Number of bytes)	NOT SIGNED	No
Issuer Public Key Modulus (N) Remainder	var b	Field only present if NI > NCA - 36, and consists of the NI-NCA + 36 least significant bytes of the Issuer Public Key Modulus (N). NI is the length, in bytes, of the Issuer Public Key Modulus and NCA is the length, in bytes, of the VSDC CA Key used for create the IPK certificate.	NOT SIGNED	Yes
Issuer Public Key Exponent Length	1 b	Length of Issuer Public Key Exponent e in hex. (Number of bytes). Either hex 01 (for exponent 3) or hex 03 (for exponent 65537).	NOT SIGNED	No
Issuer Public Key Exponent	1 or 3 b	Issuer Public Key Exponent. Is either 3 or 65537, that is, hex 03 or hex 01 00 01.	NOT SIGNED	Yes
CA Public Key Index	1 b	Public Key Index for CA Public Key used to create the Issuer Public Key Certificate	NOT SIGNED	No

Issuer Certificate

(Unsigned Data - Unsigned Issuer Public Key Output Extension)

Field Name	Length & Format	Description	Hashed
Recovered Data Header	1 b	Hex. value '6A'.	No
Certificate Format	1 b	Hex. value '02'.	Yes
Issuer Identification Number	4 b	Leftmost 3-8 digits from the PAN, right padded with hexadecimal Fs. See Note 2.	Yes
Certificate Expiration Date	2 b	MMYY after which this certificate is invalid. See Note 1.	Yes
Certificate Serial Number	3 b	Binary number unique to this certificate assigned by the Certification Authority	Yes
Hash Algorithm Indicator	1 b	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme.	Yes
Issuer Public Key Algorithm Indicator	1 b	Identifies the digital signature algorithm to be used with the Issuer Public Key.	Yes
Issuer Public Key Modulus Length	1 b	Identifies the length of the Issuer Public Key Modulus (Number of bytes)	Yes
Issuer Public Key Exponent Length	1 b	Identifies the length of the Issuer Public Key Exponent (Number of bytes)	Yes
Issuer Public Key Modulus (N) or Leftmost portion of the Issuer Public Key Modulus (N)	var b	If $N_I \leq N_{CA} - 36$, this field consists of the full Issuer Public Key Modulus (N) right padded with $N_{CA} - 36 - N_I$ 'BB' bytes. If $N_I > N_{CA} - 36$, this field consists of the $N_{CA} - 36$ most significant bytes of the Issuer Public Key Modulus (N).	Yes
Hash Result	20 b	Hash of the Issuer Public Key and related information.	No
Recovered Data Trailer	1 b	Hex. value 'BC'.	No

*Issuer Certificate**(Issuer Public Key Certificate)*

Field Name	Length & Format	Description
Header	1 b	Hex. value '00'.
Block Format Code	1 b	Hex. value '01'.
Padding Characters	var b	Hex. value 'FF'. The length of the padding is equal to the Signing key modulus - 38.
Separator	1 b	Hex. value '00'.
Algorithm Indicator	15 b	Hash Algorithm indicator used by the CA For SHA-1, Hex Value = '3021300906052b0e03021a05000414'
Hash Results	20 b	SHA-1 Hash of the concatenation of the Unsigned Data and the Issuer Public Key Certificate

Issuer Certificate

(Detached Signature)

Card Issuing Appendix E – Issuer Public Key Certificate Format (Mastercard)

Field Name	Length & Format	Description		Hashed
Issuer Identification Number	4 b	Leftmost 3-8 digits from the PAN, right padded with hexadecimal Fs. See Note 2.	NOT SIGNED	No
Issuer Public Key Index	3 b	Number, chosen by the Issuer, which uniquely identifies the Public Key.	NOT SIGNED	No
CA Public Key Index	1 b	The CA Public Key Index uniquely identifies a CA Public Key.	NOT SIGNED	No
Issuer (Subject) Public Key Modulus Remainder	var b	Field only present if $N_i > N_{CA} - 36$, and consists of the $N_i - N_{CA} + 36$ least significant bytes of the Issuer Public Key Modulus	NOT SIGNED	Yes
Issuer (Subject) Public Key Exponent	var b	Exponent ($e = 1$ to $N_i / 4$).	NOT SIGNED	Yes

Issuer Certificate

(Unsigned Data)

Field Name	Length & Format	Description	Hashed
Recovered Data Header	1 b	Hex. value '6A'.	No
Certificate Format	1 b	Hex. value '02'.	Yes
Issuer Identification Number	4 b	Leftmost 3-8 digits from the PAN, right padded with hexadecimal F. See Note 2.	Yes
Certificate Expiration Date	2 b	MMYY after which this certificate is invalid. See Note 1.	Yes
Certificate Serial Number	3 b	Binary number unique to this certificate assigned by the Certification Authority	Yes
Hash Algorithm Indicator	1 b	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme.	Yes
Issuer Public Key Algorithm Indicator	1 b	Identifies the digital signature algorithm to be used with the Issuer Public Key.	Yes
Issuer Public Key Modulus Length	1 b	Identifies the length of the Issuer Public Key Modulus (Number of bytes).	Yes
Issuer Public Key Exponent Length	1 b	Identifies the length of the Issuer Public Key Exponent (Number of bytes).	Yes
Issuer Public Key Modulus (N) or Leftmost portion of the Issuer Public Key Modulus (N)	var b	If $N_I \leq N_{CA} - 36$, this field consists of the full Issuer Public Key Modulus (N) right padded with $N_{CA} - 36 - N_I$ 'BB' bytes. If $N_I > N_{CA} - 36$, this field consists of the $N_{CA} - 36$ most significant bytes of the Issuer Public Key Modulus (N).	Yes
Hash Result	20 b	Hash of the Issuer Public Key and related information.	No
Recovered Data Trailer	1 b	Hex. value 'BC'.	No

Issuer Certificate
(Issuer Public Key Certificate)

Card Issuing Appendix F – Issuer Public Key Certificate Format (American Express)

Field Name	Length & Format	Description		Hashed
Header	1 b	Hex. value '24'.	NOT SIGNED	No
Service Identifier	4 b	American Express Product Identifier Fixed value '00 00 00 00'.	NOT SIGNED	No
Issuer Identification Number	4 b	Issuer Identification Number (left justified and padded on the right with hexadecimal 'F's). See Note 2.	NOT SIGNED	No
Certificate Serial Number	3 b	'01nnnn' where nnnn is the Tracking Number from the certificate request. See Note 1.	NOT SIGNED	No
Certificate Expiration Date	2 b	MMYY after which this certificate is invalid. See Note 1.	NOT SIGNED	No
Issuer Public Key Modulus Remainder Length (LN _I)	1 b	Number of bytes in Public Key Modulus Remainder ($LN^R_I = \max(LN_I - LN_{CA} + 36, 0)$)	NOT SIGNED	No
Issuer Public Key Modulus Remainder (N ^R _I)	var b	Field present if $LN^R_I > 0$, contains LN^R_I least significant (rightmost) bytes of the Issuer Public Key Modulus	NOT SIGNED	Yes
Issuer Public Key Exponent Length (Le _I)	1 b	Number of bytes for Public Key Exponent in hex.	NOT SIGNED	No
Issuer Public Key Exponent (e _I)	Le _I b	Issuer Public Key Exponent in hex ($e_I = 1$ to $NI / 4$)	NOT SIGNED	Yes
CA Public Key Index	1 b	Public Key Index for CA Public Key used to create the Issuer Public Key Certificate.	NOT SIGNED	No

Issuer Certificate

(Unsigned Data - Unsigned Issuer Public Key Output Extension)

Field Name	Length & Format	Description	Hashed
Recovered Data Header	1 b	Hex. value '6A'.	No
Certificate Format	1 b	Hex. value '02'.	Yes
Issuer Identification Number	4 b	Issuer Identification Number (left justified and padded on the right with hexadecimal 'F's). See Note 2.	Yes
Certificate Expiration Date	2 b	MMYY after which this certificate is invalid. See Note 1.	Yes
Certificate Serial Number	3 b	'01nnnn' where nnnn is the Tracking Number from the certificate request.	Yes
Hash Algorithm Indicator	1 b	Identifies the hash algorithm used to produce the Hash Result.	Yes
Issuer Public Key Algorithm Indicator	1 b	Identifies the digital signature algorithm to be used with the Issuer's Public Key.	Yes
Issuer Public Key Modulus Length (LN _I)	1 b	Identifies the length of the Issuer Public Key Modulus (Number of bytes)	Yes
Issuer Public Key Exponent Length (Le _I)	1 b	Identifies the length of the Issuer Public Key Exponent (Number of bytes)	Yes
Issuer Public Key Modulus (N) or Leftmost portion of the Issuer Public Key Modulus (N)	LN _{CA36} b	LN _I > LN _{CA} -36; MS part of Modulus LN _I = LN _{CA} -36; Full Modulus only LN _I < LN _{CA} -36; Full Modulus appended with 'BB' pad of LN _{CA} -36- LN _I bytes	Yes
Hash Result	20 b	Hash of the Issuer Public Key and related information.	No
Recovered Data Trailer	1 b	Hex. value 'BC'.	No

*Issuer Certificate**(Issuer Public Key Certificate)*

Field Name	Length & Format	Description
Header	1 b	Hex. value '00'.
Block Format Code	1 b	Hex. value '01'.
Padding Characters	var b	Hex. value 'FF'. The length of the padding is equal to the Signing key modulus - 38.
Separator	1 b	Hex. value '00'.
Algorithm Indicator	15 b	OID for SHA-1, '30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14'.
Hash Results	20 b	SHA-1 Hash of the concatenation of the Unsigned Data and the Issuer Public Key Certificate.

Issuer Certificate

(Detached Signature)

Card Issuing Appendix G – Format of Card (ICC) Public Key Certificate

Field Name	Length & Format	Description
Certificate Format	1 b	Hex value '04'.
Application PAN	10 b	PAN padded on the right with hex Fs. See Note 2.
Certificate Expiration date	2 b	MMYY, after which this certificate is invalid. See Note 1.
Certificate Serial Number	3 b	Binary number unique to this certificate assigned by the issuer. See Note 1.
Hash Algorithm Indicator	1 b	Identifies the hash algorithm used to produce the Hash Result. '01' means SHA-1.
ICC Public Key Algorithm indicator	1 b	Identifies the digital signature algorithm to be used with the ICC Public Key. '01' means RSA.
ICC Public Key Modulus length	1 b	Identifies the length of ICC Public Key Modulus in bytes
ICC Public Key Exponent length	1 b	Identifies the length of the ICC Public Key Exponent in bytes. Either hex 01 (for exponent 3) or hex 03 (for exponent 65537).
Leftmost bytes of the ICC Key Modulus	N _I -42 b	If N _{IC} < N _I -42, this field consists of the full ICC Public Key padded to the right with N _I -42-N _{IC} bytes of value hex 'BB' if necessary. If N _{IC} > N _I -42, this field consists of the N _I -42 most significant bytes of the ICC Public Key Modulus.
ICC Public Key Modulus Remainder	0 or N _{IC} -N _I +42 b	This field is only present if N _{IC} > N _I -42 and consists of N _{IC} -N _I +42 least significant bytes of the ICC Public Key Modulus.
ICC Public Key Exponent	1 or 3 b	ICC Public Key Exponent. Is either 3 or 65537, that is, hex 03 or hex 01 00 01.
Static Data	var b	Static Data to be Authenticated. <i>Note: This field is only present for the Card Public Key Data and is not present for the Card PIN Encipherment Public Key Data.</i>

Card (ICC) Public Key Data to be signed by the Issuer

(Input to hash algorithm)

Field Name	Length & Format	Description
Recovered Data Header	1 b	Hex. value '6A'.
Certificate Format	1 b	Hex. value '04'.
Application PAN	10 b	PAN padded on the right with hex Fs. See Note 2.
Certificate Expiration date	2 b	MMYY, after which this certificate is invalid. See Note 1.
Certificate Serial Number	3 b	Binary number unique to this certificate assigned by the issuer. See Note 1.
Hash Algorithm Indicator	1 b	Identifies the hash algorithm used to produce the Hash Result below. '01' means SHA-1.
ICC Public Key Algorithm indicator	1 b	Identifies the digital signature algorithm to be used with the ICC Public Key. '01' means RSA
ICC Public Key Modulus length	1 b	Identifies the length of ICC Public Key Modulus in bytes
ICC Public Key Exponent Length	1 b	Identifies the length of the ICC Public Key Exponent in bytes. Either hex 01 (for exponent 2 or 3) or hex 03 (for exponent 65537).
ICC Public Key modulus or leftmost bytes of the ICC Public Key modulus	N _I -42 b	If N _I C =< N _I -42, this field consists of the full ICC Public Key padded to the right with N _I -42-N _I C bytes of value hex 'BB' if necessary. If N _I C > N _I -42, this field consists of the N _I -42 most significant bytes of the ICC Public Key Modulus.
Hash Result	20 b	Hash of Card (ICC) Public Key and its related information
Recovered data trailer	1 b	'BC'.

*Content of the Card (ICC) Certificate**(Deciphered)*

Card Issuing Appendix H – Private Key Encodings

ASN.1 encoding of a Private Key

An RSA Private Key has the following ASN.1 encoded format:

```
RSAPrivateKey ::= SEQUENCE{
    p BIT STRING,
    q BIT STRING,
    d1 BIT STRING,
    d2 BIT STRING,
    q-1 mod p BIT STRING}
```

When using ASN.1 encoding, the value 30 indicates a sequence and the value 03 indicates a bit string. As a result, a ASN.1 encoded private key will appear as follows:

```
30 | Length of Complete Sequence | 03 | Bit String Length | p | 03 | Bit String Length | q | 03 | Bit
String Length | d1| 03 | Bit String Length | d2| 03 | Bit String Length | q-1 mod p |
```

When defining the length of the bit string, the length of the bit string in bytes is given first, followed by the number of bits that are ignored in the last byte. For example "101010" is encoded as 03 02 02 A8, where 03 is a bit string, 02 is the length, 02 is the number of bits dropped from the end of the data, and A8 is the zero padded data (note that the padding can be any value as it is ignored).

The following example shows the five data items that make up a key and then shows the key ASN.1 encoded:

p:
FADD62A62492706C 5784790CDC40D76C
5CA0736FA0E07CAA EB1729C1C7FF18E1
70EFC25B7711C907 B515542ACFD80823

q:
EC43DD6A0F955408 09579E9A8D0DECC3
B4050712A28C97F0 6521505342D6E102
58F3BBBB845CBAB0 3B136EC6A7E1F6E9

dp (d1):
A73E41C41861A048 3A5850B33D808F9D
9315A24A6B40531C 9CBA1BD68554BB40
F5F52C3CFA0BDB5A 78B8E2C7353AB017

dq (d2):
9D82939C0A638D5A B0E5146708B3F32D
22AE04B71708654A EE16358CD739EB56
E5F7D27D02E87C75 7CB79F2F1A96A49B

U (q inverse mod p):
CEB3DA4206C267C1 1EF3DCCB77268707
09E735BED60E68D5 3C0E573FB64A634F
376B15CCC0219C5A 02F09B834048ECB9

For the ASN.1 Encoded Private Key, the bit string indicators have been underlined and the length indicators are in italic to aid with clarity.

```
30 81 FF 03 31 00 FA DD 62 A6 24 92 70 6C 57 84  
79 0C DC 40 D7 6C 5C A0 73 6F A0 E0 7C AA EB 17  
29 C1 C7 FF 18 E1 70 EF C2 5B 77 11 C9 07 B5 15  
54 2A CF D8 08 23 03 31 00 EC 43 DD 6A 0F 95 54  
08 09 57 9E 9A 8D 0D EC C3 B4 05 07 12 A2 8C 97  
F0 65 21 50 53 42 D6 E1 02 58 F3 BB BB 84 5C BA  
B0 3B 13 6E C6 A7 E1 F6 E9 03 31 00 A7 3E 41 C4  
18 61 A0 48 3A 58 50 B3 3D 80 8F 9D 93 15 A2 4A  
6B 40 53 1C 9C BA 1B D6 85 54 BB 40 F5 F5 2C 3C  
FA 0B DB 5A 78 B8 E2 C7 35 3A B0 17 03 31 00 9D  
82 93 9C 0A 63 8D 5A B0 E5 14 67 08 B3 F3 2D 22  
AE 04 B7 17 08 65 4A EE 16 35 8C D7 39 EB 56 E5  
F7 D2 7D 02 E8 7C 75 7C B7 9F 2F 1A 96 A4 9B 03  
31 00 CE B3 DA 42 06 C2 67 C1 1E F3 DC CB 77 26  
87 07 09 E7 35 BE D6 0E 68 D5 3C 0E 57 3F B6 4A  
63 4F 37 6B 15 CC C0 21 9C 5A 02 F0 9B 83 40 48  
EC B9
```

CRT Encoding of Private Key Components

This section describes how the 5 Chinese Remainder Theorem (CRT) components are formatted.

The length in bits of each of the CRT components is half the modulus length rounded up to the next bit (i.e. if the modulus is 1007 bits, then the CRT component size is 504 bits).

The size of each component is determined by defining a function CEIL(X) as X/24 rounded up to the next highest integer, and then multiplied by 3, where X is the CRT component size in bits (i.e. CEIL(504) is 504/24=21, multiplied by 3 to get 63). This will be the native size of CRT components before any formatting or padding (required to make it a multiple of 8 bytes for DES encryption).

The plaintext component block is generally formatted as follows:

Length	CRT component	Padding
(1 byte) optional	Var.	'0000..' to 8 bytes or '80' '00..' to 8 bytes or 4 bytes (8000 0000) or 8 bytes (8000 0000 0000 0000)

- If Length Bytes is 0 the length is not included with the CRT component.
- If mandatory padding *is not* required, the padding characters are '00' to make the length a multiple of 8 bytes.
- If mandatory padding *is* required, the padding characters will be a single byte of 80 followed by 00 bytes to make a multiple of 8 bytes, or 4 bytes (8000 0000) or 8 bytes (8000 0000 0000 0000).

Alternative CRT Output formats for a Private Key

Commands in this document have the ability to output a Private Key in the form of 5 Chinese Remainder Theorem components. These are p, q, d1, d2, q-1 mod p. It is also possible to select either of the conditions q>p or p>q.

Some applications may require that the 5th component (q-1 mod p) is provided in a different form such as the modular inverse of p (or p-1 mod q). It is possible to obtain an output in this format as follows:

1. If the condition q>p is required:

- Select the condition p>q (i.e. the opposite of what is required)
- From the returned 5 components (p, q, d1, d2, q-1 mod p) rearrange them according to the following table.

For new component	Use returned component
p	q
q	p
d1	d2
d2	d1
$p^{-1} \text{ mod } q$	$q^{-1} \text{ mod } p$

2. If the condition p>q is required:

- Select the condition q>p (i.e. the opposite of what is required)
- From the returned 5 components (p, q, d1, d2, q-1 mod p) rearrange them according to the table above.

Exponent/Modulus Encoding of Private Keys

The private key exponent (d) and modulus (n) are given in the following format:

Length | Private Key Exponent (d) or Modulus (n) | Padding

The length is an n byte value (though usually 0 or 1) which indicates the length (in bytes) of the following field, which may be the Private Key Exponent (d) or the Modulus (n). This value is given in HEX E.g. 0x40 corresponds to a key size of 64. If the number of bytes specified for the length is zero then this field will be omitted, giving an output as follows:

Private Key Exponent (d) or Modulus (n) | Padding

If mandatory padding **is not** required, the padding characters are '00' to make the total length of all three (or two) parts a multiple of 8 bytes.

If mandatory padding is required, the padding characters will be either 4 bytes (8000 0000) or 8 bytes (8000 0000 0000 0000).

Card Issuing Appendix I – MULTOS Card Public Key Certificate Format

MULTOS V3.0

A MULTOS v3.0 public key certificate (MCD_PK_C) is a total of 136 bytes, comprising:

Certificate public key length	2 bytes
Certificate key header	38 bytes
Key Certificate	96 bytes

The 38 byte Certificate key header has the following format:

Miscellaneous data	18 bytes
Public key exponent length	2 bytes
Public exponent	4 bytes
Miscellaneous data	5 bytes
msm_controls_data_date	1 byte
mcd_no	8 bytes

Notes:

- The miscellaneous data will be ignored.
- The "Public Key Exponent Length" denotes (in bytes) the actual length of the public exponent.
- The "Public Exponent" is left justified and padded with 00 to a total of 4 bytes.

Examples:

- If public exponent = 3 (decimal) then:
 "public exponent" = 03 00 00 00 , and
 "public key exponent length" = 00 01
- If public exponent = 65537 (decimal) then:
 "public exponent" = 01 00 01 00 , and
 "public key exponent length" = 00 03

Extraction of Public Key from Certificate - The Key Certificate is encrypted using the MULTOS CA Key Transport Key (TKCK_PK). The plain value of the Key Certificate comprises:

Hash Digest	16 bytes
Card public key modulus	72 bytes
Random padding	8 bytes

The Hash Digest is an Asymmetrical Hash of the certificate header.

Certificate Authentication - In order to authenticate the certificate, the hash digest recovered from the certificate must match the digest of the header. The hash algorithm is described in Card Issuing Appendix K – MULTOS Hash Modulus File Format. For MULTOS v3.0 it is a single hash.

MULTOS V4.0

A MULTOS v4.0 public key certificate (MCD_PK_C) can take one of two forms, depending on the relative lengths of the smart card public key modulus and the MULTOS CA Key Transport Key (TKCK_PK) modulus.

Let N = length (in bytes) of the MULTOS CA Key Transport Key (TKCK_PK) modulus and let M = length (in bytes) of the smart card public key modulus. The case of $N \geq M+56$ is not allowed. If the keys submitted in the command satisfy this condition an error code will be returned to the host.

Case 1 $(M+32) \leq N < (M+56)$

In this case the card public key certificate (MCD_PK_C) has the following format:

Certificate public key length	2 bytes
Key Header	38 bytes
Key Certificate	N bytes

The 38 byte Key Header has the following format:

Miscellaneous data	13 bytes
Public key length	2 bytes
Certifying key length	2 bytes
Miscellaneous data	1 byte
Public key exponent length	2 bytes
Public exponent	4 bytes
Miscellaneous data	5 bytes
msm_controls_data_date	1 byte
mcd_no	8 bytes

Notes:

- The 19 bytes of miscellaneous data will be ignored by the HSM.
- The "Public exponent" is left justified and padded with 00 to a total of 4 bytes.
- The "Public key exponent length" denotes (in bytes) the actual length of the public exponent.

Examples:

- If public exponent = 3 (decimal) then:
 "Public exponent" = 03 00 00 00 , and
 "Public key exponent length" = 00 01
- If public exponent = 65537 (decimal) then:
 "Public exponent" = 01 00 01 00 , and
 "Public key exponent length" = 00 03

- If public exponent = 257 (decimal) then:

"Public exponent" = 01 01 00 00 , and

"Public key exponent length" = 00 02

Extraction of Public Key from Certificate - The Key Certificate is encrypted using the MULTOS CA Key Transport Key (TKCK_PK). The plain value of the Key Certificate comprises:

Hash Result	16 bytes
Padding	N-M-32 bytes
Card public key modulus	M bytes
Redundancy	16 bytes

Case 2 N < (M+32)

In this case the card public key certificate (MCD_PK_C) has the following format:

Certificate public key length	2 bytes
Key Header	38 bytes
Card public key modulus left part	M-N+32 bytes
Key Certificate	N bytes

The 38 byte Key header has the same format as in Case 1.

Extraction of Public Key from Certificate - The Key Certificate is encrypted using the MULTOS CA Key Transport Key (TKCK_PK). The plain value of the Key Certificate comprises:

Hash Digest	16 bytes
Card public key modulus right part	N-32 bytes
Redundancy	16 bytes

Concatenate the Card Public Key modulus left part and the Card Public key right part to form the card public key modulus.

Certificate Authentication - In order to authenticate the certificate, the hash digest recovered from the certificate must match the digest of the header. The hash algorithm is described in Card Issuing Appendix K – MULTOS Hash Modulus File Format. For a MULTOS v4.0 this is done with two asymmetric hashes.

Card Issuing Appendix J – MULTOS Transport Key Certifying Key File Format

The MULTOS CA Public Key (TKCK) is supplied in the following file format prior to being reformatted into standard ASN.1 DER encoded public key.

Data Field	Description	Length (in bytes)
File_Type_Code	ASCII, 4 Character. Set to "TKCK"	4
File_Protection_Method	Binary. Set to 0x01	1
File_Structure_Method	Binary. Set to 0x01	1
Consignment_File_ID	ASCII. 8 Characters. Set to "TKCK", followed by 4 characters presenting the identifier (in hex). This will be the same as the MKD_Cert_Method_ID. For example: "TKCK0113" would be version 19 (decimal) of a MULTOS 4 96 byte TKCK	8
Date	Date	4
Time	Time	3
MKD_Cert_Method_ID	Binary. Comprised of: scheme ID, 1 byte + key version number, 1 byte Currently defined scheme IDs are: 0x00 for MULTOS 3 platforms with a 96 byte TKCK 0x01 for MULTOS 4 platforms with a 96 byte TKCK 0x02 for MULTOS 4 platforms with a 128 byte TKCK	2
Key_Length	Binary. This should match the value inferred from the scheme ID byte of the MKD_Cert_Method_ID	2
Key_Data	Binary. The actual public key (TKCK_PK)	Key-Length
Hash_Code	Binary. A SHA-1 hash of the MKD_Cert_Method_ID, Key_Length and Key_Data.	20

Key data contains the public key modulus. The exponent is always assumed to be 3.

Card Issuing Appendix K – MULTOS Hash Modulus File Format

The MULTOS Hash Modulus File (HASH) is supplied in the following format prior to being reformatted into standard ASN.1 DER encoded format public key.

Data Field	Description	Length (in bytes)
File_Type_Code	ASCII, 4 Character. Set to "HASH"	4
File_Protection_Method	Binary. Set to 0x01	1
File_Structure_Method	Binary. Set to 0x01	1
Consignment_File_ID	ASCII. 8 Characters. Set to "HASH", followed by 4 characters presenting the identifier (in hex). This will be the same as the Hash_Method_ID. For example: "HASH0105"	8
Date	Date	4
Time	Time	3
Hash_Method_ID	Binary	2
Key_Length	Binary	2
Key_Data	Binary. The actual Hash Modulus	Key_Length
Hash_Code	Binary. A SHA-1 hash of the Hash_Method_ID, Key_Length and Key_Data.	20

Card Issuing Appendix L – Self Signed CA Public Key Certificate Format (Visa)

Field Name	Length & Format	Description	Signed	Hashed
Header	1 b	Hex value '20'	No	No
Service Identifier	4 b	<p>Identifies a Visa Service. The Proprietary Application Identifier Extension (PIX) is left justified and padded on the right with four hex zeros.</p> <p>Current valid International Service Identifiers are:</p> <ul style="list-style-type: none"> Hex 1010 0000 – for Debit/Credit Hex 2010 0000 – for Electron Hex 3010 0000 – for Interlink Hex 8010 0000 – for PLUS <p>Note: The Service Identifier of the VSDC CA Public Key is always 1010 0000, regardless of the Service Identifier of the Issuer's Public Key as requested in the Issuer's Public Key Input File.</p>	No	No
Length of Public Key Modulus (N_{CA})	2 b	Length of CA Public Key Modulus in Hex. (No. of bytes)	No	No
Public Key Algorithm Indicator	1 b	Identifies cryptographic algorithm to be used with the CA Public Key. RSA = "01" hex	No	No
Public Key Exponent Length	1 b	Length of CA Public Key Exponent in Hex. (No. of bytes)	No	No
Registered Application Provider Identifier (RID)	5 b	Visa Identifier = 'A000000003'	No	Yes
Public Key Index	1 b	Unique CA Public Key Serial No.	No	Yes
Public Key Modulus (N_{CA})	var b	CA Public Key Modulus	No	Yes
Public Key Exponent (e)	var b	CA Public Key Exponent	No	Yes
Hash Result	20 b	Hash of fields indicated above	No	No

Self Signed CA Public Key Certificate

(Clear Data - Unsigned Output Extension)

Field Name	Length & Format	Description
Header	1 b	Hex value '21'
Service Identifier	4 b	<p>Identifies a Visa Service. The Proprietary Application Identifier Extension (PIX) is left justified and padded on the right with four hex zeros. Current valid International Service Identifiers are: Hex 1010 0000 – for Debit/Credit Hex 2010 0000 – for Electron Hex 3010 0000 – for Interlink Hex 8010 0000 – for PLUS</p>
Registered Application Provider Identifier (RID)	5 b	Visa Identifier = 'A00000003'
Public Key Index	1 b	Unique CA Public Key Serial Number
Certificate Expiration Date	2 b	MMYY after which this certificate is invalid. See Note 1.
Public Key Algorithm Indicator	1 b	Identifies cryptographic algorithm to be used with the CA Public Key
Leftmost portion of CA Public Key Modulus (N_{CA})	var b	(N - [36+e]) bytes of the CA Public Key Modulus (N)
Hash Algorithm Indicator	1 b	Identifies the hash algorithm used to produce the Hash Result. SHA-1 = "01" hex.
Public Key Exponent Length	1 b	Length of CA Public Key Exponent (Number of bytes)
Public Key Exponent (e)	var b	Exponent of CA Public Key
Hash Result	20 b	Hash value from unsigned output extension

*Self Signed CA Public Key Certificate**(Self-Signed Certificate)*

Card Issuing Appendix M – Self Signed CA Public Key Certificate Format (Mastercard)

Field Name	Length & Format	Description	Signed	Hashed
ID of Certificate	5 b	The "Registered Application Provider Identifier" (RID)	No	No
Public Key Index	1 b	Public Key Index, which uniquely identifies a Public Key.	No	No
Public Key Algorithm Indicator	1 b	Indicates the algorithm to be used with the Public Key. RSA = "01" hex	No	No
Public Key Length	1 b	Length of Public Key Modulus (equal to N_{CA})	No	No
Public Key Exponent Length	1 b	Length of Public Key Exponent	No	No
Leftmost Digits of Public Key	N_{CA} -37 b	N_{CA} -37 most significant bytes of the Public Key Modulus	No	No
Public Key Remainder	37 b	37 least significant bytes of the Public Key Modulus	No	Yes
Public Key Exponent	var b	Public Key Exponent	No	Yes

Self Signed CA Public Key Certificate

(Clear Data)

Field Name	Length & Format	Description	Hashed
Recovered Data Header	1 b	Hex value '6A'	No
Certificate Format	1 b	Hex value '10'	Yes
ID of Certificate	5 b	The "Registered Application Provider Identifier" (RID)	Yes
Certificate Expiration Date	2 b	MMYY after which this certificate is invalid. See Note 1.	Yes
Certificate Serial Number	3 b	Inserted by scheme provider.	Yes
Hash Algorithm Indicator	1 b	Identifies the hash algorithm used to produce the Hash Result. SHA-1 = "01" hex.	Yes
Public Key Algorithm Indicator	1 b	Identifies the digital signature algorithm to be used with the Public Key. RSA = "01" hex	Yes
Public Key Length	1 b	Length of the Public Key Modulus in bytes (N_{CA})	Yes
Public Key Exponent Length	1 b	Length of Issuer Public Key Exponent in bytes (from 01 to 04)	Yes
Leftmost Digits of Public Key	$N_{CA}-37$ b	Leftmost $N_{CA}-37$ bytes of the Public Key Modulus	Yes
Hash Result	20 b	Hash of Public Key and its associated information.	No
Recovered Data Trailer	1 b	Hex value "BC"	No

Self Signed CA Public Key Certificate

(Self-Signed Certificate)

Card Issuing Appendix N - Self Signed CA Public Key Certificate Format (American Express)

Field Name	Length& Format	Description	Signed	Hashed
Header	1 b	Fixed value '20'	No	No
Service Identifier (SI)	4 b	American Express Product Identifier Fixed value '00 00 00 00'	No	No
Length of Public Key Modulus (N _{CA})	2 b	Number of bytes in Public Key Modulus (i.e., '80' = 1024 bits, '90' = 1152 bits, 'B0' = 1408 bits, 'F8' = 1984 bits) Length is right justified and padded with '00'	No	No
Public Key Algorithm Identifier	1 b	Cryptographic algorithm to be used with the Public Key ('01' = RSA)	No	No
Public Key Exponent Length	1 b	Number of bytes in Public Key Exponent (e.g., '01')	No	No
Registered Application Provider Identifier (RID)	5 b	American Express Identifier = 'A000000025'	No	Yes
Public Key Index	1 b	CA Key Pair Index	No	Yes
Public Key Modulus (N _{CA})	var b	Public Key Modulus	No	Yes
Public Key Exponent (e _{CA})	var b	Public Key Exponent (e _{CA} = 1 to N _{CA} / 4) (e.g., '03' Hexadecimal)	No	Yes
Hash Result	20 b	Hash of the fields indicated above	No	No

Self Signed CA Public Key Certificate

(Clear Data - Unsigned Output Extension)

Field Name	Length & Format	Description
Header	1 b	Fixed value '21'
Service Identifier (SI)	4 b	American Express Product Identifier Fixed value '00 00 00 00'
Registered Application Provider Identifier (RID)	5 b	American Express Identifier = 'A000000025'
Public Key Index	1 b	CA Key Pair Index
Certificate Expiration Date	2 b	MMYY after which the certificate is invalid (CA private key expiration date). See Note 1.
Public Key Algorithm Indicator	1 b	Cryptographic algorithm to be used with the Public Key ('01' - RSA)
Most Significant Part of Public Key Modulus (N _{CA})	var b	N _{CA} - [36+e _{CA}] bytes of the Modulus data. (36 = number of bytes in fixed fields)
Hash Algorithm Indicator	1 b	Cryptographic algorithm used to generate the Hash ('01' - SHA-1)
Public Key Exponent Length	1 b	Number of bytes in Public Key Exponent (e.g., '01')
Public Key Exponent (e _{CA})	var b	Public Key Exponent (e _{CA} = 1 to N _{CA} / 4) (e.g., '03' Hexadecimal)
Hash Result	20 b	Hash value from unsigned output extension

Self Signed CA Public Key Certificate

(Self-Signed Certificate)

Card Issuing Appendix O – DC_SUK block template

The DC_SUK block has JSON format. The 'IY' command accepts as input a JSON template having the form:

```
{
  "serviceData": {
    "DC_SUK_CONTENT": {
      "ATC": "*",
      "IDN": "*",
      "RFU": "*",
      "SK_CL_MD": "*",
      "SK_RP_MD": "*",
      "SUKInfo": "*",
      "SUK_CL_UMD": "*",
      "SUK_RP_UMD": "*",
      "hash": "*"
    },
    "DC_SUK_ID": "5413339000001513FFFF001503840903280001150326"
  },
  "serviceID": "PROVISIONSUK",
  "serviceRequestID": "1427295513175"
}
```

The 'IY' command populates the JSON template replacing the wildcard '*' characters with the actual plain text key and data values for example:

```
{
  "serviceData": {
    "DC_SUK_CONTENT": {
      "ATC": "0001",
      "IDN": "DA98438667C8FDC2",
      "RFU": "00",
      "SK_CL_MD": "225BC8E86ED81A00F9CF9C74A6653BD5",
      "SK_RP_MD": "E8E486F384C8F1F8D5ED020E035391D8",
      "SUKInfo": "38",
      "SUK_CL_UMD": "FC24AF40DA0D2E8F5A83D7933CF521B6",
      "SUK_RP_UMD": "4F982FBF2186B4A7F82C45C25C0E216D",
      "hash": "01B05522B12D0BB1A61215F762D4005686CC5769"
    },
    "DC_SUK_ID": "5413339000001513FFFF001503840903280001150326A25EE16119ED291D2EE9651B"
  },
  "serviceID": "PROVISIONSUK",
  "serviceRequestID": "1427295513175"
}
```

14 AS2805 Appendices

AS2805 Appendix A – One-Way Functions

OWF - 1988

One-way functions for single and double length keys are defined as follows:

Single Length Key

Let K be a single length key and let D be a 64-bit data block.

- Step 1 Decrypt D with K.
- Step 2 Combine the result of Step 1 with D using the exclusive-or operation.

The result of Step 2 is the required value, denoted OWF(K,D).

Double Length Key

Let *K be a double length key and let D be a 64-bit data block.

- Step 1 Decrypt D with the left half of *K.
- Step 2 Encrypt the result of Step 1 with the right half of *K.
- Step 3 Decrypt the result of Step 2 with the left half of *K.
- Step 4 Combine the result of Step 3 with D using the exclusive-or operation.

The result of Step 4 is the required value, denoted *OWF(*K,D).

OWF - 2000

Described in AS2805 Appendix N – AS 2805.6.2 Support Appendices.

AS2805 Appendix B – Derivation of the Privacy Key

The Privacy Key (denoted KD) is derived from the Transaction Key (KT) and two 64-bit fields (known as the E Field and the F Field) as described below.

The E Field is derived from the Systems Trace Audit Number (STAN) and the F Field is derived from the Card Acceptor Terminal Identification (CATID) as follows:

E Field: The 6 digits (24 bits) of the STAN, left justified and right zero filled to a total length of 64 bits, shifted left 1 bit.

F Field: The 16 characters (64 bits) of the CATID, shifted left 1 bit and zero filled.

Step 1 Combine the E Field and the F Field using the exclusive-or operation.

Step 2 Combine the KT and the constant value 2222222222222222 (hex) using the exclusive-or operation.

Step 3 The KD is the result of the OWF (see AS2805 Appendix A – One-Way Functions) with the result of step 1 as the key and the result of step 2 as the data.

AS2805 Appendix C – Key Check Value

Check values for single and double length keys are defined as follows:

Single Length Key

Let K be a single length key.

Step 1 Encrypt a block of 64 binary zeros with K.

The leftmost 24 bits of the result of Step 1 is the required check value, denoted KCV(K).

Double Length Key

Let K be a double length key.

Step 1 Encrypt a block of 64 binary zeros with the left half of K.

Step 2 Decrypt the result of Step 1 with the right half of K.

Step 3 Encrypt the result of Step 2 with the left half of K.

The leftmost 24 bits of the result of Step 3 is the required check value, denoted KCV(K).

See Ref.8.4 - AS2805.6.3,

See Ref.8.5 - AS2805.6.4,

AS2805 Appendix D – Key Encrypting Key Variants

Different variants of key encrypting keys (ZMK or TMK) are required to encrypt different types of session keys during distribution between communicating entities. These variants are defined as follows:

NOTE: The variant used is determined by the length of the key being encrypted, NOT the length of the key performing the encryption

Zone or Terminal Authentication keys

ZAK / TAK (Variant A)

variant Single length = 2424 2424 2424 2424 (hex)

variant Double length = 2424 2424 2424 2424 2424 2424 2424 2424 (hex)

variant Triple length = N /A

ZAKs / TAKs (Variant B)

Generate variant Single Length = 2424 2424 2424 2424 (hex)

Generate variant Double Length = 24C0 24C0 24C0 24C0 24C0 24C0 24C0 24C0 (hex)

Generate variant Triple Length = 2430 2430 2430 2430 2430 2430 2430 2430 2430 2430 2430 2430 2430 (hex)

ZAKr / TAKr (Variant C)

Verify variant Single Length = 4848 4848 4848 4848 (hex)

Verify variant Double Length = 48C0 48C0 48C0 48C0 48C0 48C0 48C0 48C0 (hex)

Verify variant Triple Length = 4830 4830 4830 4830 4830 4830 4830 4830 4830 4830 4830 4830 4830 (hex)

Zone or Terminal Encryption keys

ZEK / TEK (Variant E)

variant Single Length = 2222 2222 2222 2222 (hex)

variant Double Length= 2222 2222 2222 2222 2222 2222 2222 2222 (hex)

variant Triple Length = N / A

ZEKs / TEKs (Variant F)

Encipher variant Single Length = 2222 2222 2222 2222 (hex)

Encipher variant Double Length = 22C0 22C0 22C0 22C0 22C0 22C0 22C0 22C0 (hex)

Encipher variant Triple Length = 2230 2230 2230 2230 2230 2230 2230 2230 2230 2230 2230 2230 2230 (hex)

ZEKr / TEKr / KA / KCA (Variant G)

Decipher variant Single Length = 4444 4444 4444 4444 (hex)

Decipher variant Double Length = 44C0 44C0 44C0 44C0 44C0 44C0 44C0 44C0 (hex)

Decipher variant Triple Length = 4430 4430 4430 4430 4430 4430 4430 4430 4430 4430 4430 4430 4430 4430 (hex)

Zone or Terminal PIN keys

ZPK or TPK (Variant H)

variant Single Length = 2828 2828 2828 2828 (hex)
variant Double Length = 28C0 28C0 28C0 28C0 28C0 28C0 28C0 28C0 (hex)
variant Triple Length (hex) = 2830 2830 2830 2830 2830 2830 2830 2830 2830 2830 2830 2830

Variant 7 (Variant I)

variant Single Length = 8282 8282 8282 8282 (hex)
variant Double Length = 8282 8282 8282 8282 8282 8282 8282 8282 (hex)
variant Triple Length = N /A
Note: When key scheme type is H
variant Double Length = 82C0 82C0 82C0 82C0 82C0 82C0 82C0 82C0 (hex)

Variant 8 (Variant J)

variant Single Length = 8484 8484 8484 8484 (hex)
variant Double Length = 8484 8484 8484 8484 8484 8484 8484 8484 (hex)
variant Triple Length = N /A
Note: When key scheme type is H
variant Double Length = 84C0 84C0 84C0 84C0 84C0 84C0 84C0 84C0 (hex)

Variant 88 (Variant K)

variant = 88888888888888888888888888888888 (hex)
{Used for enciphering PPASN under KIA}

In each case the appropriate variant is combined with the double length key encrypting key using the exclusive-or operation and the result is used to encrypt the session key.

Variant 0 (Variant M)

variant = 00000000 00000000 00000000 00000000 (hex)
{Used for enciphering TMK* under KIA}

In each case the appropriate variant is combined with the double length key encrypting key using the exclusive-or operation and the result is used to encrypt the session key.

AS2805 Appendix G – Definition of Card Values

Card Values CV_1 - CV_5 are generated from four values, each 8 hexadecimal characters in length, known as the A Field, B Field, C Field and D Field.

CV_1 - CV_5 are formed from the concatenation of pairs of these fields as follows:

- CV_1 : concatenation of A and B
- CV_2 : concatenation of B and A
- CV_3 : concatenation of A and C
- CV_4 : concatenation of B and D
- CV_5 : concatenation of C and D

See Ref.8.5 - AS2805.6.4.

AS2805 Appendix H – Generation of Initial Terminal Master Keys

Initial double length Terminal Master Keys (TMKs) are derived from the Card Values CV_1 - CV_6 and the PIN Pad Acquirer Security Number (PPASN). CV_1 - CV_5 are derived from the A, B, C and D Fields, as defined in AS2805 Appendix G – Definition of Card Values.

Step 1 - Derive a Temporary TMK₁

This value is formed from the concatenation of OWF(CV_6, CV_1) and OWF(CV_6, CV_5), where OWF(K,D) is defined in AS2805 Appendix A – One-Way Functions.

Step 2 - Derive a Temporary TMK₂

This value is formed from the concatenation of OWF(CV_6, CV_2) and OWF(CV_6, CV_4), where OWF(K,D) is defined in AS2805 Appendix A – One-Way Functions.

Step 3 - Form Initial TMK₁

Let K_L and K_R denote, respectively, the left and right halves of the result of Step 1. The Initial TMK₁ is formed from the concatenation of OWF($K_L, PPASN$) and OWF($K_R, PPASN$), where OWF(K,D) is defined in AS2805 Appendix A – One-Way Functions.

Step 4 - Form Initial TMK₂

Let K_L and K_R denote, respectively, the left and right halves of the result of Step 2. The Initial TMK₂ is formed from the concatenation of OWF($K_L, PPASN$) and OWF($K_R, PPASN$), where OWF(K,D) is defined in AS2805 Appendix A – One-Way Functions.

See Ref.8.5 - AS2805.6.4

AS2805 Appendix I – Terminal Master Key Update

There are two possibilities for the update of the Terminal Master Keys - either TMK₁ only needs to be updated or else both TMK₁ and TMK₂ need to be updated.

AS2805 – 1988 Method

Update TMK1 only

The inputs in this case are Old TMK₁ and the PIN Pad Acquirer Security Number (PPASN). The output is the New TMK₁.

Let K_L and K_R denote, respectively, the left and right halves of Old TMK₁, then New TMK₁ is formed from the concatenation of OWF(K_L,PPASN) and OWF(K_R,PPASN), where OWF(K,D) is defined in AS2805 Appendix A – One-Way Functions.

Update TMK₁ and TMK₂

The inputs in this case are Old TMK₂ and the PIN Pad Acquirer Security Number (PPASN). The output is the New TMK₁ and New TMK₂.

Step 1

Form an Intermediate TMK, by combining each half of the Old TMK₂ with PPASN, using the exclusive-or operation. Let K_L and K_R denote, respectively, the left and right halves of Intermediate TMK, then New TMK₁ is formed from the concatenation of OWF(K_L,PPASN) and OWF(K_R,PPASN), where OWF(K,D) is defined in AS2805 Appendix A – One-Way Functions.

Step 2

Let K_L and K_R denote, respectively, the left and right halves of Old TMK₂, then New TMK₂ is formed from the concatenation of OWF(K_L,PPASN) and OWF(K_R,PPASN), where OWF(K,D) is defined in AS2805 Appendix A – One-Way Functions.

AS2805 – 2001 Method

Update TMK1 only

The inputs in this case are Old TMK₁ and the PIN Pad Acquirer Security Number (PPASN). The output is the New TMK₁.

See AS2805.6.4 – 2001 §6.4.3 as follows, for method. (uses OWF – 2000 {AS2805.4 – 2000 §6})

Update TMK1 and TMK2

The inputs in this case are Old TMK₂ and the PIN Pad Acquirer Security Number (PPASN). The output is the New TMK₁ and New TMK₂.

See AS2805.6.4 – 2001 §6.4.4 as follows, for method. (uses OWF – 2000 {AS2805.4 – 2000 §6})

Terminal KEK update

General

The terminal maintains two terminal master keys for each acquirer with which it is required to communicate. These are known as KEK1 and KEK2

Inputs

The inputs to the key enciphering key update procedure shall be PPASN and the existing terminal key enciphering keys.

Algorithm KEK1 update

KEK1 shall be updated as follows

- Concatenate PPASN with itself to form the temporary value D.
- Use the OWF with the existing KEK1 as the key and the temporary value D as the data to produce the new 128-bit value of KEK1.
- The new value of KEK1 replaces the existing value in storage.

The process is illustrated in Figure 1.

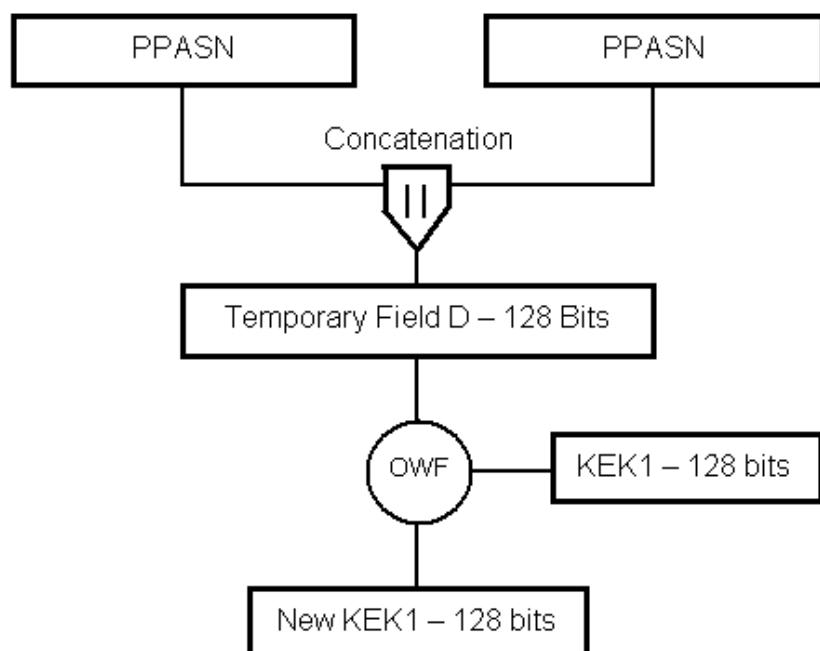


FIGURE 1 KEK1 UPDATE PROCEDURE

© Standards Australia

Algorithm KEK2 update

KEK2 shall be updated as follows:

Concatenate PPASN with itself to form the temporary value D.

Create a temporary new KEK by the modulo 2 addition of D to the existing KEK2.

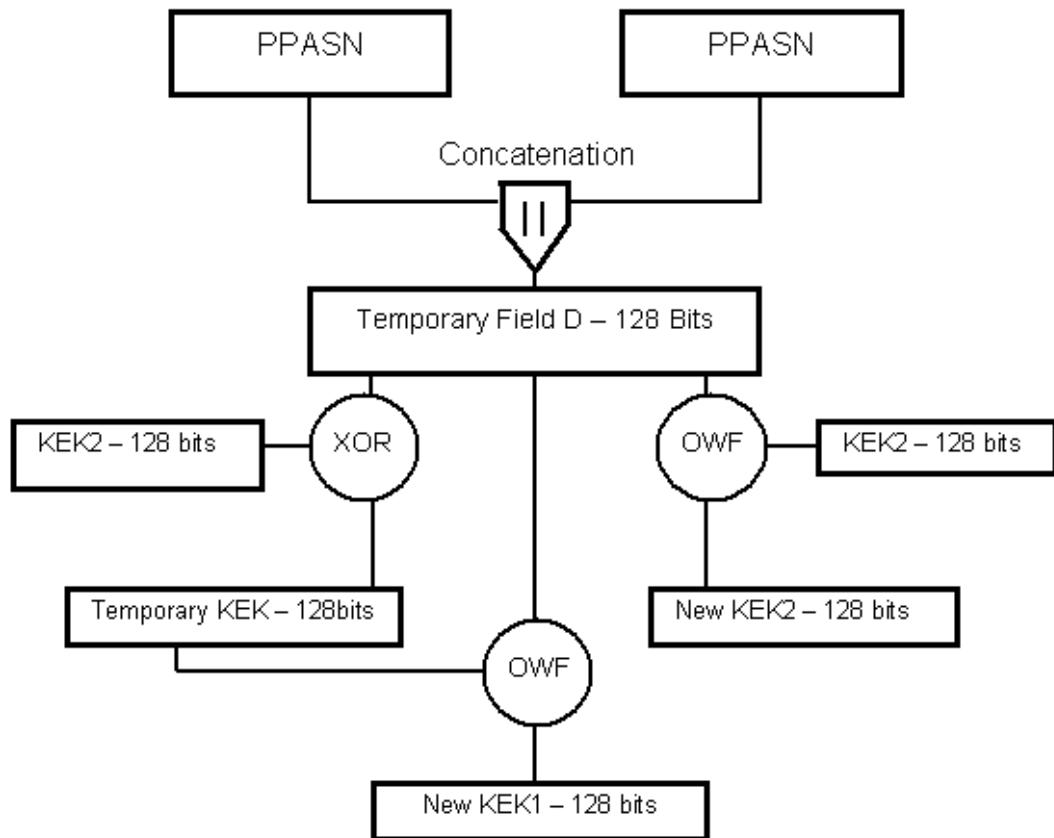
Use the OWF with the existing KEK2 as the key and the D as the data to produce the new 128-bit value of KEK2.

The new value of KEK2 replaces the existing value in storage.

Use the OWF with the temporary KEK produced in Step (b) as the key and the value D as the data to produce the new 128-bit value of KEK1.

The new value of KEK1 replaces the old KEK1 in storage.

The process is illustrated in Figure 2.



**FIGURE 2 KEK2 UPDATE
PROCEDURE**

© Standards Australia

AS2805 Appendix J – Derivation of the PIN Encryption Key

Single Length TPK

The PIN Encryption Key (KPE) is formed by combining a single length Terminal PIN Key (TPK) with two 64-bit fields (known as the E Field and the F Field) using the exclusive-or operation.

The E Field is derived from the Systems Trace Audit Number (STAN) and the F Field is derived from the transaction amount, as follows:

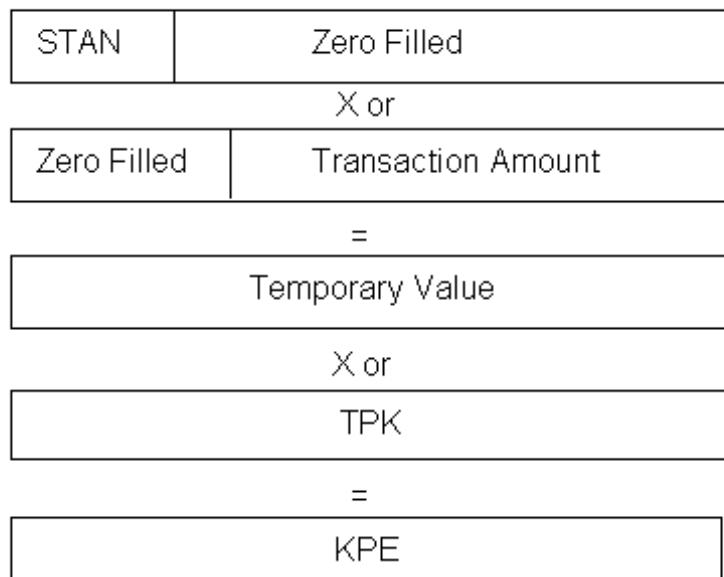
E Field: The 6 digits (24 bits) of the STAN, left justified and right zero filled to a total length of 64 bits, shifted left 1 bit.

F Field: The 12 digits (48 bits) of the transaction amount, right justified and left zero filled to a total length of 64 bits, shifted left 1 bit.

Fields E & F are X'or ed to form a temporary value.

This temporary value is then X'or ed with the TPK to form the KPE

Example:



See - AS2805.6.4, Section 6.9. (1988)

Double Length TPK

See Ref.8.5 - AS2805.6.4 § 6.6.3 (2001) as follows:

PIN enciphering key (KPE)

General

The PIN enciphering key (KPE) is used to encipher the PIN block.

Inputs

The inputs to the KPE calculation shall be the systems trace audit number (STAN), transaction amount, and PIN protection key (KPP)

Algorithm

KPE shall be calculated as follows:

Field E comprises the 6 digits (24 bits) of the STAN, left justified, and right zero-filled to a total length of 64 bits.

Field F comprises the 12 digits (48 bits) of the transaction amount, right justified and left zero-filled to a total length of 64 bits.

Field E and F are concatenated to produce the temporary value D.

Use the OWF with the KPP as the key and D as the data.

The result is KPE.

The process is illustrated in Figure 3.

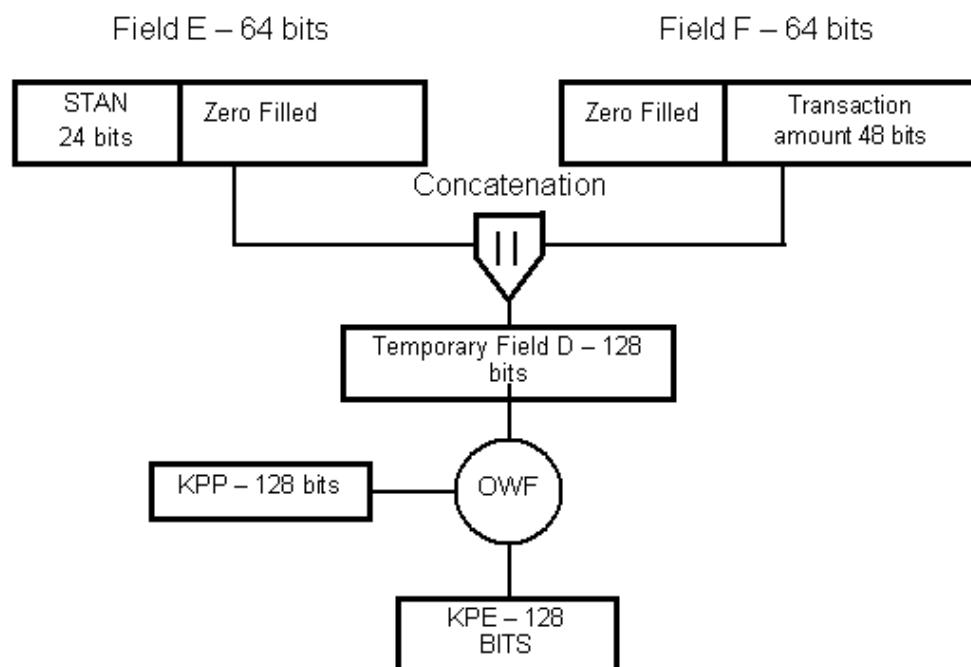


FIGURE 3 KPE CALCULATION

AS2805 Appendix K – AS2805.3 PIN block formats

AS2805 Format 1 PIN block

The AS2805 Format 1 PIN block is used in situations where the account number is not available. The PIN block is formed by concatenation of the PIN and other data.

The AS2805 Format 1 PIN block has the format;

C	N	P	P	P	P	P/T	T	T							
---	---	---	---	---	---	-----	-----	-----	-----	-----	-----	-----	-----	---	---

Where;

- C = Control field = binary 0001
- N = PIN length = binary 0100 to 1100
- P = PIN digit = binary 0000 to 1001
- P/T = PIN/other = determined by PIN length
- T = Other data = binary 0000 to 1111

This format is accommodated by using the standard Format 05 for the PIN block and entering all "zero's" in place of the account number in PIN functions.

AS2805.3 Format 8 PIN block (format 46)

Support for "zero" length PIN block

The zero length PIN block format is identical to format 01 with the following exceptions.

If the Control Field is 0, then the PIN block is processed as a standard format 01 PIN block. If the Control Field is not 0 then the following rules apply.

If the second character is 0 then the PIN block is a Zero PIN block. No checking of the PIN block is required in this case.

If the second character is not 0 or in the range 4 to C (hex), inclusive, then return error code 24 and terminate processing.

If the input command is a verify PIN command and the second character is 0 then return error code 88 and terminate processing.

If the input command is a translate PIN command and the second character is 0, form a new PIN block as follows:

The new PIN block has the format 80RRRRRRRRRRFF (hex), where R denotes a random hexadecimal character.

When a Zero PIN block is encountered in a standard PIN verify or PIN translate command, error code 88 will be returned as notification only. Processing will continue.

The individual standard commands affected by this PIN Block format are:

CA, CC, DA, DC, EA and EC

AS2805 Appendix L – Error messages

Most error messages are standard across all commands. Each command lists those errors specifically for it, but some standard checking functions may produce other errors that are only shown in this table. Some codes have more than one description where the error condition is more specific in a particular command; this is detailed in the command response.

Code : Description

00 : No errors	16 : Console or printer not ready / not connected
01 : Verification failure. CAM validation error. Data Length error.	17 : HSM not in authorized state
02 : Key inappropriate length for algorithm. Hash validation failure. Invalid MK length.	18 : Document definition format not loaded
03 : Invalid message type. Invalid secret key type. Data Length error. Zero PINblock received.	19 : Specified Diebold table is invalid
04 : Invalid key type code. Invalid secret key flag. Public key does not conform to encoding rules. Key Length invalid	20 : PIN block error.
05 : Invalid key length flag. Invalid message block number. Invalid hash identifier. Invalid number of Input pairs or not even.	21 : Invalid index value, or index / block count would cause overflow condition
06 : Invalid signature identifier. Invalid public key Algorithm Identifier	22 : Invalid account number
07 : Public exponent length error. MAC mode, key length mismatch.	23 : Invalid PIN block format code
08 : Invalid public exponent	24 : PIN is fewer than 4 or more than 12 digits long. PIN is not 4 digits.
09 : Secret key error, report to supervisor	25 : Decimalization table error
10 : Source key parity error. Or other input key parity error.	26 : Invalid key scheme
11 : Destination key parity error. Key all 0s.	27 : Incompatible key length
12 : Contents of user storage not available. Reset, power down or overwrite.	28 : Invalid key type
13 : LMK error - report to Supervisor	29 : Key function not permitted
14 : PIN encrypted under LMK pair 02-03 is invalid	30 : Invalid reference number
15 : Invalid input data – unable to identify the individual fields in the input	31 : Insufficient solicitation entries for batch
78 : SK length error	33 : LMK key change storage is corrupt
80 : Data length error. The MAC or other data amount is not as expected	40 : Invalid firmware checksum
81 : Signature length error	41 : Internal hardware / software error: bad RAM, invalid error codes, etc.
82 : Invalid trailer	42 : DES failure
83 : Invalid certificate format	47 : Hardware failure
	49 : Corrupt SK
	50 : Key comprises all zeros
	51 : KV parity error
	76 : Signature/KEK length <> modulus length
	77 : Decrypted Signature/KEK blocks corrupt
	90 : Data parity error in the request message received by the HSM
	97 : RSA key generation error

84 : Invalid subject ID	
-------------------------	--

88 : Zero PIN block encountered; advice only.	
---	--

AS2805 Appendix M – Australian Key Schemes

Five key schemes (G, H, I, K and L) are specified for this firmware. They are used for the import and export of keys under Zone Master keys, Terminal Master Keys and Key Encrypting Keys.

The Key scheme G applies to single length keys. The Key schemes H & K apply to double length keys. The key schemes I & L apply to triple length keys.

The mechanism for the key schemes G, H and I is to apply an appropriate variant (see AS2805 Appendix D – Key Encrypting Key Variants) to the encrypting key then to encrypt the working key using the CBC method.

Key schemes K and L also use the CBC mode of encryption, but do not apply a variant prior to encrypting the key.

NOTE: The variant used is determined by the length of the key being encrypted, **NOT** the length of the key performing the encryption

Examples:

G Scheme. (Single Length Data/Session Key)

With the 'G' scheme regardless of the length of the key encrypting the Data/Session key the variant applied from AS2805 Appendix D – Key Encrypting Key Variants is the single length variant.

e.g.

ZMK – 0404 0404 0404 0404 0808 0808 0808 0808

ZAK – 2020 2020 2020 2020

ZAK Variant - 2424 2424 2424 2424 2424 2424 2424 2424 (from AS2805 Appendix D – Key Encrypting Key Variants)

Encrypting Key (ZMK with variant applied) – 2020 2020 2020 2020 2C2C 2C2C 2C2C 2C2C

ZAK Encrypted under ZMK (ZAK CBC encrypted using ZMK with variant applied)

G 7B19 0BFF 522D E15D

H Scheme. (Double Length Data/Session Key)

With the 'H' scheme regardless of the length of the key encrypting the Data/Session key the variant applied from Appendix D is the double length variant.

e.g.

ZMK – 0404 0404 0404 0404 0808 0808 0808 0808

ZAK – 2020 2020 2020 2020 4040 4040 4040 4040

ZAK Variant - 24C0 24C0 24C0 24C0 24C0 24C0 24C0 24C0 (from AS2805 Appendix D – Key Encrypting Key Variants)

Encrypting Key (ZMK with variant applied) – 20C4 20C4 20C4 20C4 2CC8 2CC8 2CC8 2CC8

ZAK Encrypted under ZMK (ZAK CBC encrypted using ZMK with variant applied)

H 27C9 B3BA C267 FEA7 1BF6 8BC1 5837 5F8C

I Scheme. (Triple Length Data/Session Key)

With the 'I' scheme regardless of the length of the key encrypting the Data/Session key the variant applied from AS2805 Appendix D – Key Encrypting Key Variants is the triple length variant.

e.g.

ZMK – 0404 0404 0404 0404 0808 0808 0808 0808

ZAK – 2020 2020 2020 2020 4040 4040 4040 4040 0D0D 0D0D 0D0D 0D0D 0D0D

ZAK Variant - 2430 2430 2430 2430 2430 2430 2430 2430 (AS2805 Appendix D – Key Encrypting Key Variants)

Encrypting Key (ZMK with variant applied) – 2034 2034 2034 2034 2C38 2C38 2C38 2C38

ZAK Encrypted under ZMK (ZAK CBC encrypted using ZMK with variant applied)

I E2D5 D40F 9433 DBCB 77AB 8654 D404 1AAF 4F53 4FE0 C7C0 E103

K Scheme. (Double Length Data/Session Key)

This scheme uses the CBC mode of encryption, and no variant is applied to the key encryption key.

e.g.

ZMK – 0404 0404 0404 0404 0808 0808 0808 0808

ZAK – 2020 2020 2020 2020 4040 4040 4040 4040

ZAK encrypted under ZMK (ZAK CBC encrypted using ZMK with no variant applied) –

K C1FB 7F83 BA2E 91C0 C466 7057 C58A 1A72

L Scheme. (Triple Length Data/Session Key)

This scheme uses the CBC mode of encryption, and no variant is applied to the key encryption key.

e.g.

ZMK – 0404 0404 0404 0404 0808 0808 0808 0808

ZAK – 2020 2020 2020 2020 4040 4040 4040 4040 0D0D 0D0D 0D0D 0D0D 0D0D

ZAK Encrypted under ZMK (ZAK CBC encrypted using ZMK with no variant applied) –

L C1FB 7F83 BA2E 91C0 C466 7057 C58A 1A72 99D4 E6AE 4BEB 49CD 29C3 7CE6 F6AB CB0B

Commands that support Australian key schemes

Standard console commands

KG, IK, KE

Standard host commands

A0, A6, A8, BW, EA, EC, CC, BU

AS2805 host commands

OI, OK, OO, OQ, CO, OY, PI, D6, E0, E2, E8, H8

AS2805 Appendix N – AS 2805.6.2 Support Appendices

AS2805 Appendix N – A: One-way Function

The One-way Function (OWF) used in the commands specified in this document is defined in the AS2805.5.4 standard (Ref.8). It is described below.

Let K be a DES key and let D be a data block, of arbitrary length, n bits.

If n is not a multiple of 64 then append a single binary "1" followed by as many binary zeros as necessary to make the data a multiple of 64 bits (possibly none). Let D^* denote the padded data. Two distinct cases exist:

Case 1 – D^* has length 64 (and so $n \leq 64$)

Decrypt D^* with K.

Combine the result of step 1 with D^* , using the exclusive-or operation.

Discard the rightmost $(64-n)$ bits of the result of step 2 and denote the result by X, so that X has length n bits.

Then:

$$X = OWF(K, D).$$

Case 2 – D^* has length greater than 64 (and so $n > 64$)

Let V denote the final 64-bit block of CBC encryption of D^* with K, with a zero initial value.

Encrypt D^* with K, using CBC encryption and an initial vector = V.

Combine the result of step 2 with D^* , using the exclusive-or operation.

Discard the number of padding bits originally appended to D from the result of step 3 and denote the result by Y, so that Y has length n bits.

Then:

$$Y = OWF(K, D).$$

AS2805 Appendix N – B: Derivation of Data Values

A number of 128-bit Data Values (DV1, DV2, DV4, DV5 and DV6) are derived from data fields on track 2 of the card. These fields are each 32 bits in length and are known as fields A, B, C and D. They are defined as follows, where " | " denotes concatenation:

"A | B" denotes the 16 character PAN, including the check digit, immediately preceding the Field Separator.

"C | D" denotes the 16 character "Other Card Data", immediately following the YYMM field.

From fields A, B, C and D, five Card Values (CV1 – CV5) are formed:

$$CV1 = A | B$$

$$CV2 = B | A$$

$$CV3 = A | C$$

$$CV4 = B | D$$

$$CV5 = C | D$$

Then,

$$DV1 = CV1 | CV1$$

$$DV2 = CV2 | CV2$$

$$DV4 = CV3 | CV4$$

$$DV5 = CV4 | CV3$$

$$DV6 = CV5 | CV5$$

Finally, two other Data Values DV3 (128 bits) and DV7 (64 bits) are defined as follows.

Define the 64-bit values (left justified and zero padded, if necessary):

STAN = Systems Trace Audit Number

CATID = Card Acceptor Terminal Identification

AT = Transaction Amount

Then,

$$DV3 = STAN | CATID$$

$$DV7 = (STAN \oplus CATID \oplus AT),$$

where " \oplus " denotes the exclusive-or operation.

AS2805 Appendix N – C: MAC Key Derivation

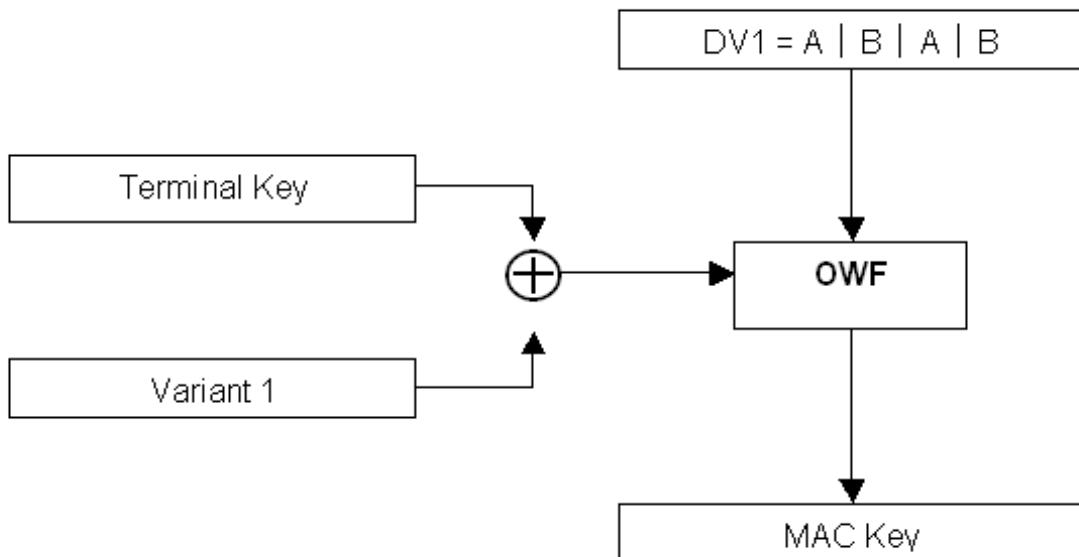
The transaction MAC Key is derived from the Data Value DV1 (see AS2805 Appendix N – B: Derivation of Data Values) and a variant of the Terminal Key, via:

$$\text{MAC Key} = \text{OWF}((\text{Terminal Key}) \oplus (\text{Variant 1}), \text{DV1}),$$

where \oplus denotes the exclusive-or operation and Variant 1 is defined as

Variant 1 = X'24C024C024C024C024C024C024C024C0.

In diagrammatic form:



AS2805 Appendix N – D: PIN Encipherment Key Derivation

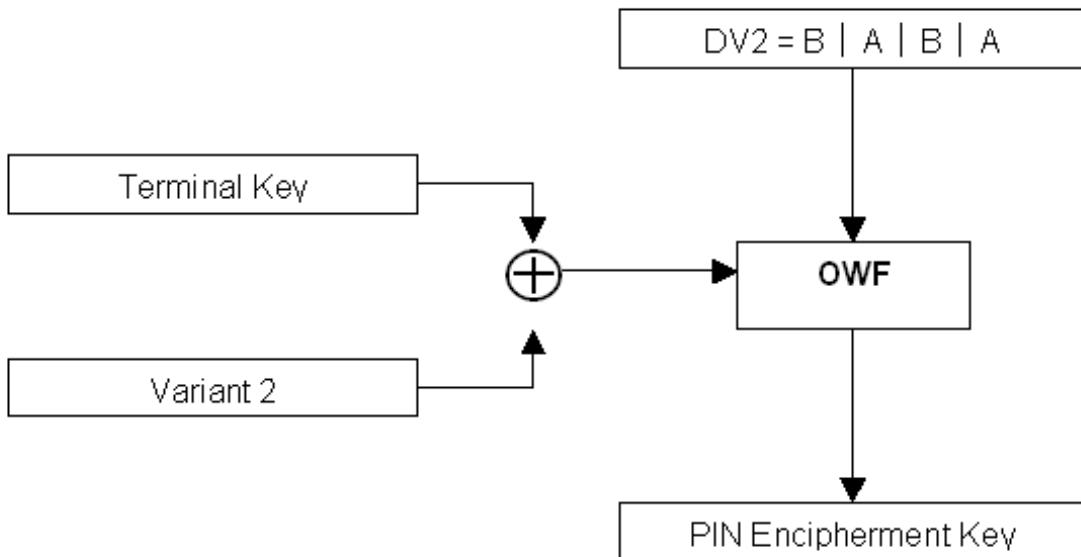
The transaction PIN Encipherment Key is derived from the Data Value DV2 (see AS2805 Appendix N – B: Derivation of Data Values) and a variant of the Terminal Key, via:

PIN Encipherment Key = OWF(Terminal Key) \oplus (Variant 2), DV2,

where \oplus denotes the exclusive-or operation and Variant 2 is defined as

Variant 2 = X'28C028C028C028C028C028C028C0.

In diagrammatic form:



AS2805 Appendix N – E: Privacy Key Derivation

The Privacy Key derivation used with the QM & QO commands specified at Section 10.15 and 10.16 respectively.

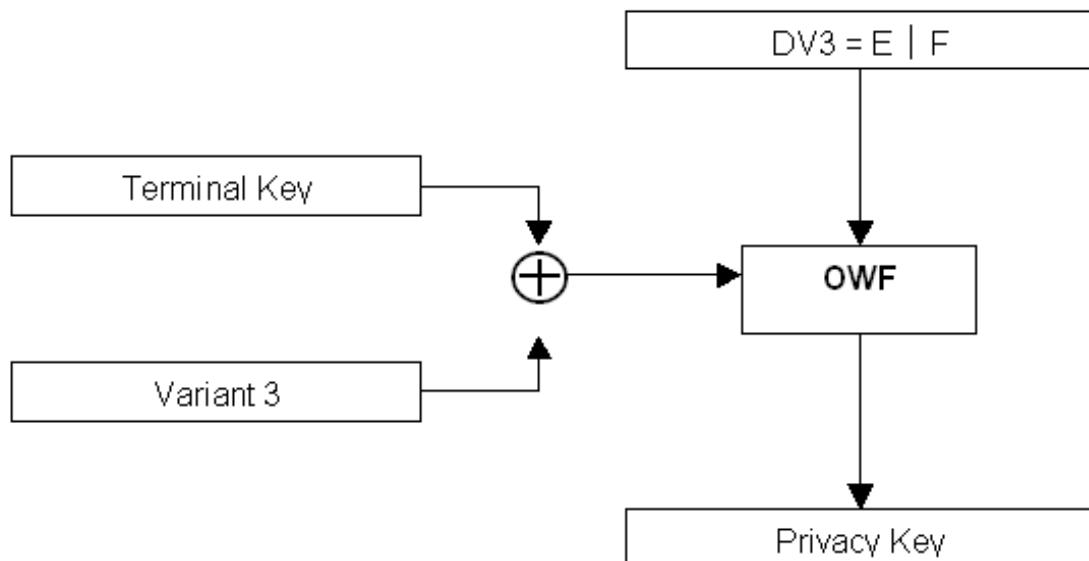
The transaction Privacy Key is derived from the Data Value DV3 (see AS2805 Appendix N – B: Derivation of Data Values) and a variant of the Terminal Key, via:

Privacy Key = OWF((Terminal Key) \oplus (Variant 3), DV3),

where \oplus denotes the exclusive-or operation and Variant 3 is defined as

Variant 3 = X'22C022C022C022C022C022C022C022C0.

In diagrammatic form:



AS2805 Appendix N – F: Terminal Key Update (AS2805.6.2)

A Terminal Key is updated as follows:

Concatenate the 64-bit MAC Residue (X) from the Request Message and the 64-bit MAC Residue (Y) from the Response Message, to form a 128-bit value, Data. Then,

New Terminal Key = OWF(Current Terminal Key, Data).

AS2805 Appendix N – G: MAC and MAC Residue Calculation

A Message Authentication Code (MAC) is calculated over a data block D, using a double length key K. A MAC may be 32, 48 or 64 bits in length, as required.

1. Append as many binary zeros to D as necessary to produce a data block D* with length a multiple of 64 bits.
2. Let C denote the last ciphertext block obtained by encrypting D* with K, using the CBC mode of encryption with a zero initial value.
3. Then

$$C = MAB(K, D)$$

and

MAC(K, D) = leftmost 32, 48 or 64 bits of MAB(K, D), as required.

4. Encrypt C with K, using the ECB mode of encryption to produce the MAB Extension.
5. Concatenate MAB(K, D) and the MAB Extension to form the Extended MAB.
6. Then the MAC Residue, MAR(K, D), is defined as the **next** 64 bits of the Extended MAB after MAC(K, D).

Three cases are possible:

MAC Length	MAR(K, D)
32 bits	Bits 33 – 96 of the Extended MAB, where the leftmost bit is bit 1
48 bits	Bits 49 – 112 of the Extended MAB, where the leftmost bit is bit 1
64 bits	Bits 65 – 128 of the Extended MAB, where the leftmost bit is bit 1

AS2805 Appendix N – H: Authentication Parameter

The Authentication Parameter (AP or Auth Para) is a 64-bit value constructed by the Card Issuer, or his agent, to confirm the approval of a transaction and, specifically, the amount of the transaction. AP is calculated using the One-way Function (OWF), defined in AS2805 Appendix N – A: One-way Function and various Data Values, defined in AS2805 Appendix N – B: Derivation of Data Values, as follows:

Let

Card Key = OWF(DV4, DV5),

then

Decoupling Key = OWF(Card Key, DV6)

and

AP = OWF(Decoupling Key, DV7).

AS2805 Appendix O – AS 2805.6.2 (Single DES) Support Appendices

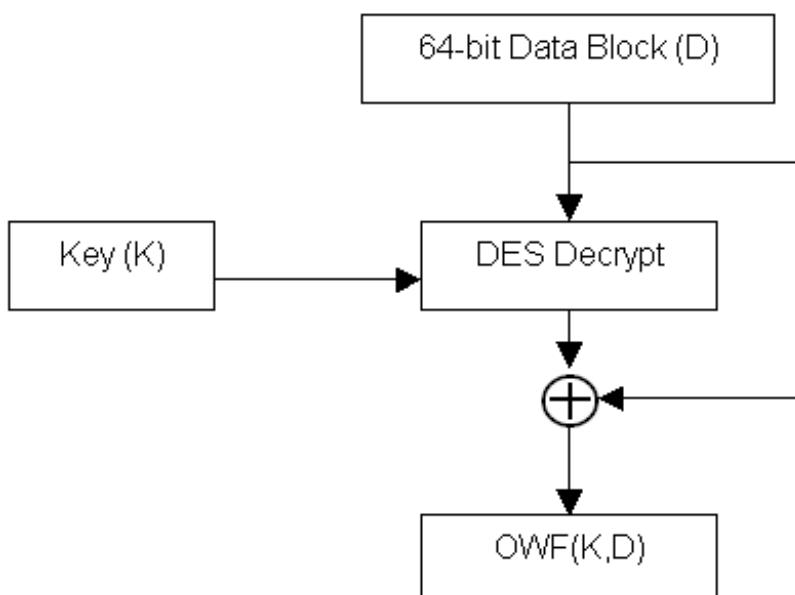
AS2805 Appendix O – A: One-way Function

The One-way Function (OWF) used in the commands specified in this document is described below. Let K be a single length DES key and let D be a 64-bit data block.

1. Decrypt D with K.
2. Combine the result of step 1 with D, using the exclusive-or operation, and denote the result by X.
3. Then:

$$X = \text{OWF}(K, D).$$

In diagrammatic form:



AS2805 Appendix O – B: Derivation of Card and Data Values

A number of Card Values (CV1, CV2, CV3, CV4 and CV5) are derived from data fields on track 2 of the card. These fields are each 32 bits in length and are known as fields A, B, C and D. They are defined as follows, where " | " denotes concatenation:

"A | B" denotes the 16 character PAN, including the check digit, immediately preceding the Field Separator.

"C | D" denotes the 16 character "Other Card Data", immediately following the YYMM field.

From fields A, B, C and D, the five Card Values (CV1 – CV5) are formed:

$$CV1 = A | B$$

$$CV2 = B | A$$

$$CV3 = A | C$$

$$CV4 = B | D$$

$$CV5 = C | D$$

One further Data Value DV6 (64 bits) is defined as follows.

Define the 64-bit values:

STAN = Systems Trace Audit Number (6 digits (24 bits), left shifted one bit and right filled with binary zeros);

CATID = Card Acceptor Terminal Identification (8 characters (64 bits), left shifted one bit and right filled with binary zeros);

AT = Transaction Amount (12 digits (48 bits), right justified and left filled with binary zeros).

Then,

$$DV6 = (STAN \oplus CATID \oplus AT),$$

where " \oplus " denotes the exclusive-or operation.

where " \oplus " denotes the exclusive-or operation.

AS2805 Appendix O – C: MAC Key Derivation

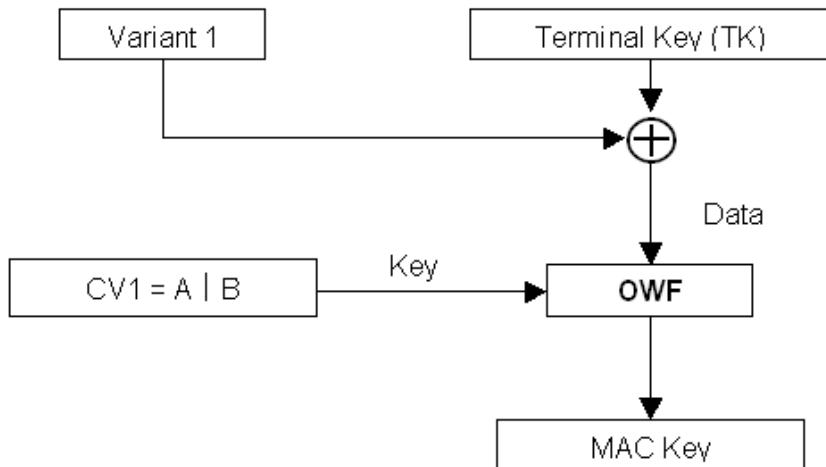
The transaction MAC Key is derived from the Card Value CV1 (see AS2805 Appendix O – B: Derivation of Card and Data Values) and a variant of the Terminal Key, via:

$$\text{MAC Key} = \text{OWF}(\text{CV1}, (\text{Terminal Key}) \oplus (\text{Variant 1})),$$

where \oplus denotes the exclusive-or operation and Variant 1 is defined as

Variant 1 = X'2424242424242424.

In diagrammatic form:



Important Note:

In the MAC Key derivation, above, CV1 is used as the key input to the OWF and ((Terminal Key) \oplus (Variant 1)) is used as the data input to the OWF.

AS2805 Appendix O – D: PIN Encipherment Key Derivation

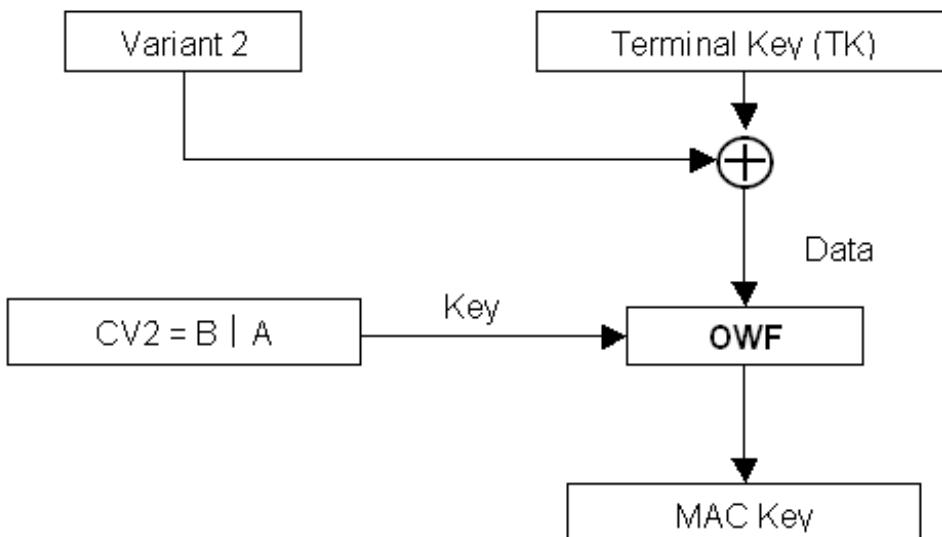
The transaction PIN Encipherment Key is derived from the Card Value CV2 (see AS2805 Appendix O – B: Derivation of Card and Data Values) and a variant of the Terminal Key, via:

PIN Encipherment Key = OWF(CV2, (Terminal Key) \oplus (Variant 2)),

where \oplus denotes the exclusive-or operation and Variant 2 is defined as

Variant 2 = X'2828282828282828.

In diagrammatic form:



Important Note:

In the PIN Encipherment Key derivation, above, CV2 is used as the key input to the OWF and $(\text{Terminal Key}) \oplus (\text{Variant 2})$ is used as the data input to the OWF.

AS2805 Appendix O – E: Terminal Key Update

A Terminal Key is updated as follows:

Concatenate the 32-bit MAC Residue (MARX) from the Request Message and the 32-bit MAC Residue (MARY) from the Response Message, to form a 64-bit value, Data. Then,

New Terminal Key = OWF(Current Terminal Key, Data).

Important Note:

The New Terminal Key must **not** be adjusted for parity.

Important Note:

In the New Terminal Key derivation, above, the Current Terminal Key is used as the **key** input to the OWF and the concatenation of the MARX and MARY is used as the **data** input to the OWF.

AS2805 Appendix O – F: MAC and MAC Residue Calculation

A 32-bit Message Authentication Code (MAC) is calculated over a data block D, using a single length key K. This process also produces a 32-bit MAC Residue (MAR).

1. Append as many binary zeros to D as necessary to produce a data block D* with length a multiple of 64 bits.
2. Let C denote the last ciphertext block obtained by encrypting D* with K, using the Cipher Block Chaining (CBC) mode of encryption with a zero initial value.
3. Then

MAC(K, D) = leftmost 32 bits of C and MAR(K, D) = rightmost 32 bits of C.

AS2805 Appendix O – G: Card Key and Authentication Parameter

The Authentication Parameter (AP or Auth Para) is a 64-bit value constructed by the Card Issuer, or his agent, to confirm the approval of a transaction and, specifically, the amount of the transaction. AP is calculated using the One-way Function (OWF), defined in AS2805 Appendix O – A: One-way Function and various Card and Data Values, defined in AS2805 Appendix O – B: Derivation of Card and Data Values, as follows:

Let

Card Key = OWF(CV3, CV4),

then

Decoupling Key = OWF(CV5, Card Key)

and

AP = OWF(Decoupling Key, DV6).

Important Note:

In the above calculations, CV3, CV5 and Decoupling Key are used as the key inputs to the OWF and CV4, Card Key and DV6 used as the data inputs to the OWF, respectively.

AS2805 Appendix S – APCA Functional Specification Comparison Guide

APCA SCM Function	APCA Command Code	Thales Command Code	
		Base HSM F/W	This Specification
General			
1.1.1 Echo Test	0000	B2	
1.1.2 SCM Status Extended	0002	NO	
1.1.2 Function Status	0005	None	None
1.1.4 KM Status	0006	NC	
1.1.5 Format Status	0007	None	None
1.1.6 Set Clock	0015	Console: SETTIME	None
1.1.7 Get Clock	0016	Console: GETTIME	None
1.1.8 MD5Gen	0020	GM	
1.1.9 SHAGen	0021	GM	
Interchange			
1.2.1 Encipher	2500		PU
1.2.2 Decipher	2600		PW
1.2.3 KEKGEN – 6.3	D501		F6
1.2.4 KEKREC – 6.3	D502		F8
1.2.5 NodeKeyGen - 6.3	3A00		OI
1.2.6 RTMK (Key Translation - Receive)	4500		OK
1.2.7 VISA REC	4501	A6	
1.2.8 KEKGEN –VISA	4502	A0	
1.2.9 VISA-REC-IWK	4503	A6	
1.2.10 VISA-REC-AWK	4504	A6	
1.2.11 Kmmigrate (KM Translation)	4600	BW	
1.2.12 MACGen - 6.3 and 6.4	5500		C2
1.2.13 MACVerify - 6.3 and 6.4	5600		C4
1.2.14 NodeProof	E520		E0
1.2.15 NodeResp	E530		E2
1.2.16 KVC request	7510	BU	
1.2.17 ENCIPHER – OFB	2700		PU
1.2.18 DECRYPTER – OFB	2800		PW
Terminal to node AS 2805.6.4			
2.1 TermKeyGen1-2000	3500		PI & OU
2.2 TermKeyGen2-2000	3510		PI & OW
2.3 TermKeyInit - 6.4-2000	3630		C0
2.4 PINVerify - 6.4-2000	6510		F0
2.5 PINVerify VISA 6.4-2000	6511		F2
2.6 KACalc-2000	B520		C8
2.7 KAExport-2000	B530	FE	
2.8 KAImport-2000	B540	FC	
2.9 VerifyPPID-2000	E540		D2

2.10 TermProof-2000 – 6.4 2000	E500		E4
2.11 HostProof-2000 – 6.4 2000	E510		E6
2.12 KIA Send	B550	A8	
2.13 KIA Receive	B560	A6	
2.14 TKEYGEN	3144	None	None
Terminal to node AS 2805.6.2			
3.1 PINKEYCHANGE	46A0	None	
3.2 ENCIPHER CBC	2511		PU
3.3 DECRYPT CBC	2611		PW
3.4 ENCIPHER ECB	2501		PU
3.5 DECRYPT ECB	2601		PW
3.6 PINBLOCKTRANS 6.2 -> 6.3	6640	None	None
3.7 TERMKEYUPDATE	3710	None	None
3.8 ENCIPHER OFB	25A0		PU
3.9 DECRYPT OFB	26A0		PW
3.10 MAC GENERATE	5510	None	None
3.11 MAC VERIFY	5610		RE
3.12 MAC VERIFY (Completion Confirmation Message)	5620		RQ
3.13 TERMKEYINIT	3640		RW
3.14 APGEN	E600		RU
3.15 MAC GENERATE NDC+	5530	None	None
3.16 MAC VERIFY NDC+	5630	None	None
ATM			
4.1 ABKeyGen-2000	3B00	HC	
4.2 CkeyGen-2000	3B10	HC	
4.3 MkeyGen-2000	3B20	HC	
4.4 ATMKEYGEN	3B30	A0	
Public Key			
5.5 KMMigrate DEA2	4610	EM	
5.6 GetPublic-2000	C500	None	None
5.7 NodeKEKSend-2000	C600		H4
5.8 NodeKEKRec-2000	C610		H6
5.9 GetDEA2Pair	C620		EO & EI
5.10 NodeKEKSend-2000-Export	C700		H4
5.11 NodeKEKRec-2000-Export	C710		H6
5.12 Load Public	C6A0	None	None
5.13 Load Public-NDC+	C6B0	None	None
5.14 SignPublic NDC+	C6C0	None	None
5.15 Verify EPP NDC+	C6D0	None	None
5.16 NodeKEKsend-NDC+	C720	A0, GK & EW	
5.17 Verify Certificate	C800	ES	
5.18 SignPublic PKCS#10	C810		
5.19 Construct Key Token B1	C850	None	None
5.20 Verify Key Token A2	C860	None	None
Retained			
6.1 CHESSKEKGEN – 6.3	D001	F6	F6
6.2 CHESSKEKREC – 6.3	D002	F8	F8
6.3 APGEN (old replaced by 3.14)			

PIN and CARD Functions			
7.1 PINTrans - IBM3624 to 6.3	6680	CA	
7.2 PINTrans - 6.3 to 6.3	6600	CC	
7.4 PVVGen - using given PIN	65B4	DG	
7.5 PINVerify VISA 6.3	6501	DC	
7.6 PINVerify 6.3	6500	EC	
7.7 PPASNVerify	F013		E4
7.8 PPIDEncrypt	F014		D0
7.9 PINTrans - 6.4 to 6.3	6610		PO
7.10 CVVGEN	8500	CW	
7.11 CVVKEYGEN	8600	AS	
7.12 CVVKEYIMPORT	8510	AW	
7.13 CVVVERIFY	8520	CY	
Terminal Remote Initialisation			
8.1 SponsorKeyGen	B510	A0	
8.2 InitialKeyRec	B580		I0
8.3 LoadKCA	B590	A8	
8.4 GetPublicPair -TCU	C630	EI	
8.5 TCUPublicRec	C640		H0
8.6 TermKeyInit - remote	3633		PI & PK & F4
8.7 TermKeyReinit - remote	3634		PI & D0
8.8 RandGen	B570		C6
8.9 TermKeyInit Remote – 6.2	3643		RW & PK & F4
Approved Extensions			
9.1 KTKALC	B510	None	

Notes:

Other commands available in this specification which have no equivalent in the APCA specification but which are required for Thales customers include:

C0, C2, C4, D4, D6, D8, E8, OO, OQ, OU, OY, PM, H8

AS2805 Appendix T – Key Notation comparison table

Australian Standards		Thales	
Code	Meaning	Code	Meaning
A	ATM A Key	TMK1	Terminal Master Key
B	ATM B Key	TMK2	Terminal Master Key
C	Communications Key	C	Communications Key
CATID	Card Acceptor terminal Identification	CATID	Card Acceptor terminal Identification
CVV	Card Verification Value	CVV	Card Verification Value
KCA	Cross Acquirer Key	KCA	Cross Acquirer Key encrypting Key
KCVV	Card Verification Value Keys	CVK	Card Verification Key
KD	Data Key	KD	Privacy Key (Denoted KD)
KEK	Key Encrypting Key	KEK	Key Encrypting Key
KIA	Acquirer Initialization Key	TMK/TEK	Terminal Master/Encryption Key
KM	Domain Master Key	LMK	Local Master Key
KMAC	MAC Key	TAK/ZAK	Terminal/Zone Authentication Key
KMACH	HouseKeeping MAC Key	TAK	Terminal Authentication Key
KMACI	Initial MAC Key	TAK	Terminal Authentication Key
KPE	Pin Encryption Key	TPK	Terminal Pin Key
KPP	Pin Protect Key	TPK / ZPK	Terminal / Zone Pin Key
KPV	Pin Verification Key	PVK	Pin Verification Key
KPVVA	Visa Pin Verification Key A	PVK	Pin Verification Key
KPVVB	Visa Pin Verification Key B	PVK	Pin Verification Key
KT	Terminal Key	KT	Transaction Key
KTK	Key Transport Key	ZMK	Zone Master Key
KVC	Key Verification Code	KCV	Key Check Value
M	ATM M Key (Master)	TMK	Terminal Master Key
PK	Public Keys	PK	Public Key
PPASN	Pin Pad Security Number	PPASN	Pin Pad Acquirer Secret Number
PPID	Pinpad Identification Number	PPID	Pin Pad Identification Number
PVC	Verification Code of Public Key	PVC	Public Key Verification Code
PVV	Pin Verification Value	PVV	Pin Verification Value
SK	Secret Key	SK	Secret Key
STAN	System Trace Audit Number	STAN	System Trace Audit Number
KMA	Acquirer Master Key Encrypting Key	KMA	Acquirer Master Key Encrypting Key
		ZEK	Zone Encryption Key

Note: 1= Variant1, 2=Variant2 e.g TMK1 or TMK2

Note: s=Send r=Receive e.g KEKs or KEKr

AS2805 Appendix U – RSA Public Key Encoding

AS2805 Appendix U1 – DEA 2 Text Block - DFormat 1

The RSA datablock format conforms to the APCA Dformat1 specifications (described in APCA2000 Specification Version 3, § 5.4.4.1).

The clear datablock has the following format:

Byte	Bits	Description
0	7-6	00 = Always less than modulus.
	5-1	00001 = block format 1.
	0	0 = no padding used, 1 = padding used.
1		Normally zero unless an identity transform (concealing) would have occurred.
2		Number n of 8 byte blocks in the modulus of the key enciphering this data.
3-4		Checksum of bytes 5 through 8n-1.
Var (5 to 8n-1)		Up to 8n-5 bytes of data, left justified. If data is less than (8n-5) bytes, append random pad bytes and pad byte count in byte 8n-1. The pad count includes byte 8n-1.

Notes:

1. 8n represents the size of the modulus of the DEA 2 key that enciphers the DFormat 1 textblock.
2. The leftmost byte of a block (byte 0) is the most significant byte and the rightmost byte (e.g. byte 63) is the least significant byte.
3. A short data sequence will be padded to the right with random bits, and a pad count.
4. The checksum is calculated as the 16-bit sum of bytes 4 to 8n-1 with a rotate left of 1 bit to the working total before each byte is added in.
5. The maximum amount of data that can be enciphered is 8n-6 bytes. The actual data block size is 8n-6-[8n-1] (where [x] means "contents of byte x").

Validation of this block includes the following steps:

The length of the data to be validated is equal to the length (in bytes) of the modulus of the key to be used for the validation - if not, return error code 76.

1. Byte 0 of the clear data block is 0x02 or 0x03 - if not, return error code 77.
2. Byte 1 of the clear data block is 0x00 - if not, return error code 77.
3. Byte 2 of the clear data block must be equal to the modulus length in bytes - if not return error code 77.
4. Compute a checksum on the clear data; if not equal to bytes 3-4 of the clear data block return error code 77.

AS2805 Appendix U2 – Public Key Encoding

The HSM supports the following public key encoding types:

Type = 01 (DER encoding for an ASN.1 public key)

An ASN.1 RSAPublicKey has the following definition (see Ref.6):

```
RSAPublicKey ::= SEQUENCE {  
    modulus INTEGER, - - n  
    publicExponent INTEGER - - e }
```

AS2805 Appendix V – Plaintext Data Block Formats

This Appendix describes the Plaintext Data Block Formats used in the H8 and I0 commands.

Format 01:

The Plaintext Data Block is the same length (in bits) as the input KHSK Modulus Length and has the following binary format, with the *rightmost* byte, the least significant byte, labelled byte 0:

Byte 0-19	All 0x'00
Byte n	0x'1D or 0x'1E
Byte n+1 to n+8	Random Number
Byte n+9 to n+13	DTS
Byte n+14 to n+21	PPSN
Byte n+22 to n+37	KTI

Format 02:

The Plaintext Data Block is the same length (in bits) as the input KHSK Modulus Length and has the following binary format, with the *leftmost* byte, the least significant byte, labelled byte 0:

Byte 0-19	All 0x'00
Byte n	0x'1D or 0x'1E
Byte n+1 to n+8	Random Number
Byte n+9 to n+13	DTS
Byte n+14 to n+21	PPSN
Byte n+22 to n+37	KTI

Format 03:

Byte	Value	Comment
0	03	Indicates checksum and padding are present (1 byte)
1	00	Null transform byte (1 byte)
2	...	Variable field specifying the number of 64 bit blocks in the modulus (1byte) (NOTE: It is the total number of bits of this Data Block.)
3..4	...	Checksum of the rest of the data (2 bytes)
5..20	...	KT (16 bytes)
21..28	...	PPID (8 bytes)
29..34	...	DTS (YYMMDDHHmmss) (6 bytes)
35..42	...	RN (8 bytes)
43..(N-1)	...	Padding (any value)
N	(N-42)	Variable field specifying the length of Padding including this byte (1 byte)

Where N = 47 or above AND

$$N = (\text{number of Bytes in Byte 2 of Data Block} - 1) \quad \text{i.e. } [(value \text{ in Byte 2}) / 8] - 1$$

e.g. Format 03 Data Block = 112 Bytes

$$\text{Byte 2} = 0x0E \quad (14 \text{ decimal})$$

$$N = (0x0E) \times 64 / 8 - 1$$

$$= 14 \times 64 / 8 - 1$$

$$= 111$$

Then the last two fields become:

43..110	0x00..0x00
111	(N-42) = (111-42) = 69 = 0x45

e.g. Format 03 Data Block = 184 Bytes

$$\text{Byte 2} = 0x17 \quad (23 \text{ decimal})$$

$$N = (0x17) \times 64 / 8 - 1$$

$$= 23 \times 64 / 8 - 1$$

$$= 183$$

Then the last two fields become:

43..182	0x00..0x00
---------	------------

183	$(N-42) = (183-42) = 141 = 0x8D$
-----	----------------------------------

Format 04:

Byte	Value	Comment
0	03	Indicates checksum and padding are present (1byte)
1	00	Null transform byte (1 byte)
2	..	Variable field specifying the number of 64 bit blocks in the modulus (1byte) (NOTE: It is the total number of bits of this Data Block.)
3..4	Checksum of the rest of the data (2 bytes)
5..20	KT (16 bytes)
21..28	PPID (8 bytes)
29..34	DTS (YYMMDDHHmmss) (6 bytes)
35..42	RN (8 bytes)
43..58	0x00 or private data	Optional user numeric data (16 bytes)
59..(N-1)	Padding (any value)
N	(N-58)	Variable field specifying the length of Padding including this byte (1 byte)

Where N = (Byte 2 of Data Block x 64 / 8) - 1

e.g. Format 04 Data Block = length of 112 Bytes

Byte 2 = 0x0E (14 decimal)

$$N = (0x0E \times 64 / 8) - 1$$

$$= (14 \times 64 / 8) - 1$$

$$= 111$$

Then the last two fields become:

59..110	00..00
111	$(N-58) = (111-58) = 53 = 0x35$

e.g. Format 04 Data Block = length of 184 Bytes

Byte 2 = 0x17 (23 decimal)

$$N = (0x17 \times 64 / 8) - 1$$

$$= (23 \times 64 / 8) - 1$$

= 183

Then the last two fields become:

59..182	00..00
183	$(N-58) = (183-58) = 125 = 0x7D$



Contact us

For all office locations and contact
information, please visit
cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <

