THALES

payShield 9000 v2.3b

Host Command Reference Manual

www.thales-esecurity.com

>> Revision Status

Document No.	Manual Set	Software Version	Release Date
1270A546-016	Issue 16	payShield 9000 v2.3b	August 2014

>> References

The following documents are referenced in this document:

1	payShield 9000 Installation Manual Document Number: 1270A543
2	PKCS#1: RSA Encryption Standard - Version 1.5 – Revised November 1993 (www.rsalabs.com)
3	PKCS#1: RSA Cryptography Standard – Version 2.0 – October 1998 (www.rsalabs.com)
4	Visa Integrated Circuit Card Specification, Version 1.4.0 – April 2001, plus August 2002 Corrections
5	MasterCard M/Chip 4 Cryptography and Key Management v4.0 – May 2002
7	EMV Integrated Circuit Card Specification for Payment Systems Book 2 – Security and Key Management Version 4.3 November 2011
9	EMV Specification Update Bulletin No. 46 First Edition October 2005

>> List of Chapters

>> Chapter 1 – Introduction 1

>> Chapter 2 – Host Commands 17

>> Chapter 3 – PIN Block Formats 486

>> Chapter 4 – Error Codes 487

>> Table of Contents

>> Revision Status ii

>> References iii

>> List of Chapters iv

>> Table of Contents v

>> End User License Agreement vii

>> Notices ix

>> Chapter 1 – Introduction 1

Local Master Keys (LMKs) 1
Multiple LMKs 1
LMK Usage in Host Commands 2
Key Scheme Table 2
Host Command Set 3
List of Host Commands (Alphabetical) 4
List of Host Commands (Functional) 10

>> Chapter 2 – Host Commands 17

General 17
Symmetric Key Management Commands 18
PIN and Offset Generation Commands 59
PIN Change Commands 84
PIN Verification Commands 93
PIN Translation Commands 112
PIN Mailer Printing Commands 127
PIN Solicitation Data Processing Commands 136
Clear PIN Commands 141
Watchword Commands 144
Message Authentication Code Commands 151
Message Encryption Commands 162
BDKs used with Message Encryption Commands 163
HMAC Commands 176
User Storage Commands 194
Print Output Formatting Commands 200
LMK Translation Commands 204
Miscellaneous Commands 212
Diagnostic Commands 227
Auditing Commands 245
Card Verification Code/Value Commands 251
EMV Chip Card Commands 267

Racal Transaction Key Scheme (RTKS) Commands 292
Derived Unique Key Per Transaction (X9.24-1) Commands 319
RSA Cryptosystem Commands 339
VISA Cash Commands 375
Legacy Commands 385

>> Chapter 3 – PIN Block Formats 486
General 486

>> Chapter 4 – Error Codes 487
General 487

>> Appendix A – EBCDIC to ASCII Table 490

>> Appendix B – Internal Auditing 491
General 491
Audit Record Format 491
Command Code Types 492
Command Code Type 00 – Host Command 492
Command Code Type 01 – Console Command 492
Command Code Type 10 – Fraud Event 493
Command Code Type 11 – User Action 493

>> Appendix C – Fraud Detection 495

>> Appendix D – Key Usage Table 496

>> Appendix E – Mode of Use Table 497

>> Appendix F – Key Usage Conversion Table 498

>> Appendix G – Example Host Commands and Sample Code 499

>> End User License Agreement

("EULA")

Please read this Agreement carefully.

Opening this package or installing any of the contents of this package or using this product in any way indicates your acceptance of the terms and conditions of this License.

This document is a legal agreement between Thales UK Ltd., ("THALES") and the company that has purchased a THALES product containing a computer program ("Customer"). If you do not agree to the terms of this Agreement, promptly return the product and all accompanying items (including cables, written materials, software disks, etc.) at your mailing or delivery expense to the company from whom you purchased it or to Thales e-Security, Meadow View House, Crendon Industrial Estate, Long Crendon, Aylesbury, Bucks HP18 9EQ, United Kingdom and you will receive a refund.

1. **OWNERSHIP.** Computer programs, ("Software") provided by THALES are provided either separately or as a bundled part of a computer hardware product. Software shall also be deemed to include computer programs which are intended to be run solely on or within a hardware machine, ("Firmware").Software, including any documentation files accompanying the Software, ("Documentation") distributed pursuant to this license consists of components that are owned or licensed by THALES or its corporate affiliates. Other components of the Software consist of free software components ("Free Software Components") that are identified in the text files that are provided with the Software. ONLY THOSE TERMS AND CONDITIONS SPECIFIED FOR, OR APPLICABLE TO, EACH SPECIFIC FREE SOFTWARE COMPONENT SHALL BE APPLICABLE TO SUCH FREE SOFTWARE COMPONENT. Each Free Software Component is the copyright of its respective copyright owner. The Software is licensed to Customer and not sold. Customer has no ownership rights in the Software. Rather, Customer has a license to use the Software. The Software is copyrighted by THALES and/or its suppliers. You agree to respect and not to remove or conceal from view any copyright or trademark notice appearing on the Software or Documentation, and to reproduce any such copyright or trademark notice on all copies of the Software and Documentation or any portion thereof made by you as permitted hereunder and on all portions contained in or merged into other programs and Documentation.

2. **LICENSE GRANT.** THALES grants Customer a non-exclusive license to use the Software with THALES provided computer equipment hardware solely for Customer's internal business use only. This license only applies to the version of Software shipped at the time of purchase. Any future upgrades are only authorised pursuant to a separate maintenance agreement. Customer may copy the Documentation for internal use. Customer may not decompile, disassemble, reverse engineer, copy, or modify the THALES owned or licensed components of the Software unless such copies are made in machine readable form for backup purposes. In addition, Customer may not create derivative works based on the Software except as may be necessary to permit integration with other technology and Customer shall not permit any other person to do any of the same. Any rights not expressly granted by THALES to Customer are reserved by THALES and its licensors and all implied licenses are disclaimed. Any other use of the Software by any other entity is strictly forbidden and is a violation of this EULA. The Software and any accompanying written materials are protected by international copyright and patent laws and international trade provisions.

3. **NO WARRANTY.** Except as may be provided in any separate written agreement between Customer and THALES, the software is provided "as is." To the maximum extent permitted by law, THALES disclaims all warranties of any kind, either expressed or implied, including, without limitation, implied warranties of merchantability and fitness for a particular purpose. THALES does not warrant that the functions contained in the software will meet any requirements or needs Customer may have, or that the software will operate error free, or in an uninterrupted fashion, or that any defects or errors in the software will be corrected, or that the software is compatible with any particular platform. Some jurisdictions do not allow for the waiver or exclusion of implied warranties so they may not apply. If this exclusion is held to be unenforceable by a court of competent jurisdiction, then all express and implied warranties shall be limited in duration to a period of thirty (30) days from the date of purchase of the software, and no warranties shall apply after that period.

4. **LIMITATION OF LIABILITY.** In no event will THALES be liable to Customer or any third party for any incidental or consequential damages, including without limitation, indirect, special, punitive, or exemplary damages for loss of business, loss of profits, business interruption, or loss of business information) arising out of the use of or inability to use the program, or for any claim by any other party, even if THALES has been advised of the possibility of such damages. THALES' aggregate liability with respect to its obligations under this agreement or otherwise with respect to the software and documentation or otherwise shall be equal to the purchase price. However nothing in these terms and conditions shall however limit or exclude THALES' liability for death or personal injury resulting

from negligence, fraud or fraudulent misrepresentation or for any other liability which may not be excluded by law. Because some countries and states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply.

5. **EXPORT RESTRICTIONS.** The software is subject to the export control laws of the United Kingdom, the United States and other countries. This license agreement is expressly made subject to all applicable laws, regulations, orders, or other restrictions on the export of the software or information about such software which may be imposed from time to time. Customer shall not export the software, documentation or information about the software and documentation without complying with such laws, regulations, orders, or other restrictions.

6. **TERM & TERMINATION.** This EULA is effective until terminated. Customer may terminate this EULA at any time by destroying or erasing all copies of the Software and accompanying written materials in Customer's possession or control. This license will terminate automatically, without notice from THALES if Customer fails to comply with the terms and conditions of this EULA. Upon such termination, Customer shall destroy or erase all copies of the Software (together with all modifications, upgrades and merged portions in any form) and any accompanying written materials in Customer's possession or control.

7. **SPECIAL PROCEDURE FOR U.S. GOVERNMENT.** If the Software and Documentation is acquired by the U.S. Government or on its behalf, the Software is furnished with "RESTRICTED RIGHTS," as defined in Federal Acquisition Regulation ("FAR") 52.227-19(c)(2), and DFAR 252.227-7013 to 7019, as applicable. Use, duplication or disclosure of the Software and Documentation by the U.S. Government and parties acting on its behalf is governed by and subject to the restrictions set forth in FAR 52.227-19(c)(1) and (2) or DFAR 252.227-7013 to 7019, as applicable.

8. **TRANSFER RIGHTS.** Customer may transfer the Software, and this license to another party if the other party agrees to accept the terms and conditions of this Agreement. If Customer transfers the Software, it must at the same time either transfer all copies whether in printed or machine-readable form, together with the computer hardware machine on which Software was intended to operate to the same party or destroy any copies not transferred; this includes all derivative works of the Software. FOR THE AVOIDANCE OF DOUBT, IF CUSTOMER TRANSFERS POSSESSION OF ANY COPY OF THE SOFTWARE TO ANOTHER PARTY, EXCEPT AS PROVIDED IN THIS SECTION 8, CUSTOMER'S LICENSE IS AUTOMATICALLY TERMINATED.

9. **GOVERNING LAW AND VENUE.** This License Agreement shall be construed, interpreted and governed either by the laws of England and Wales or by the laws of the State of New York, United States of America, in both cases without regard to conflicts of laws and provisions thereof. If the Software is located or being used in a country located in North America, South America, Central America or the Caribbean region, the laws of the State of the State of New York, United States of America shall apply and the exclusive forum for any disputes arising out of or relating to the EULA, including the determination of the scope or applicability of this EULA to arbitrate, shall be shall be settled by arbitration in accordance with the Arbitration Rules of the International Chamber of Commerce ("ICC") by one arbitrator appointed in accordance with said Rules. The arbitration shall be administered by the ICC. The arbitration shall be held in New York City (State of New York), and shall be conducted in the English language. Either Party may seek interim or provisional relief in any court of competent jurisdiction if necessary to protect the rights or property of that party pending the appointment of the arbitrator or pending the arbitrator's determination of the merits of the dispute. The arbitration award will be in writing and will specify the factual and legal basis for the award. The arbitration award will be final and binding upon the parties, and any judgment on the award rendered by the arbitrator may be entered by any court having jurisdiction thereof. If the Software is located or being used in any other location throughout the world, then in that event the laws of England and Wales shall apply and the exclusive forum for any disputes arising out of or relating to this EULA shall be an appropriate court sitting in England, United Kingdom.

>> Notices

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

>> Chapter 1 – Introduction

Local Master Keys (LMKs)

For an introduction to LMKs (Local Master Keys) and information about LMKs, see Chapters 3-5 of the payShield 9000 General Information Manual. See also Chapter 10 of the payShield 9000 General information manual about changes made to key types for PCI HSM certification.

Multiple LMKs

It is possible to install multiple LMKs within a single payShield 9000. The precise details of the number and type of installed LMKs are controlled via the payShield 9000's license file:

License	Description
HSM9-LIC001 (standard license)	Two concurrent LMKs can be installed; however, one must be a Variant LMK, and the other a Keyblock LMK.
HSM9-LIC012 LMK x 2 (optional license)	Two concurrent LMKs can be installed; they can be any combination of Variant and Keyblock LMKs.
HSM9-LIC013 LMK x 5 (optional license)	Five concurrent LMKs can be installed; they can be any combination of Variant and Keyblock LMKs.
HSM9-LIC021 LMK x 10 (optional license)	Ten concurrent LMKs can be installed; they can be any combination of Variant and Keyblock LMKs.

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

Two additional (optional) fields will be added at the end of the each host command request message. These fields will be:

Field	Length & Type	Details
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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
…	…

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 keyblock 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.

Key Scheme Table

The Key Scheme Table can be found at Appendix C of the payShield 9000 General Information Manual.

Host Command Set

The payShield 9000 HSM provides a variety of functions to implement key management, PIN management (including PIN verification) and Message Authentication Code (MAC) processing.

The individual commands are described in Chapter 2. They are divided into the following groupings:

- Symmetric Key Management Commands
- PIN and Offset Generation Commands
- PIN Change Commands
- PIN Verification Commands
- PIN Translation Commands
- PIN Mailer Printing Commands
- PIN Solicitation Data Processing Commands
- Clear PIN Commands
- Watchword Commands
- Message Authentication Code Commands
- Message Encryption Commands
- HMAC Commands
- User Storage Commands
- Print Output Formatting
- LMK Translation Commands
- Miscellaneous Commands
- Auditing Commands
- Card Verification Code/Value Commands
- EMV Chip Card Commands
- Racal Transaction Key Scheme (RTKS) Commands
- Derived Unique Key Per Transaction (X9.24-1) Commands
- RSA Cryptosystem Commands
- VISA Cash Commands
- Legacy Commands

List of Host Commands (Alphabetical)

Host Command (Response)	Function	Page
A0 (A1)	Generate a Key	20
A2 (A3, AZ)	Generate and Print a Component	27
A4 (A5)	Form a Key from Encrypted Components	34
A6 (A7)	Import a Key	37
A8 (A9)	Export a Key	42
AA (AB) *	Translate a TMK, TPK or PVK	413
AC (AD)	Translate a TAK	419
AE (AF) *	Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK	55
AG (AH)	Translate a TAK from LMK to TMK Encryption	57
AS (AT)	Generate a CVK Pair	388
AU (AV)	Translate a CVK Pair from LMK to ZMK Encryption	409
AW (AX)	Translate a CVK Pair from ZMK to LMK Encryption	411
AY (AZ)	Translate a CVK Pair from Old LMK to New LMK Encryption	407
B0 (B1)	Translate Key Scheme	47
B2 (B3)	Echo Command	213
BA (BB)	Encrypt a Clear PIN	142
BC (BD)	Verify a Terminal PIN Using the Comparison Method	108
BE (BF)	Verify an Interchange PIN Using the Comparison Method	110
BG (BH)	Translate a PIN and PIN Length	205
BI (BJ)	Generate a BDK	449
BK (BL)	Generate an IBM PIN Offset (of a customer selected PIN)	71
BM (BN)	Load the Excluded PIN Table	82
BQ (BR)	Translate PIN Algorithm	124
BS (BT)	Erase the Key Change Storage	211
BU (BV)	Generate a Key Check Value	216
BW (BX)	Translate Keys from Old LMK to New LMK	207
BY (BZ)	Translate ZMK from ZMK to LMK encryption	48
CA (CB)	Translate a PIN from TPK to ZPK/BDK (3-DES DUKPT) Encryption	115
CC (CD)	Translate a PIN from One ZPK to Another	113
CE (CF)	Generate a Diebold PIN Offset	75
CG (CH)	Verify a Terminal PIN Using the Diebold Method	100
CI (CJ)	Translate a PIN from BDK to ZPK Encryption (DUKPT)	474
CK (CL)	Verify a PIN Using the IBM Method (DUKPT)	476
CM (CN)	Verify a PIN Using the VISA PVV Method (DUKPT)	480
CO (CP)	Verify a PIN Using the Diebold Method (DUKPT)	482
CQ (CR)	Verify a PIN Using the Encrypted PIN Method (DUKPT)	484
CS (CT)	Modify Keyblock Header	224
CU (CV)	Verify & Generate a VISA PVV (of a customer selected PIN)	90

Host Command (Response)	Function	Page
CW (CX)	Generate a Card Verification Code/Value	252
CY (CZ)	Verify a Card Verification Code/Value	254
DA (DB)	Verify a Terminal PIN Using the IBM Method	94
DC (DD)	Verify a Terminal PIN Using the VISA Method	104
DE (DF)	Generate an IBM PIN Offset (of an LMK encrypted PIN)	67
DG (DH)	Generate a VISA PIN Verification Value (of an LMK encrypted PIN)	77
DI (DJ)	Generate and Export a KML	454
DK (DL)	Import a KML	456
DM (DN)	Verify Load Signature S1 and Generate Load Signature S2	377
DO (DP)	Verify Load Completion Signature S3	379
DQ (DR)	Verify Unload Signature S1 and Generate Unload Signature S2	381
DS (DT)	Verify Unload Completion Signature S3	383
DU (DV)	Verify & Generate an IBM PIN Offset (of customer selected new PIN)	85
DW (DX)	Translate a BDK from ZMK to LMK Encryption	450
DY (DZ)	Translate a BDK from LMK to ZMK Encryption	452
EA (EB)	Verify an Interchange PIN Using the IBM Method	97
EC (ED)	Verify an Interchange PIN Using the VISA Method	106
EE (EF)	Derive a PIN Using the IBM Method	60
EG (EH)	Verify an Interchange PIN Using the Diebold Method	102
EI (EJ)	Generate a Public/Private Key Pair	340
EK (EL)	Load a Private Key	343
EM (EN)	Translate a Private Key	345
EO (EP)	Import a Public Key	347
EQ (ER)	Validate a Public Key	350
ES (ET)	Validate a Certificate and Import the Public Key	352
EU (EV)	Translate a Public Key	355
EW (EX)	Generate an RSA Signature	357
EY (EZ)	Validate an RSA Signature	359
FA (FB)	Translate a ZPK from ZMK to LMK Encryption	437
FC (FD) *	Translate a TMK, TPK or PVK from ZMK to LMK Encryption	417
FE (FF) *	Translate a TMK, TPK or PVK from LMK to ZMK Encryption	415
FG (FH) *	Generate a Pair of PVKs	392
FI (FJ)	Generate ZEK/ZAK	397
FK (FL)	Translate a ZEK/ZAK from ZMK to LMK Encryption	431
FM (FN)	Translate a ZEK/ZAK from LMK to ZMK Encryption	429
FO (FP)	Generate a Watchword Key	395
FQ (FR)	Translate a Watchword Key from LMK to ZMK Encryption	425
FS (FT)	Translate a Watchword Key from ZMK to LMK Encryption	427
FU (FV)	Verify a Watchword Response	145
FW (FX)	Generate a VISA PIN Verification Value (of a customer selected PIN)	79

Host Command (Response)	Function	Page
GO (G1)	Translate a PIN from BDK to BDK or ZPK Encryption (3-DES DUKPT)	321
GA (GB)	Derive a PIN Using the Diebold Method	63
GC (GD)	Translate a ZPK from LMK to ZMK Encryption	435
GE (GF)	Translate a ZMK	439
GG (GH)	Form a ZMK from Three ZMK Components	401
GI (GJ)	Import Key or data under an RSA Public Key	361
GK (GL)	Export Key under an RSA Public Key	369
GM (GN)	Hash a Block of Data	374
GO (GP)	Verify a PIN Using the IBM Method (3-DES DUKPT)	324
GQ (GR)	Verify a PIN Using the VISA PVV Method (3-DES DUKPT)	328
GS (GT)	Verify a PIN Using the Diebold Method (3-DES DUKPT)	331
GU (GV)	Verify a PIN Using the Encrypted PIN Method (3-DES DUKPT)	334
GW (GX)	Generate/Verify a MAC (3-DES DUKPT)	337
GY (GZ)	Form a ZMK from 2 to 9 ZMK Components	403
HA (HB)	Generate a TAK	53
HC (HD) *	Generate a TMK, TPK or PVK	51
HI (HJ)	Transaction Request With a PIN (T/AQ Key) *(when selected Transaction Key Scheme is Australian)* [*NOTE: See also RI*]	297
HK (HL)	Transaction Request With a PIN (T/AQ Key) *(when selected Transaction Key Scheme is Australian)* [*NOTE: See also RK*]	297
HM (HN)	Administration Request Message *(when selected Transaction Key Scheme is Australian)* [*NOTE: See also RM*]	309
HO (HP)	Transaction Response with Auth Para from Card Issuer (*when selected Transaction Key Scheme is Australian*) [*NOTE: See also RO*]	312
HQ (HR)	Generate Auth Para and Transaction Response *(when selected Transaction Key Scheme is Australian)* [*NOTE: See also RQ*]	315
HS (HT)	Confirmation *(when selected Transaction Key Scheme is Australian)* [*NOTE: See also RS*]	318
HU (HV)	Transaction Request With a PIN (T/CI Key) *(when selected Transaction Key Scheme is Australian)* [*NOTE: See also RU*]	303
HW (HX)	Translate KEYVAL *(when selected Transaction Key Scheme is Australian)* [*NOTE: See also RW*]	306
IA (IB)	Generate a ZPK	399
J2 (J3)	Get HSM Loading	234
J4 (J5)	Get Host Command Volumes	236
J6 (J7)	Reset Utilization Statistics	238
J8 (J9)	Get Health Check Accumulated Counts	239
JA (JB)	Generate a Random PIN	65
JC (JD)	Translate a PIN from TPK to LMK Encryption	120
JE (JF)	Translate a PIN from ZPK to LMK Encryption	118
JG (JH)	Translate a PIN from LMK to ZPK Encryption	122
JI (JJ)	Reset Health Check Accumulated Counts	241

Host Command (Response)	Function	Page
JK (JL)	Get Instantaneous Health Check Status	242
KO (K1)	Decrypt Encrypted Counters (EMV 4.x)	286
K2 (K3)	Verify Truncated Application Cryptogram (MasterCard CAP)	289
KA (KB) *	Generate a Key Check Value (Not Double-Length ZMK)	441
KC (KD)	Translate a ZPK	433
KQ (KR)	ARQC Verification and/or ARPC Generation (EMV 3.1.1)	268
KS (KT)	Data Authentication Code and Dynamic Number Verification (EMV 3.1.1)	271
KU (KV)	Generate Secure Message (EMV 3.1.1)	273
KW (KX)	ARQC Verification and/or ARPC Generation (EMV 4.x)	283
KY (KZ)	Generate Secure Message (EMV 4.x)	277
LO (L1)	Generate an HMAC Secret Key	177
LA (LB)	Load Data to User Storage	195
LC (LD)	Verify the Diebold Table in User Storage	199
LE (LF)	Read Data from User Storage	197
LG (LH)	Set HSM Response Delay	219
LI (LJ)	Load a PIN Text String	203
LK (LL)	Generate a Decimal MAC	147
LM (LN)	Verify a Decimal MAC	149
LO (LP)	Translate Decimalization Table from Old to New LMK	220
LQ (LR)	Generate an HMAC on a Block of Data	180
LS (LT)	Verify an HMAC on a Block of Data	182
LU (LV)	Import an HMAC key under a ZMK	184
LW (LX)	Export an HMAC key under a ZMK	188
LY (LZ)	Translate a HMAC Key from Old LMK to New LMK	191
MO (M1)	Encrypt Data Block	164
M2 (M3)	Decrypt Data Block	168
M4 (M5)	Translate Data Block	172
M6 (M7)	Generate MAC	152
M8 (M9)	Verify MAC	155
MA (MB)	Generate a MAC	458
MC (MD)	Verify a MAC	460
ME (MF)	Verify and Translate a MAC	462
MG (MH)	Translate a TAK from LMK to ZMK Encryption	421
MI (MJ)	Translate a TAK from ZMK to LMK Encryption	423
MK (ML)	Generate a Binary MAC	468
MM (MN)	Verify a Binary MAC	470
MO (MP)	Verify and Translate a Binary MAC	472
MQ (MR)	Generate MAC (MAB) for Large Message	464
MS (MT)	Generate MAC (MAB) using ANSI X9.19 Method for a Large Message	466
MY (MZ)	Verify and Translate MAC	158

Host Command (Response)	Function	Page
N0 (N1)	Generate a Random Value	226
NC (ND)	Perform Diagnostics	228
NE (NF, NZ)	Generate and Print a Key as Split Components	31
NG (NH)	Decrypt an Encrypted PIN	143
NI (NJ)	Return Network Information	231
NK (NL)	Command Chaining	221
NO (NP)	HSM Status	229
OA (OB, OZ)	Print a PIN Solicitation Mailer	130
OC (OD, OZ)	Generate and Print a ZMK Component	405
OE (OF, OZ) *	Generate and Print a TMK, TPK or PVK	390
PA (PB)	Load Formatting Data to HSM	201
PC (PD)	Load Additional Formatting Data to HSM	202
PE (PF, PZ)	Print PIN/PIN and Solicitation Data	128
PG (PH)	Verify PIN/PIN and Solicitation Mailer Cryptography	132
PM (PN)	Verify a Dynamic CVV/CVC	on page 258
Q0 (Q1)	Translate Audit Record MAC key	246
Q2 (Q3)	Retrieve Audit Record	247
Q4 (Q5)	Archive (Print) Audit Record	248
Q6 (Q7)	Delete Audit Record	249
Q8 (Q9)	Audit Record Verification	250
QA (QB)	Load Solicitation Data to User Storage	137
QC (QD)	Final Load of Solicitation Data to User Storage	139
QK (QL)	Translate Account Number for LMK-encrypted PIN	125
QY (QZ)	Generate a Dynamic CVV	256
RA (RB)	Cancel Authorized Activities	214
RC (RD)	Verify Solicitation Mailer Cryptography	133
RI (RJ)	Transaction Request With a PIN (T/AQ Key) (*when selected Transaction Key Scheme is Racal*) [*NOTE: See also HI*]	294
RK (RL)	Transaction Request Without a PIN (*when selected Transaction Key Scheme is Racal*) [*NOTE: See also HK*]	298
RM (RN)	Administration Request Message *(when selected Transaction Key Scheme is Racal)* [*NOTE: See also HM*]	307
RO (RP)	Transaction Response with Auth Para from Card Issuer *(when selected Transaction Key Scheme is Racal)* [*NOTE: See also HO*]	310
RQ (RR)	Generate Auth Para and Transaction Response *(when selected Transaction Key Scheme is Racal)* [*NOTE: See also HQ*]	313
RS (RT)	Confirmation *(when selected Transaction Key Scheme is Racal)* [*NOTE: See also HS*]	316
RU (RV)	Transaction Request With a PIN (T/CI Key) *(when selected Transaction Key Scheme is Racal)* [*NOTE: See also HU*]	301
RW (RX)	Translate KEYVAL *(when selected Transaction Key Scheme is Racal)* [*NOTE:*	304

Host Command (Response)	Function	Page
	See also HW]	
RY (RZ)	Calculate Card Security Codes	263
RY (RZ)	Verify Card Security Codes	265
RY (RZ)	Generate a CSCK	443
RY (RZ)	Export a CSCK	445
RY (RZ)	Import a CSCK	447
TA (TB, TZ)	Print TMK Mailer	134

* These commands are disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value of "Y". They should be replaced with newer Host commands as follows:

Host Command		Replaced by	
AA	Translate a TMK, TPK or PVK	BW	Translate Keys from Old LMK to New LMK
AE	Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK	A8	Export a Key
FC	Translate a TMK, TPK or PVK from ZMK to LMK Encryption	A6	Import a Key
FE	Translate a TMK, TPK or PVK from LMK to ZMK Encryption	A8	Export a Key
FG	Generate a pair of PVKs	A0	Generate a Key
HC	Generate a TMK, TPK or PVK	A0	Generate a Key
KA	Generate a Key Check Value (Not Double-Length ZMK)	BU	Generate a Key Check Value
OE	Generate and Print a TMK, TPK or PVK	NE	Generate and Print a Key as Split Components

List of Host Commands (Functional)

Function	Command	Page
Symmetric Key Management Commands		
Generate a Key	A0 (A1)	20
Generate and Print a Component	A2 (A3, AZ)	27
Generate and Print a Key as Split Components	NE (NF, NZ)	31
Form a Key from Encrypted Components	A4 (A5)	34
Import a Key	A6 (A7)	37
Export a Key	A8 (A9)	42
Translate Key Scheme	B0 (B1)	47
Translate ZMK from ZMK to LMK encryption	BY (BZ)	48
Generate a TMK, TPK or PVK	HC (HD) *	51
Generate a TAK	HA (HB)	53
Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK	AE (AF) *	55
Translate a TAK from LMK to TMK Encryption	AG (AH)	57
PIN and Offset Generation Commands		
Derive a PIN Using the IBM Method	EE (EF)	60
Derive a PIN Using the Diebold Method	GA (GB)	63
Generate a Random PIN	JA (JB)	65
Generate an IBM PIN Offset (of an LMK encrypted PIN)	DE (DF)	67
Generate an IBM PIN Offset (of a customer selected PIN)	BK (BL)	71
Generate a Diebold PIN Offset	CE (CF)	75
Generate a VISA PIN Verification Value (of an LMK encrypted PIN)	DG (DH)	77
Generate a VISA PIN Verification Value (of a customer selected PIN)	FW (FX)	79
Load the Excluded PIN Table	BM (BN)	82
PIN Change Commands		
Verify & Generate an IBM PIN Offset (of customer selected new PIN)	DU (DV)	85
Verify & Generate a VISA PVV (of a customer selected PIN)	CU (CV)	90
PIN Verification Commands		
Verify a Terminal PIN Using the IBM Method	DA (DB)	94
Verify an Interchange PIN Using the IBM Method	EA (EB)	97
Verify a Terminal PIN Using the Diebold Method	CG (CH)	100
Verify an Interchange PIN Using the Diebold Method	EG (EH)	102
Verify a Terminal PIN Using the VISA Method	DC (DD)	104
Verify an Interchange PIN Using the VISA Method	EC (ED)	106
Verify a Terminal PIN Using the Comparison Method	BC (BD)	108
Verify an Interchange PIN Using the Comparison Method	BE (BF)	110

Function	Command	Page
PIN Translation Commands		
Translate a PIN from One ZPK to Another	CC (CD)	113
Translate a PIN from TPK to ZPK/BDK (3-DES DUKPT) Encryption	CA (CB)	115
Translate a PIN from ZPK to LMK Encryption	JE (JF)	118
Translate a PIN from TPK to LMK Encryption	JC (JD)	120
Translate a PIN from LMK to ZPK Encryption	JG (JH)	122
Translate PIN Algorithm	BQ (BR)	124
Translate Account Number for LMK-encrypted PIN	QK (QL)	125
Translate a PIN from BDK to BDK or ZPK Encryption (3-DES DUKPT)	GO (G1)	321
PIN Mailer Printing Commands		
Print PIN/PIN and Solicitation Data	PE (PF, PZ)	128
Print a PIN Solicitation Mailer	OA (OB, OZ)	130
Verify PIN/PIN and Solicitation Mailer Cryptography	PG (PH)	132
Verify Solicitation Mailer Cryptography	RC (RD)	133
Print TMK Mailer	TA (TB, TZ)	134
PIN Solicitation Data Processing Commands		
Load Solicitation Data to User Storage	QA (QB)	137
Final Load of Solicitation Data to User Storage	QC (QD)	139
Clear PIN Commands		
Encrypt a Clear PIN	BA (BB)	142
Decrypt an Encrypted PIN	NG (NH)	143
Watchword Commands		
Verify a Watchword Response	FU (FV)	145
Generate a Decimal MAC	LK (LL)	147
Verify a Decimal MAC	LM (LN)	149
Message Authentication Code Commands		
Generate MAC	M6 (M7)	152
Verify MAC	M8 (M9)	155
Verify and Translate MAC	MY (MZ)	158
Message Encryption Commands		
Encrypt Data Block	M0 (M1)	164
Decrypt Data Block	M2 (M3)	168
Translate Data Block	M4 (M5)	172
HMAC Commands		

Function	Command	Page
Generate an HMAC Secret Key	LO (L1)	177
Generate an HMAC on a Block of Data	LQ (LR)	180
Verify an HMAC on a Block of Data	LS (LT)	182
Import an HMAC key under a ZMK	LU (LV)	184
Export an HMAC key under a ZMK	LW (LX)	188
Translate a HMAC Key from Old LMK to New LMK	LY (LZ)	191
User Storage Commands		
Load Data to User Storage	LA (LB)	195
Read Data from User Storage	LE (LF)	197
Verify the Diebold Table in User Storage	LC (LD)	199
Print Output Formatting Commands		
Load Formatting Data to HSM	PA (PB)	201
Load Additional Formatting Data to HSM	PC (PD)	202
Load a PIN Text String	LI (LJ)	203
LMK Translation Commands		
Translate a PIN and PIN Length	BG (BH)	205
Translate Keys from Old LMK to New LMK	BW (BX)	207
Erase the Key Change Storage	BS (BT)	211
Miscellaneous Commands		
Echo Command	B2 (B3)	213
Cancel Authorized Activities	RA (RB)	214
Generate a Key Check Value	BU (BV)	216
Set HSM Response Delay	LG (LH)	219
Translate Decimalization Table from Old to New LMK	LO (LP)	220
Command Chaining	NK (NL)	221
Modify Keyblock Header	CS (CT)	224
Generate a Random Value	N0 (N1)	226
Diagnostic Commands		
Perform Diagnostics	NC (ND)	228
HSM Status	NO (NP)	229
Return Network Information	NI (NJ)	231
Get HSM Loading	J2 (J3)	234
Get Host Command Volumes	J4 (J5)	236
Reset Utilization Statistics	J6 (J7)	238
Get Health Check Accumulated Counts	J8 (J9)	239
Reset Health Check Accumulated Counts	JI (JJ))	241

Function	Command	Page
Get Instantaneous Health Check Status	JK (JL)	242
Auditing Commands		
Translate Audit Record MAC key	Q0 (Q1)	246
Retrieve Audit Record	Q2 (Q3)	247
Archive (Print) Audit Record	Q4 (Q5)	248
Delete Audit Record	Q6 (Q7)	249
Audit Record Verification	Q8 (Q9)	250
Card Verification Code/Value Commands		
Generate a Card Verification Code/Value	CW (CX)	252
Verify a Card Verification Code/Value	CY (CZ)	254
Generate a Dynamic CVV	QY (QZ)	256
Verify a Dynamic CVV/CVC	PM (PN)	258
Calculate Card Security Codes	RY (RZ)	263
Verify Card Security Codes	RY (RZ)	265
EMV Chip Card Commands		
ARQC Verification and/or ARPC Generation (EMV 3.1.1)	KQ (KR)	268
Data Authentication Code and Dynamic Number Verification (EMV 3.1.1)	KS (KT)	271
Generate Secure Message (EMV 3.1.1)	KU (KV)	273
Generate Secure Message (EMV 4.x)	KY (KZ)	277
ARQC Verification and/or ARPC Generation (EMV 4.x)	KW (KX)	283
Decrypt Encrypted Counters (EMV 4.x)	K0 (K1)	286
Verify Truncated Application Cryptogram (MasterCard CAP)	K2 (K3)	289
Racal Transaction Key Scheme (RTKS) Commands		
Transaction Request With a PIN (T/AQ Key) (*when selected Transaction Key Scheme is Racal*)	RI (RJ)	294
Transaction Request With a PIN (T/AQ Key) *(when selected Transaction Key Scheme is Australian)*	HI (HJ)	297
Transaction Request Without a PIN (*when selected Transaction Key Scheme is Racal*)	RK (RL)	298
Transaction Request Without a PIN (*when selected Transaction Key Scheme is Australian*)	HK (HL)	300
Transaction Request With a PIN (T/CI Key) *(when selected Transaction Key Scheme is Racal)*	RU (RV)	301
Transaction Request With a PIN (T/CI Key) *(when selected Transaction Key Scheme is Australian)*	HU (HV)	303
Translate KEYVAL *(when selected Transaction Key Scheme is Racal)*	RW (RX)	304
Translate KEYVAL *(when selected Transaction Key Scheme is Australian)*	HW (HX)	306
Administration Request Message *(when selected Transaction Key*	RM (RN)	307

Function	Command	Page
Scheme is Racal)		
Administration Request Message *(when selected Transaction Key Scheme is Australian)*	HM (HN)	309
Transaction Response with Auth Para from Card Issuer *(when selected Transaction Key Scheme is Racal)*	RO (RP)	310
Transaction Response with Auth Para from Card Issuer (*when selected Transaction Key Scheme is Australian*)	HO (HP)	312
Generate Auth Para and Transaction Response *(when selected Transaction Key Scheme is Racal)*	RQ (RR)	313
Generate Auth Para and Transaction Response *(when selected Transaction Key Scheme is Australian)*	HQ (HR)	315
Confirmation *(when selected Transaction Key Scheme is Racal)*	RS (RT)	316
Confirmation *(when selected Transaction Key Scheme is Australian)*	HS (HT)	318
Derived Unique Key Per Transaction (X9.24-1) Commands		
Translate a PIN from BDK to BDK or ZPK Encryption (3-DES DUKPT)	GO (G1)	321
Verify a PIN Using the IBM Method (3-DES DUKPT)	GO (GP)	324
Verify a PIN Using the VISA PVV Method (3-DES DUKPT)	GQ (GR)	328
Verify a PIN Using the Diebold Method (3-DES DUKPT)	GS (GT)	331
Verify a PIN Using the Encrypted PIN Method (3-DES DUKPT)	GU (GV)	334
Generate/Verify a MAC (3-DES DUKPT)	GW (GX)	337
RSA Cryptosystem Commands		
Generate a Public/Private Key Pair	EI (EJ)	340
Load a Private Key	EK (EL)	343
Translate a Private Key	EM (EN)	345
Import a Public Key	EO (EP)	347
Validate a Public Key	EQ (ER)	350
Validate a Certificate and Import the Public Key	ES (ET)	352
Translate a Public Key	EU (EV)	355
Generate an RSA Signature	EW (EX)	357
Validate an RSA Signature	EY (EZ)	359
Import Key or data under an RSA Public Key	GI (GJ)	361
Export Key under an RSA Public Key	GK (GL)	369
Hash a Block of Data	GM (GN)	374
VISA Cash Commands		
Verify Load Signature S1 and Generate Load Signature S2	DM (DN)	377
Verify Load Completion Signature S3	DO (DP)	379
Verify Unload Signature S1 and Generate Unload Signature S2	DQ (DR)	381
Verify Unload Completion Signature S3	DS (DT)	383

Function	Command	Page
Legacy Commands		
Generate a CVK Pair	AS (AT)	388
Generate and Print a TMK, TPK or PVK	OE (OF, OZ)	390
Generate a Pair of PVKs	FG (FH) *	392
Generate a Watchword Key	FO (FP)	395
Generate ZEK/ZAK	FI (FJ)	397
Generate a ZPK	IA (IB)	399
Form a ZMK from Three ZMK Components	GG (GH)	401
Form a ZMK from 2 to 9 ZMK Components	GY (GZ)	403
Generate and Print a ZMK Component	OC (OD, OZ)	405
Translate a CVK Pair from Old LMK to New LMK Encryption	AY (AZ)	407
Translate a CVK Pair from LMK to ZMK Encryption	AU (AV)	409
Translate a CVK Pair from ZMK to LMK Encryption	AW (AX)	411
Translate a TMK, TPK or PVK	AA (AB) *	413
Translate a TMK, TPK or PVK from LMK to ZMK Encryption	FE (FF) *	415
Translate a TMK, TPK or PVK from ZMK to LMK Encryption	FC (FD) *	417
Translate a TAK	AC (AD)	419
Translate a TAK from LMK to ZMK Encryption	MG (MH)	421
Translate a TAK from ZMK to LMK Encryption	MI (MJ)	423
Translate a Watchword Key from LMK to ZMK Encryption	FQ (FR)	425
Translate a Watchword Key from ZMK to LMK Encryption	FS (FT)	427
Translate a ZEK/ZAK from LMK to ZMK Encryption	FM (FN)	429
Translate a ZEK/ZAK from ZMK to LMK Encryption	FK (FL)	431
Translate a ZPK	KC (KD)	433
Translate a ZPK from LMK to ZMK Encryption	GC (GD)	435
Translate a ZPK from ZMK to LMK Encryption	FA (FB)	437
Translate a ZMK	GE (GF)	439
Generate a Key Check Value (Not Double-Length ZMK)	KA (KB)	441
Generate a CSCK	RY (RZ)	443
Export a CSCK	RY (RZ)	445
Import a CSCK	RY (RZ)	447
Generate a BDK	BI (BJ)	449
Translate a BDK from ZMK to LMK Encryption	DW (DX)	450
Translate a BDK from LMK to ZMK Encryption	DY (DZ)	452
Generate and Export a KML	DI (DJ)	454
Import a KML	DK (DL)	456
Generate a MAC	MA (MB)	458
Verify a MAC	MC (MD)	460
Verify and Translate a MAC	ME (MF)	462
Generate MAC (MAB) for Large Message	MQ (MR)	464
Generate MAC (MAB) using ANSI X9.19 Method for a Large Message	MS (MT)	466

Function	Command	Page
Generate a Binary MAC	MK (ML)	468
Verify a Binary MAC	MM (MN)	470
Verify and Translate a Binary MAC	MO (MP)	472
Translate a PIN from BDK to ZPK Encryption (DUKPT)	CI (CJ)	474
Verify a PIN Using the IBM Method (DUKPT)	CK (CL)	476
Verify a PIN Using the VISA PVV Method (DUKPT)	CM (CN)	480
Verify a PIN Using the Diebold Method (DUKPT)	CO (CP)	482
Verify a PIN Using the Encrypted PIN Method (DUKPT)	CQ (CR)	484

* These commands are disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value of "Y". They should be replaced with newer Host commands as follows:

Host Command		Replaced by	
AA	Translate a TMK, TPK or PVK	BW	Translate Keys from Old LMK to New LMK
AE	Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK	A8	Export a Key
FC	Translate a TMK, TPK or PVK from ZMK to LMK Encryption	A6	Import a Key
FE	Translate a TMK, TPK or PVK from LMK to ZMK Encryption	A8	Export a Key
FG	Generate a pair of PVKs	AO	Generate a Key
HC	Generate a TMK, TPK or PVK	AO	Generate a Key
KA	Generate a Key Check Value (Not Double-Length ZMK)	BU	Generate a Key Check Value
OE	Generate and Print a TMK, TPK or PVK	NE	Generate and Print a Key as Split Components

>> Chapter 2 – Host Commands

General

This Chapter 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.

For convenience, the STX and ETX control characters, which bracket every command and response when using asynchronous communications, are not shown in the details that follow.

In a command to the payShield 9000 HSM, 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 9000 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 9000 can support 1 or 2 digit Atalla variants.

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

Symmetric Key Management Commands

The payShield 9000 HSM provides the following host commands to support generic key management operations:

Command	Page
Generate a Key (A0)	20
Generate and Print a Component (A2)	27
Generate and Print a Key as Split Components (NE)	31
Form a Key from Encrypted Components (A4)	34
Import a Key (A6)	37
Export a Key (A8)	42
Translate Key Scheme (B0)	47
Translate ZMK from ZMK to LMK encryption (BY)	48
Generate a TMK, TPK or PVK (HC) *	51
Generate a TAK (HA)	53
Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK (AE) *	55
Translate a TAK from LMK to TMK Encryption (AG)	57

* These commands are disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value of "Y". They should be replaced with newer Host commands as follows:

Host Command		Replaced by	
AE	Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK	A8	Export a Key
HC	Generate a TMK, TPK or PVK	A0	Generate a Key

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 ϕ
402	Card Verification Key, CVK
402	Card Verification Key, CSCK
003	Terminal Authentication Key, TAK
006	Watchword key, WWK
008	Zone authentication key, ZAK
009	DUKPT Base Derivation Key, BDK Type 1
609	DUKPT Base Derivation Key, BDK Type 2
809	DUKPT Base Derivation Key, BDK Type 3
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 ø	Terminal PIN Key, TPK
80D ø	Terminal Master Key, TMK

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

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

ϕ IKEY is also known as IPEK.

Keyblock LMK

Usage	Key Name
01	WatchWord Key (WWK)
B0	DUKPT Base Derivation Key (BDK Type 1)
41	DUKPT Base Derivation Key (BDK Type 2)
42	DUKPT Base Derivation Key (BDK Type 3)
B1	DUKPT Initial Key, IKEY ϕ
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	Visa Cash Master Load Key (KML)
32	Dynamic CVV Master Key (MK-CVC3)
K0	Key encryption or wrapping (generic)
51	Terminal key encryption (TMK)
52	Zone key encryption (ZMK)
M1	ISO 9797-1 MAC algorithm 1 (using DES/3-DES)
M3	ISO 9797-1 MAC algorithm 3 (using 3-DES)
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, IBM 3624
V2	PIN verification, Visa PVV

ϕ IKEY is also known as IPEK.

Generate a Key

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
Variant LMK	Authorization: **Determined by KTT(G&E)** Activities: **generate.{*key*}.host** and **export.{*key*}.host**
Keyblock LMK	Authorization: **If export to non-KB** Activity: **export.{*key*}.host**

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

	Variant LMK	Keyblock LMK
Authorization:	This command examines the 'Generate' flag of the given key type within the Key Type Table (see Chapter 4 of the payShield 9000 General Information Manual) 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. If the generated key is required to be exported under the ZMK or TMK, this command also examines the 'Export' flag of the given key type within the Key Type Table (see Chapter 4 of the payShield 9000 General Information Manual). 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.	The authorization requirement for this command depends solely on the type of export being requested: **"Key Scheme (ZMK)"** / **Authorization** No export / None 'S' (Thales Keyblock) / None 'R' (TR-31 Keyblock) / None 'U', 'T' (Variant) / Required 'Z', 'X', 'Y' (X9.17) / Required 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.

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 or TMK)
- 003 (TAK)
- 30B (TEK)
- 302 (IKEY[ϕ])

If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y":

- 70D (TPK)
- 80D (TMK)
- 003 (TAK)
- 30B (TEK)
- 302 (IKEY[ϕ])

[ϕ] IKEY is also known as IPEK.

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)
- '51' (TMK)

When exporting the new key, the ZMK (or TMK) keyblock must have the following field values:

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

[*] Note: Exporting to a keyblock format is not permitted with a single-length ZMK or TMK.

Further Notes: Exporting to a keyblock format requires the ZMK/TMK to be one of the following:

- Double or triple length DES key
- Any size AES key

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 '1' : Generate key and encrypt under ZMK (or TMK) 'A' : Derive key 'B' : Derive key and encrypt under ZMK (or TMK)
Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be generated/derived. When generating a new key (Mode = '0' or '1'), a list of possible values is shown in Available Key Types/Usages (p.19). When deriving a key from a master key (Mode = 'A' or 'B'), a list of possible values is listed below:

Key Type	Description	Derive Key Mode
302	IKEY[ϕ]	0 (DUKPT)
001	ZPK	1 (ZKA)
008	ZAK	1 (ZKA)
00A	ZEK	1 (ZKA)

[ϕ] IKEY is also known as IPEK.

		For a Keyblock 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 at Appendix C of the payShield 9000 General Information Manual.
Derive Key Mode	1 A	Only present if Mode = 'A' or 'B'. Indicates the operation to derive an encryption key: '0' : DUKPT - Derive IKEY[ϕ] from DUKPT Master Key Type '1' : ZKA – Derive ZKA key from ZKA Master Key [ϕ] IKEY is also known as IPEK.
DUKPT Master Key Type	1 H	Only present if Derive Key Mode = '0'. This field indicates the DUKPT Master Key Type for deriving the encryption key: '1' : BDK Type-1 (bidirectional encryption key) '2' : BDK Type-2 (unidirectional encryption key)
DUKPT Master Key		Only present if Derive Key Mode = '0'. The DUKPT Master Key (BDK).
	1 A + 32 / 48 H	For a Variant LMK: If DUKPT Master Key Type = '1': BDK Type-1 encrypted under LMK 28/29 If DUKPT Master Key Type = '2': BDK Type-2 encrypted under LMK 28/29 variant 6
	or 1 A + n A	For a Keyblock LMK, the BDK must comply with the following: Key Usage: 'B0', '41'; Algorithm: 'T'; Mode of Use: 'X', 'N'
KSN	15 H	Only be present if Derive Key Mode = '0'. A Key Set Identifier and Device ID for deriving the Initial Key. Right justified and padded with"Fs". (NOTE: there is no Transaction Counter, as there would be with a KSN sent in transaction data from a terminal.) Example: For a KSI + DID of 303950+12342468 (14 hex characters), the KSN field would be "F3039501234246 8" The last hex character (8) must be even. See the Host Programmer Manual for further information.
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. Must be one of the following values: 607 : Master Key is encrypted under LMK pair 24-25/6 002 : Master Key is encrypted under LMK pair 14-15 001 : Master Key is encrypted under LMK pair 06-07
		For a Keyblock LMK: This field is ignored; should be set to 'FFF'

<table>
<tr><td>ZKA Master Key</td><td></td><td>Only present if Derive Key Mode = '1'.</td></tr>
<tr><td></td><td>32 H
or
1 A + 32/48 H</td><td>For a Variant LMK, the ZKA Master Key is encrypted under the LMK pair/variant indicated by the ZKA Master Key Type field.</td></tr>
<tr><td></td><td>or
1 A + n A</td><td>For a Keyblock LMK, the ZKA Master Key must comply with the following:
<table>
<tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr>
<tr><td>'53'</td><td>'T'</td><td>'X'</td></tr>
</table></td></tr>
<tr><td>ZKA Option</td><td>1 H</td><td>Only present if Derive Key Mode = '1'.
'0' : Derive key using supplied RNDI
'1' : Derive key using new RNDI</td></tr>
<tr><td>ZKA RNDI</td><td>32 H</td><td>Only present if ZKA Option = '0'.
Random Number Input used to derive the PAC/MAC/DE key from the ZKA Master Key.</td></tr>
<tr><td>Delimiter</td><td>1 A</td><td>Value ';'. Optional. Can only be present if Mode = '1' or 'B'.
If present, the following field must be present.</td></tr>
<tr><td>ZMK/TMK Flag</td><td>1 N</td><td>Optional. Only present if the above delimiter is present.
'0' : ZMK (default value if these fields are not present)
'1' : TMK</td></tr>
<tr><td>ZMK (or TMK)</td><td></td><td>Only present if Mode = '1' or 'B'.
The Zone Master Key (or Terminal Master Key). For a ZMK, the length of the key must correspond to the ZMK key length as defined in the Security Settings.</td></tr>
<tr><td></td><td>16 / 32 H
or
1 A + 32/48 H</td><td>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”.</td></tr>
<tr><td></td><td>or
1 A + n A</td><td>For a Keyblock LMK, the 'ZMK (or TMK)' must comply with the following:
<table>
<tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr>
<tr><td>'K0', '51', 52'</td><td>'D', 'T', 'A'</td><td>'B', 'E', 'N'</td></tr>
</table></td></tr>
<tr><td>Key Scheme (ZMK or TMK)</td><td>1 A</td><td>Only present if Mode = '1' or 'B'.
Indicates the scheme for encrypting the key under the ZMK (or TMK). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual.</td></tr>
<tr><td>Atalla Variant</td><td>1 / 2 N</td><td>Only present if Mode = '1' or 'B'.
Optional. Atalla variant; for use in systems with Atalla equipment.</td></tr>
<tr><td>Delimiter</td><td>1 A</td><td>Value '%'. Optional; if present, the following field must be present.</td></tr>
<tr><td>LMK Identifier</td><td>2 N</td><td>LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.</td></tr>
</table>

Applies only when generating & optionally exporting in keyblock format	Delimiter	1 A	Value '#'. Required when generating a keyblock. If present, the following fields must be present.
	Key Usage	2 A	Key Usage field, to be included in the keyblock header; must be present if the above Delimiter is present. For a list of possible values, see Available Key Types/Usages (p.19).
	Algorithm	2 A	Algorithm and key length; the first character will be included in the algorithm field in the keyblock 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 keyblock 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 Chapter 5 of the General Information Manual.
	Key Version Number	2 N	Key Version Number field, to be included in the keyblock 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 keyblock header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in Chapter 5 of the General Information Manual.
	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 when the generated key is to be exported; if present, the following field must 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.

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 keyblock 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 Chapter 5 of the General Information Manual.
	Mode of Use	1 A	Mode of Use field, to be included in the keyblock 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 keyblock 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 keyblock 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 '10' : ZMK or TMK Parity error '68' : Command disabled or a standard error code.
Key (under LMK)		The new key, encrypted under the LMK.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'Key (under LMK)' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'.
	or 1 A + n A	For a Keyblock LMK, the 'Key (under LMK)' will be encrypted under the LMK.
Key (under ZMK or TMK)	16 H or 1 A + 32/48 H	Only present if Mode = '1' or 'B'. The new key, encrypted under the supplied ZMK (or TMK).
	or 1 A + n A	
Key Check Value	6 H	The key check value.
ZKA RNDI	32 H	Only present if ZKA Option = '1'. 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC0027**	
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	Keyblock 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 Available Key Types/Usages (p.19).	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 keyblock component being generated. For a list of possible values, see Available Key Types/Usages (p.19).
Notes:		In practice, the Number of Optional Blocks field in the component keyblock should be set to '00', since any such fields are discarded when the keyblock is formed (e.g. using command 'A4').

A printer must be attached to one of the USB ports on the payShield 9000, 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.

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 Chapter 4 of the payShield 9000 General Information Manual and Available Key Types/Usages (p. 19).
		For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
Component Check Flag	1 A	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'.
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 at Appendix C of the payShield 9000 General Information Manual.
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 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.
Applies only when generating components in keyblock format: Delimiter	1 A	Value '#'. Required when generating a keyblock component. If present, the following fields must be present.
Applies only when generating components in keyblock format: Key Usage	2 A	Key Usage field, to be included in the keyblock header; must be present if the above Delimiter is present. For a list of possible values, see Chapter 5 of the General Information Manual.
Applies only when generating components in keyblock format: Algorithm	2 A	Algorithm and key length; the first character will be included in the algorithm field in the keyblock 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
Applies only when generating components in keyblock format: Mode of Use	1 A	Mode of Use field, to be included in the keyblock 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 Chapter 5 of the General Information Manual.

Field		Length & Type	Details
	Key Version Number	2 N	Key Version Number field, to be included in the keyblock 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 keyblock header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in Chapter 5 of the General Information Manual.
	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.
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		The new component, encrypted under the LMK.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'Component' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'.
	or 1 A + n A	For a Keyblock 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.
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 ☑	Keyblock LMK ☑
License: **HSM9-LIC027**	
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	Keyblock 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 Available Key Types/Usages (p.19).	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 keyblock/component being generated. For a list of possible values, see Available Key Types/Usages (p.19).

Notes:

A printer must be attached to one of the USB ports on the payShield 9000, 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.

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	For a Variant LMK: Indicates the key type of the key to be generated. For a list of possible values, see Key Type Codes in Chapter 4 of the General Information Manual. and Available Key Types/Usages (p. 19). For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
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 at Appendix C of the payShield 9000 General Information Manual.
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 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.
Applies only when generating components in keyblock format: Delimiter	1 A	Value '#'. Required when generating a keyblock. If present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the keyblock header; must be present if the above Delimiter is present. For a list of possible values, see Chapter 5 of the General Information Manual.
Algorithm	2 A	Algorithm and key length; the first character will be included in the algorithm field in the keyblock 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 keyblock 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 Chapter 5 of the General Information Manual.
Key Version Number	2 N	Key Version Number field, to be included in the keyblock header; any permitted values; must be present if the above Delimiter is present.
Exportability	1 A	Exportability field, to be included in the keyblock header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in Chapter 5 of the General Information Manual.

Field	Length & Type	Details
Number of Optional Blocks	2 N	Number of Optional Bocks 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		The new key, encrypted under the LMK.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'Key' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'.
	or 1 A + n A	For a Keyblock 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.
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. Maximum length 32 characters

Form a Key from Encrypted Components

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
Authorization: **Required** Activity: **component.{*key*}.host**	

Function: To form a key from encrypted components.

	Variant LMK	Keyblock 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 Available Key Types/Usages (p.19).	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 keyblock being formed. For a list of possible values, see Available Key Types/Usages (p.19).
Notes:		The Key Usage, Mode of Use, Algorithm and Exportability fields specified after the '#' delimiter must match the corresponding values in all component keyblocks. 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.

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	For a Variant LMK: Indicates the key type of the key to be generated. For a list of possible values, see Key Type Codes in Chapter 4 of the General Information Manual and Available Key Types/Usages (p. 19).
		For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
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 at Appendix C of the payShield 9000 General Information Manual.

	Key Component 1	16 H or 1 A + 32/48 H or 1 A + n A	Encrypted key component 1.
	Key Component 2	16 H or 1 A + 32/48 H or 1 A + n A	Encrypted key component 2.
	…	…	…
	Key Component n	16 H or 1 A + 32/48 H or 1 A + n A	Encrypted key component n.
	Delimiter	1 A	Value '%'. Optional; if present, the following field must 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.
Applies only when combining components in keyblock format	Delimiter	1 A	Value '#'. Required when forming a keyblock. If present, the following fields must be present.
	Key Version Number	2 N	Key Version Number field, to be included in the keyblock 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)		The formed key, encrypted under the LMK.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'Key (under LMK)' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'.
	or 1 A + n A	For a Keyblock 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

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
Variant LMK	Authorization: **Determined by KTT(I)** Activities: **import.{*key*}.host**
Keyblock LMK	Authorization: **If import from non-KB** Activity: **import.{*key*}.host**

Function: To import a key encrypted under a ZMK.

	Variant LMK	Keyblock LMK
Authorization:	This command examines the 'Import' flag of the given key type within the Key Type Table (see Chapter 4 of the payShield 9000 General Information Manual) 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: **Scheme of "Key (ZMK)"** / **Auth** 'S' (Thales Keyblock) / None 'R' (TR-31 Keyblock) / None 'U', 'T' (Variant) / Required 'Z', 'X', 'Y' (X9.17) / Required 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.
Notes:	This command cannot be used to import a ZMK.	When importing, the ZMK keyblock must have the following field values: **"ZMK" Keyblock Header** / **Value(s)** Key Usage / 'K0', '52' Algorithm / 'D'*, 'T' Mode of Use / 'B', 'D', 'N' * Note: Importing from a keyblock format is not permitted with a single-length ZMK.

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 (ø)
TPK ZPK	1 or 01	002 LMK 14-15 001 LMK 06-07	70D LMK 36-37/7 001 LMK 06-07
ZEK	2 or 02	00B LMK 32-33 00A LMK 30-31	00B LMK 32-33 00A LMK 30-31
TAK ZAK CVK	3 or 03	003 LMK 16-17 008 LMK 26-27 402 LMK 14-15/4	003 LMK 16-17 008 LMK 26-27 402 LMK 14-15/4
TMK TPK PVK	4 or 04	002 LMK 14-15 002 LMK 14-15 002 LMK 14-15	80D LMK 36-37/8 70D LMK 36-37/7 002 LMK 14-15
TMK	5 or 05	002 LMK 14-15	80D LMK 36-37/8
BDK type-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 type-2	30	609 LMK 28-29/6	609 LMK 28-29/6
BDK type-3	8 or 08	809 LMK 28-29/8	809 LMK 28-29/8

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

ø Applies if the security setting "`Enforce key type 002 separation for PCI HSM compliance`" 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 'A6'.
Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be imported. For a list of possible values, see Key Type Codes in Chapter 4 of the General Information Manual. For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
ZMK		The ZMK encrypted under the LMK.
	16 / 32 H or 1 A + 16/32/48 H	For a Variant LMK, the 'ZMK' is encrypted under LMK pair 04-05.
	or 1 A + n A	For a Keyblock LMK, the 'ZMK' must comply with the following: Key Usage: 'K0', '52'; Algorithm: 'D', 'T', 'A'; Mode of Use: 'B', 'D', 'N'
Key (ZMK)		The Key to be imported, encrypted under the ZMK. The Key can be in X9.17, Variant, TR-31 Keyblock, or Thales Keyblock format.
	16 H or 1 A + 16/32/48 H or 1 A + n A	If in Thales or TR-31 keyblock format, the 'Key (ZMK)' must comply with the following: Key Usage: Any valid value; Algorithm: 'D', 'T', 'A'; Mode of Use: Any valid value For a list of valid Key Usage values, refer to Available Key Types/Usages (p. 19).
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 at Appendix C of the payShield 9000 General Information Manual.
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 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.
TR-31 keyblock$_{ZMK}$ → Keyblock$_{LMK}$ only: Delimiter	1 A	Value '#'. Optional; can only be present when the key to be imported is in TR-31 keyblock format; if present, the following fields must be present.
Modified Key Usage	2 A	Key Usage field, to be included in the imported keyblock 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.

Field		Length & Type	Details
$Variant_{ZMK} \rightarrow Keyblock_{LMK}$ only	Delimiter	1 A	Value '#'. Optional; can only be present when the key to be imported is not in a keyblock 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 Chapter 5 of the General Information Manual.
	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 Chapter 5 of the General Information Manual.
	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 '68' : Command disabled or a standard error code..
Key (under LMK)		The imported key, encrypted under the LMK.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'Key (under LMK)' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'.
	or 1 A + n A	For a Keyblock 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.

Note: For legacy reasons, the import of a ZMK or DEK from encryption under a ZMK (in variant/X9.17 format) to encryption under a keyblock LMK will not be permitted. Specifically, such import of keys with key usage = "K0", "52", "D0", "21" or "22" will be prohibited.

Export a Key

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
Variant LMK	Authorization: **Determined by KTT(E)** Activity: **export.{*key*}.host**
Keyblock 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	Keyblock LMK
Authorization:	This command examines the 'Export' flag of the given key type within the Key Type Table (see Chapter 4 of the payShield 9000 General Information Manual) 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.	The authorization requirement for this command depends on the type of export being requested: "Key Scheme (ZMK)" — Authorization 'S' (Thales Keyblock) — None 'R' (TR-31 Keyblock) — None 'V' (Verifone/GISKE Keyblock) — None 'U', 'T' (Variant) — Required 'Z', 'X', 'Y' (X9.17) — Required 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.
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) If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y": • 70D (TPK) • 003 (TAK) • 30B (TEK)	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) A keyblock that is exported to Verifone/GISKE keyblock format must have the following Key Usage values: • 'P0', '71' (TPK) • 'M0', 'M3' (TAK) The ZMK (or TMK) keyblock must have the following field values: "ZMK" KB Header — Value(s) Key Usage — 'K0', '51', or '52' Algorithm — 'D'*, 'T', or 'A' Mode of Use — 'B', 'E', or 'N' * Note: Exporting to a keyblock format is not permitted with a single-length ZMK or TMK. When exporting from Thales keyblock to TR-31 format, any Thales proprietary Key Usage value is converted to a standard TR-31 value.

Further Notes: Exporting to a keyblock format requires the use of a 3-DES or AES ZMK or TMK.

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

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	For a Variant LMK: Indicates the key type of the key to be exported. For a list of possible values, see Available Key Types/Usages (p.19). For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
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)		The Zone Master Key (or Terminal Master Key).
	16 / 32 H or 1 A + 16/32/48 H	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").
	or 1 A + n A	For a Keyblock LMK, the 'ZMK (or TMK)' must comply with the following: Key Usage: 'K0', '51', '52'; Algorithm: 'D', 'T', 'A'; Mode of Use: 'B', 'D', 'N'
Key		Key to be exported; encrypted under the LMK.
	16 H or 1 A + 16/32/48 H	For a Variant LMK, the 'Key' is encrypted under the LMK pair/variant indicated by the Key Type. For export to Verifone/GISKE keyblock format, the 'Key' must be a 3-DES TPK or TAK.
	or 1 A + n A	For a Keyblock LMK, the 'Key' must comply with the following: Key Usage: Any valid value; Algorithm: 'D', 'T', 'A'; Mode of Use: Any valid value For a list of valid Key Usage values, refer to Available Key Types/Usages (p. 19). For export to Verifone/GISKE keyblock format, the 'Key' must comply with the following: Key Usage: 'M0', 'M3', 'P0', '71'; Algorithm: 'T'; Mode of Use: Any valid value

	Field	Length & Type	Details
	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 at Appendix C of the payShield 9000 General Information Manual.
	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 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.
$Keyblock_{LMK} \rightarrow Keyblock_{ZMK}$	Delimiter	1 A	Value '&'. Optional; can only be present when the exported key is in keyblock 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.
$Variant_{LMK} \rightarrow Keyblock_{ZMK}$ (TR-31 only)	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 Chapter 5 of the General Information Manual.
	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 Chapter 5 of the General Information Manual.
	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 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.

$Variant_{LMK} \rightarrow Keyblock_{ZMK}$ (GISKE only)	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	Keyblock 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 '68' : Command disabled or a standard error code.
Key (under ZMK or TMK)	16 H or 1 A + 32/48 H or 1 A + 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.

Note: For legacy reasons, the export of a ZMK, ZEK or DEK from encryption under a key block LMK to encryption under a ZMK (in variant/X9.17 format) will not be permitted. Specifically, such export of keys with key usage = "K0", "52", "D0", "21" or "22" will be prohibited.

Translate Key Scheme

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC001**	
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 1 A + 32/48 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 at Appendix C of the payShield 9000 General Information Manual.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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	1 A + 32/48 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
Variant LMK	Authorization: **Required** Activities: **import.{*key*}.host**
Keyblock LMK	Authorization: **Not required**

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

Authorization:

Variant LMK	Keyblock LMK
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: **Scheme of "Key (ZMK)"** — **Authorization** 'S' (Thales Keyblock) — None 'R' (TR-31 Keyblock) — None 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.

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		The ZMKi encrypted under the LMK.
	16 / 32 H or 1 A + 32/48 H	For a Variant LMK, the 'ZMKi' is encrypted under LMK pair 04-05.
	or 1 A + n A	For a Keyblock LMK, the 'ZMKi' must comply with the following: **Key Usage**: 'K0', '52' **Algorithm**: 'T', 'A' **Mode of Use**: 'B', 'D', 'N'
ZMK		The ZMK encrypted under ZMKi.
	16 / 32 H or 1 A + 32/48 H or 1 A + n A	For a Variant LMK, the 'ZMK' must be in Variant or TR-31 format. If in Thales or TR-31 keyblock format, the 'ZMK' must comply with the following: **Key Usage**: 'K0', '52' **Algorithm**: 'D', 'T', 'A' **Mode of Use**: 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 at Appendix C of the payShield 9000 General Information Manual.
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.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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.
TR-31 $ZMK_{ZMKi} \rightarrow Keyblock_{LMK}$ only: Delimiter	1 A	Value '#'. Optional; can only be present when the ZMK to be imported is in TR-31 keyblock format; if present, the following fields must be present.
Modified Key Usage	2 A	Key Usage field, to be included in the imported keyblock 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.
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 '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		The translated ZMK, encrypted under the LMK.
	16 / 32 H or 1 A + 32/48 H	For a Variant LMK, the 'ZMK' will be encrypted under LMK pair 04-05.
	or 1 A + n A	For a Keyblock 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.

Generate a TMK, TPK or PVK

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Generate a random key, and encrypt it under a TMK (TPK or PVK) and under LMK pair 14-15.

Notes:

- This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'HC'.
Current TMK, TPK or PVK	16 H or 1 A + 32/48 H	The current TMK, TPK or PVK encrypted under LMK pair 14-15.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (TMK)	1 A	Optional. Key scheme for encrypting key under TMK (or 'O'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or 'O'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual.
Reserved	1 A	Optional. If present must be 'O'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'HD'.
Error Code	2 A	'00' : No error '10' : TMK, TPK or PVK parity error '68' : Command disabled or a standard error code.
New key under the current key	16 H or 1 A + 32/48 H	The new key encrypted under the current key.
New key under LMK	16 H or 1 A + 32/48 H	The new key under LMK pair 14-15.
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 TAK

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Generate a random key, encrypt it under a TMK and under LMK pair 16-17.

Notes: If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", then PVKs and TPKs are encrypted under the same LMK pair and variant as TMKs. However, PVKs and TPKs must not be used with this command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'HA'.
TMK	16 H or 1 A + 32/48 H	The TMK 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".
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (TMK)	1 A	Optional. Key scheme for encrypting key under TMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual.
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 at Appendix C of the payShield 9000 General Information Manual.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'HB'.
Error Code	2 A	'00' : No error '10' : TMK parity error '68' : Command disabled or a standard error code.
TAK under TMK	16 H or 1 A + 32/48 H	The random TAK encrypted under the TMK.
TAK under LMK	16 H or 1 A + 32/48 H	The random TAK 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.

Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a TMK, TPK or PVK from encryption under LMK pair 14-15 to encryption under another TMK (TPK or PVK).

Note:
- The command is used to replace an existing key with another key from the database.
- This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AE'.
Current TMK, TPK or PVK	16 H or 1 A + 32/48 H	The current TMK, TPK or PVK encrypted under LMK pair 14-15.
Stored TMK, TPK or PVK	16 H or 1 A + 32/48 H	The stored TMK, TPK or PVK under LMK pair 14-15.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (TMK)	1 A	Optional. Key scheme for encrypting key under TMK (or 'O'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual.
Reserved	1 A	Optional. If present must be '0'.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'AF'.
Error Code	2 A	'00' : No error '10' : Current TMK, TPK or PVK parity error '11' : Stored TMK, TPK or PVK parity error '68' : Command disabled or a standard error code.
Stored key under the current key	16 H or 1 A + 32/48 H	The stored key encrypted under the current 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.

Translate a TAK from LMK to TMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a TAK from encryption under the LMK to encryption under a TMK. Used to send a key to a terminal.

Notes: This command is superseded by host command 'A8'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AG'.
TMK	16 H or 1 A + 32/48 H	TMK encrypted under the 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".
TAK	16 H or 1 A + 32/48 H	TAK encrypted under LMK pair 16-17.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Key Scheme (TMK)	1 A	Optional. Key scheme for encrypting key under TMK (or 'O'). For a list of key schemes, see Appendix C of the payShield 9000 General Information Manual.
Reserved	1 A	Optional. If present must be 'O'.
Reserved	1 A	Optional. If present must be 'O'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'AH'.
Error Code	2 A	'00' : No error '10' : TMK parity error '11' : TAK parity error '68' : Command disabled or a standard error code.
TAK	16 H or 1 A + 32/48 H	Translated TAK; encrypted under the TMK.
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.

PIN and Offset Generation Commands

The payShield 9000 HSM 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.

These commands are capable of rejecting 'weak' PINs (i.e. PINs that are considered easily guessed by someone other than the legitimate cardholder) if the Security Setting "*Enable weak PIN checking*" has been set to Yes. Weak PINs can be defined by passing them into the payShield in an 'Excluded PIN Table':

- Using the '**Load the Excluded PIN Table**' host command, a global Excluded PIN Table can be loaded into the payShield, containing PINs that are considered weak for all customers;
- Using one of the PIN/offset generation commands below, a local Excluded PIN Table can be loaded into the payShield, containing PINs that are considered weak for the specific customer whose PIN/offset is being generated.

The payShield 9000 HSM provides the following host commands to support the PIN/Offset generation and Weak PIN configuration operations:

Command	Page
Derive a PIN Using the IBM Method (EE)	60
Derive a PIN Using the Diebold Method (GA)	63
Generate a Random PIN (JA)	65
Generate an IBM PIN Offset (of an LMK encrypted PIN) (DE)	67
Generate an IBM PIN Offset (of a customer selected PIN) (BK)	71
Generate a Diebold PIN Offset (CE)	75
Generate a VISA PIN Verification Value (of an LMK encrypted PIN) (DG)	77
Generate a VISA PIN Verification Value (of a customer selected PIN) (FW)	79
Load the Excluded PIN Table (BM)	82

Derive a PIN Using the IBM Method

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
Authorization: **Not required**	

Function: Generate a 4 to 12-digit PIN using the IBM 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** (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 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 3-DES 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 derived PIN against an 'Excluded PIN Table' in order to exclude 'weak' PINs.
- 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.

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 3-DES Keyblock LMK) or 'L' + 32 hexadecimal digits (for an AES Keyblock 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.

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

`Enable Weak PIN checking? [Yes/No]`

- When set to 'Yes', the incoming PIN field is checked to ensure it does not match one of the entries in the appropriate global 'Excluded PIN Table'. If present, the local 'Excluded PIN Table' is also checked. If a match is found in either list, then the command fails, returning error code 86.
- When set to 'No' (the default setting), the global and local 'Excluded PIN Table' are not checked. Error code 15 is returned if a local 'Excluded PIN Table' is provided.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'EE'.
PVK		The PIN Verification Key, used to generate the derived PIN.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.
	or 1 A + n A	For a Keyblock LMK, the 'PVK' must comply with the following: Key Usage: 'V1'; Algorithm: 'D', 'T'; Mode of Use: '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.
Check Length	2 N	The minimum PIN length.
Account Number	12 N	The 12 right-most digits of the account number, excluding the check digit.
Decimalization Table	16 N or 16 H or 1 A + 3 H or 1 A + 32 H	16 N when using Plaintext decimalization tables. 16 H when using Encrypted decimalization tables and a Variant LMK or 3-DES Keyblock 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 Keyblock LMK.

Field	Length & Type	Details
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 account number; 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 '*'. 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 the 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 Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 (See the note at the start of this section.) '10' : PVK parity error '68' : Command disabled '81' : PIN length mismatch '86' : PIN exists in either global or local Excluded PIN Table or a standard error code.
PIN	L N or L H or 1 A + 32 H	The derived PIN encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' 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.

Derive a PIN Using the Diebold Method

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
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.
  - 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.
- 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.

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.
Account Number	12 N	The 12 right-most digits of the account number, excluding the check digit.
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 account number. The data must be right-justified and padded with F.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 exists in either global or local Excluded PIN Table or a standard error code.
PIN	L N or L H or 1 A + 32 H	The derived PIN encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
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 does not match any entry in the 'Excluded PIN Table' in order to prevent 'weak' PINs being returned.
- 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.

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

```
Enable Weak PIN checking? [Yes/No]
```

- When set to 'Yes', the generated PIN field is checked to ensure it does not match one of the entries in the appropriate global 'Excluded PIN Table'. If present, the local 'Excluded PIN Table' is also checked. If a match is found in either list, then the PIN is discarded, another PIN is generated, and the checking process is repeated. This does not result in an error code being returned.
- When set to 'No' (the default setting), the global and local 'Excluded PIN Table' are not checked. Error code 15 is returned if a local 'Excluded PIN Table' is provided in the command.
- When the global 'Excluded PIN Table' is required to be checked, only the one corresponding to the PIN's length is checked.
- Before the local 'Excluded PIN Table' is checked, the 'Excluded PIN Length' parameter is checked to ensure that it matches the length of the PIN being checked.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'JA'.
Account Number	12 N	The 12 right-most digits of the account number, excluding the check digit.
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 '*'. 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 the 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 Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 1 A + 32 H	The new PIN encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
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 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 3-DES 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 against an 'Excluded PIN Table' in order to exclude 'weak' PINs.
- 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.

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 3-DES Keyblock LMK) or 'L' + 32 hexadecimal digits (for an AES Keyblock 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.

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

`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.

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

`Enable Weak PIN checking? [Yes/No]`

- When set to 'Yes', the incoming PIN field is checked to ensure it does not match one of the entries in the appropriate global 'Excluded PIN Table'. If present, the local 'Excluded PIN Table' is also checked. If a match is found in either list, then the command fails, returning error code 86.
- When set to 'No' (the default setting), the global and local 'Excluded PIN Table' are not checked. Error code 15 is returned if a local 'Excluded PIN Table' is provided in the command.
- When the global 'Excluded PIN Table' is required to be checked, only the one corresponding to the PIN's length is checked.
- Before the local 'Excluded PIN Table' is checked, the 'Excluded PIN Length' parameter is checked to ensure that it matches the length of the PIN being checked.

<table>
<tr><th>Field</th><th>Length & Type</th><th>Details</th></tr>
<tr><td colspan="3">COMMAND MESSAGE</td></tr>
<tr><td>Message Header</td><td>m A</td><td>Subsequently returned to the Host unchanged.</td></tr>
<tr><td>Command Code</td><td>2 A</td><td>Value 'DE'.</td></tr>
<tr><td>PVK</td><td></td><td>The PIN Verification Key, used to generate the offset.</td></tr>
<tr><td></td><td>16 H
or
1 A + 32/48 H</td><td>For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.</td></tr>
<tr><td></td><td>or
1 A + n A</td><td>For a Keyblock LMK, the 'PVK' must comply with the following:
<table>
<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></td></tr>
<tr><td>PIN</td><td>L N or L H
or
1 A + 32 H</td><td>The PIN for which an offset is required, encrypted under the LMK.
When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length".
When using an AES Keyblock LMK, this field must consist of a 'J' followed by 32 hex digits.</td></tr>
</table>

Check Length	2 N	The minimum PIN length.
Account Number	12 N	The 12 right-most digits of the account number, excluding check digit.
Decimalization Table	16 N or 16 H or 1 A + 3 H or 1 A + 32 H	16 N when using Plaintext decimalization tables. 16 H when using Encrypted decimalization tables and a Variant LMK or 3-DES Keyblock 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 Keyblock LMK.
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 account number; 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 '*'. 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 the 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 Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 (See the notes at the start of this section.) '10' : PVK parity error '68' : Command disabled '81' : PIN length mismatch '86' : PIN exists in either global or local Excluded PIN Table or a standard error code.

Offset	12 H	The resulting 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.

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

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
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 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 3-DES 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 against an 'Excluded PIN Table' in order to exclude 'weak' PINs.

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 3-DES Keyblock LMK) or 'L' + 32 hexadecimal digits (for an AES Keyblock 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.

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

`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.

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

`Enable Weak PIN checking? [Yes/No]`

- When set to 'Yes', the incoming PIN field is checked to ensure it does not match one of the entries in the appropriate global 'Excluded PIN Table'. If present, the local 'Excluded PIN Table' is also checked. If a match is found in either list, then the command fails, returning error code 86.
- When set to 'No' (the default setting), the global and local 'Excluded PIN Table' are not checked. Error code 15 is returned if a local 'Excluded PIN Table' is provided in the command.
- When the global 'Excluded PIN Table' is required to be checked, only the one corresponding to the PIN's length is checked.
- Before the local 'Excluded PIN Table' is checked, the 'Excluded PIN Length' parameter is checked to ensure that it matches the length of the PIN being checked.

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	For a Variant LMK: 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": '001' : ZPK (encrypted under LMK 06-07 variant 0) '002' : TPK (encrypted under LMK 14-15 variant 0) The following key types are permitted if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y": '001' : ZPK (encrypted under LMK 06-07 variant 0) '70D' : TPK (encrypted under LMK 36-37 variant 7)
		For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
PIN Block Key		The Key under which the PIN blocks are encrypted.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'PIN Block Key' is either a ZPK or TPK, as specified above.

	or 1 A + n A	For a Keyblock LMK, the 'PIN Block Key' must comply with the following: Key Usage: 'P0', '71', '72'; Algorithm: 'D', 'T'; Mode of Use: 'B', 'D', 'N'
PVK		The PIN Verification Key, used to generate the offset.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.
	or 1 A + n A	For a Keyblock LMK, the 'PVK' must comply with the following: Key Usage: 'V1'; Algorithm: 'D', 'T'; Mode of Use: 'C', 'G', 'N'
PIN Block	16 H	The PIN, for which an offset is required, encrypted under the PIN Block Key.
PIN Block Format Code	2 N	One of the valid PIN block format codes. If the security setting "Restrict PIN block usage for PCI HSM compliance" has the value "Y" then the PIN Block Format must be 01 (ISO format 0) or 47 (ISO format 3).
Check Length	2 N	The minimum PIN length.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
Decimalization Table	16 N or 16 H or 1 A + 3 H or 1 A + 32 H	16 N when using Plaintext decimalization tables. 16 H when using Encrypted decimalization tables and a Variant LMK or 3-DES Keyblock LMK. 'K' + 3 H to reference a table held in the payShield 9000 User Storage Area. 'L' + 32 H when using Encrypted decimalization tables and an AES Keyblock LMK.
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 account number; 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 '*'. 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 the 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 Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.

Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 '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 exists in either global or local Excluded PIN Table or a standard error code.
PIN Offset	12 H	The resulting 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.

Generate a Diebold PIN Offset

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
Authorization: **Not required**	

Function: Generate a PIN offset using the Diebold method.

Notes:

- Requires the Diebold table to be in user storage.
  - 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.
- This command will optionally check the input PIN against an 'Excluded PIN Table' 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]
```

- When set to 'Yes', the incoming PIN field is checked to ensure it does not match one of the entries in the appropriate global 'Excluded PIN Table'. If present, the local 'Excluded PIN Table' is also checked. If a match is found in either list, then the command fails, returning error code 86.
- When set to 'No' (the default setting), the global and local 'Excluded PIN Table' are not checked. Error code 15 is returned if a local 'Excluded PIN Table' is provided in the command.
- When the global 'Excluded PIN Table' is required to be checked, only the one corresponding to the PIN's length is checked.
- Before the local 'Excluded PIN Table' is checked, the 'Excluded PIN Length' parameter is checked to ensure that it matches the length of the PIN being checked.

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 1 A + 32 H	The PIN encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' followed by 32 hex digits.
Account Number	12 N	The 12 right-most digits of the account number, excluding the check digit.
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 account number. The data must be right-justified and padded with F.
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 the 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 Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 '86' : PIN exists in either global or local Excluded PIN Table 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 a VISA PIN Verification Value (of an LMK encrypted PIN)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
Authorization: **Not required**	

Function: Generate a 4-digit VISA PVV. 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.
- This command will optionally check the input PIN against an 'Excluded PIN Table' in order to exclude 'weak' PINs.
- 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.

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

`Enable Weak PIN checking? [Yes/No]`

- When set to 'Yes', the incoming PIN field is checked to ensure it does not match one of the entries in the appropriate global 'Excluded PIN Table'. If present, the local 'Excluded PIN Table' is also checked. If a match is found in either list, then the command fails, returning error code 86.
- When set to 'No' (the default setting), the global and local 'Excluded PIN Table' are not checked. Error code 15 is returned if a local 'Excluded PIN Table' is provided in the command.
- When the global 'Excluded PIN Table' is required to be checked, only the one corresponding to the PIN's length is checked.
- Before the local 'Excluded PIN Table' is checked, the 'Excluded PIN Length' parameter is checked to ensure that it matches the length of the PIN being checked.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DG'.
PVK Pair		The two PVKs, used to generate the PVV.
	32 H or 1 A + 32 H	For a Variant LMK, each PVK in the 'PVK Pair' must be encrypted under LMK pair 14-15 variant 0.

	or 1 A + n A	For a Keyblock LMK, the 'PVK Pair' is a double-length key, and must comply with the following: Key Usage: 'V2'; Algorithm: 'T'; Mode of Use: 'C', 'G', 'N'
PIN	L N or L H or 1 A + 32 H	The PIN for which a PVV is required, encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' followed by 32 hex digits.
Account Number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PVKI	1 N	The PVKI (should be between '0' and '6').
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 the 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 Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 '86' : PIN exists in either global or local Excluded PIN Table 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 a VISA PIN Verification Value (of a customer selected PIN)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
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: 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 against an 'Excluded PIN Table' 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]
```

- When set to 'Yes', the incoming PIN field is checked to ensure it does not match one of the entries in the appropriate global 'Excluded PIN Table'. If present, the local 'Excluded PIN Table' is also checked. If a match is found in either list, then the command fails, returning error code 86.
- When set to 'No' (the default setting), the global and local 'Excluded PIN Table' are not checked. Error code 15 is returned if a local 'Excluded PIN Table' is provided in the command.
- When the global 'Excluded PIN Table' is required to be checked, only the one corresponding to the PIN's length is checked.
- Before the local 'Excluded PIN Table' is checked, the 'Excluded PIN Length' parameter is checked to ensure that it matches the length of the PIN being checked.

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	For a Variant LMK: 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": '001' : ZPK (encrypted under LMK 06-07 variant 0) '002' : TPK (encrypted under LMK 14-15 variant 0) If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y": '001' : ZPK (encrypted under LMK 06-07 variant 0) '70D' : TPK (encrypted under LMK 36-37 variant 7) For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
PIN Block Key		The Key under which the PIN blocks are encrypted.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'PIN Block Key' is either a ZPK or TPK, as specified above.
	or 1 A + n A	For a Keyblock LMK, the 'PIN Block Key' must comply with the following: Key Usage: 'P0', '71', '72'; Algorithm: 'D', 'T'; Mode of Use: 'B', 'D', 'N'
PVK Pair		The two PVKs, used to generate the PVV.
	32 H or 1 A + 32 H	For a Variant LMK, each PVK in the 'PVK Pair' must be encrypted under LMK pair 14-15 variant 0.
	or 1 A + n A	For a Keyblock LMK, the 'PVK Pair' is a double-length key, and must comply with the following: Key Usage: 'V2'; Algorithm: 'T'; Mode of Use: 'C', 'G', 'N'
PIN Block	16 H	The PIN for which a PVV is required; encrypted under the PIN Block Key.
PIN Block Format Code	2 N	One of the valid PIN block format codes. If the security setting "Restrict PIN block usage for PCI HSM compliance" has the value "Y" then the PIN Block Format must be 01 (ISO format 0) or 47 (ISO format 3).
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
PVKI	1 N	The PVKI (should be between '0' and '6').
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 the 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 Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 exists in either global or local Excluded PIN Table 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
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 "*Enable weak PIN checking*" 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 'Excluded PIN Table'.
Excluded PIN Length	2 N	'04' … '12' : The length of each excluded PIN in the 'Excluded PIN Table'.
Excluded PIN Table	n N	A 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.

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 9000 HSM provides the following host commands to support PIN change operations:

Command	Page
Verify & Generate an IBM PIN Offset (of customer selected new PIN) (DU)	85
Verify & Generate a VISA PVV (of a customer selected PIN) (CU)	90

Verify & Generate an IBM PIN Offset (of customer selected new PIN)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: Verify an IBM PIN Offset, 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 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 3-DES 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 against an 'Excluded PIN Table' 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 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 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 3-DES Keyblock LMK) or 'L' + 32 hexadecimal digits (for an AES Keyblock 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.

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

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.

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

`Enable Weak PIN checking? [Yes/No]`

- When set to 'Yes', the incoming PIN field is checked to ensure it does not match one of the entries in the appropriate global 'Excluded PIN Table'. If present, the local 'Excluded PIN Table' is also checked. If a match is found in either list, then the command fails, returning error code 86.
- When set to 'No' (the default setting), the global and local 'Excluded PIN Table' are not checked. Error code 15 is returned if a local 'Excluded PIN Table' is provided in the command.
- When the global 'Excluded PIN Table' is required to be checked, only the one corresponding to the PIN's length is checked.
- Before the local 'Excluded PIN Table' is checked, the 'Excluded PIN Length' parameter is checked to ensure that it matches the length of the PIN being checked.

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	For a Variant LMK: 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": '001' : ZPK (encrypted under LMK 06-07 variant 0) '002' : TPK (encrypted under LMK 14-15 variant 0) If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y": '001' : ZPK (encrypted under LMK 06-07 variant 0) '70D' : TPK (encrypted under LMK 14-15 variant 7) For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
PIN Block Key		The Key under which the PIN blocks are encrypted.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'PIN Block Key' is either a ZPK or TPK, as specified above.
	or 1 A + n A	For a Keyblock LMK, the 'PIN Block Key' must comply with the following: Key Usage: 'P0', '71', '72' Algorithm: 'D', 'T' Mode of Use: 'B', 'D', 'N'
PVK		The PIN Verification Key, used to generate the offset.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.
	or 1 A + n A	For a Keyblock LMK, the 'PVK' must comply with the following: Key Usage: 'V1' Algorithm: 'D', 'T' Mode of Use: 'C', 'N'
Current PIN block	16 H	The Current PIN block encrypted under the PIN Block Key.
PIN Block format code	2 N	One of the valid PIN block format codes. If the security setting "Restrict PIN block usage for PCI HSM compliance" has the value "Y" then the PIN Block Format must be 01 (ISO format 0) or 47 (ISO format 3).
Check Length	2 N	The minimum PIN length.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.

Field	Length & Type	Details
Decimalization Table	16 N or 16 H or 1 A + 3 H or 1 A + 32 H	16 N when using Plaintext decimalization tables. 16 H when using Encrypted decimalization tables and a Variant LMK or 3-DES Keyblock 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 Keyblock LMK.
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 account number; 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 PIN Block Key.
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 the 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 Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 (See the notes at the start of this section.) '10' : PIN Block Key parity error '11' : PVK parity error '68' : Command disabled '69' : PIN Block format has been disabled

Field	Length & Type	Details
		'81' : PIN length mismatch '86' : PIN exists in either global or local Excluded PIN Table or a standard error code.
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.

Field	Length & Type	Details

Verify & Generate a VISA PVV (of a customer selected PIN)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: 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: 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 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 VISA Method (EC or DC)
- Translate a PIN from TPK/ZPK to LMK Encryption (JC or JE)
- Generate a VISA PVV (DG)

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

```
Enable Weak PIN checking? [Yes/No]
```

- When set to 'Yes', the incoming PIN field is checked to ensure it does not match one of the entries in the appropriate global 'Excluded PIN Table'. If present, the local 'Excluded PIN Table' is also checked. If a match is found in either list, then the command fails, returning error code 86.
- When set to 'No' (the default setting), the global and local 'Excluded PIN Table' are not checked. Error code 15 is returned if a local 'Excluded PIN Table' is provided in the command.
- When the global 'Excluded PIN Table' is required to be checked, only the one corresponding to the PIN's length is checked.
- Before the local 'Excluded PIN Table' is checked, the 'Excluded PIN Length' parameter is checked to ensure that it matches the length of the PIN being checked.

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	For a Variant LMK: 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": '001' : ZPK (encrypted under LMK 06-07 variant 0) '002' : TPK (encrypted under LMK 14-15 variant 0) If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y": '001' : ZPK (encrypted under LMK 06-07 variant 0) '70D' : TPK (encrypted under LMK 36-37 variant 7) For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
PIN Block Key		The Key under which the PIN blocks are encrypted.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'PIN Block Key' is either a ZPK or TPK, as specified above.
	or 1 A + n A	For a Keyblock LMK, the 'PIN Block Key' must comply with the following: Key Usage: 'P0', '71', '72'; Algorithm: 'D', 'T'; Mode of Use: 'B', 'D', 'N'
PVK Pair		The two PVKs, used to generate the PVV.
	32 H or 1 A + 32 H	For a Variant LMK, each PVK in the 'PVK Pair' must be encrypted under LMK pair 14-15 variant 0.
	or 1 A + n A	For a Keyblock LMK, the 'PVK Pair' is a double-length key, and must comply with the following: Key Usage: 'V2'; Algorithm: 'T'; Mode of Use: 'C', 'N'
Current PIN block	16 H	The Current PIN block encrypted under the PIN Block Key.
PIN Block format code	2 N	One of the valid PIN block format codes. If the security setting "Restrict PIN block usage for PCI HSM compliance" has the value "Y" then the PIN Block Format must be 01 (ISO format 0) or 47 (ISO format 3).
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
PVKI	1 N	The PVKI (should be between '0' and '6').
Current PVV	4 N	The PVV for the current PIN.
New PIN block	16 H	The New PIN block encrypted under the PIN Block Key.

Field	Length & Type	Details
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 the 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 Excluded PIN Length characters. Only present if the Excluded PIN Count > '00'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 exists in either global or local Excluded PIN Table 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.

PIN Verification Commands

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 9000 HSM provides the following host commands to support PIN verification operations:

Command	Page
Verify a Terminal PIN Using the IBM Method (DA)	94
Verify an Interchange PIN Using the IBM Method (EA)	97
Verify a Terminal PIN Using the Diebold Method (CG)	100
Verify an Interchange PIN Using the Diebold Method (EG)	102
Verify a Terminal PIN Using the VISA Method (DC)	104
Verify an Interchange PIN Using the VISA Method (EC)	106
Verify a Terminal PIN Using the Comparison Method (BC)	108
Verify an Interchange PIN Using the Comparison Method (BE)	110

Verify a Terminal PIN Using the IBM Method

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 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 3-DES 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 3-DES Keyblock LMK) or 'L' + 32 hexadecimal digits (for an AES Keyblock 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		The TPK under which the PIN block is encrypted.
	16 H or 1 A + 32/48 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 1 A + n A	For a Keyblock LMK, the 'TPK' must comply with the following: Key Usage: 'P0', '71'; Algorithm: 'D', 'T'; Mode of Use: 'B', 'D', 'N'
PVK		The PVK used to verify the PIN.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.
	or 1 A + n A	For a Keyblock LMK, the 'PVK' must comply with the following: Key Usage: 'V1'; Algorithm: 'D', 'T'; Mode of Use: 'C', 'V', 'N'
Maximum PIN Length	2 N	Value '12'.
PIN block	16 H	The PIN block encrypted under the TPK.
PIN block format code	2 N	One of the valid PIN block format codes.
Check Length	2 N	The minimum PIN length.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
Decimalization Table	16 N or 16 H or 1 A + 3 H or 1 A + 32 H	16 N when using Plaintext decimalization tables. 16 H when using Encrypted decimalization tables and a Variant LMK or 3-DES Keyblock 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 Keyblock LMK.
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 account number; 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'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.

Field	Length & Type	Details
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	'00' : No error '01' : PIN verification failure '02' : Warning PVK not single length (See the notes at the start of this section.) '10' : TPK parity error '11' : PVK 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 IBM Method

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 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 3-DES 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 3-DES Keyblock LMK) or 'L' + 32 hexadecimal digits (for an AES Keyblock 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		The ZPK under which the PIN block is encrypted.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'ZPK' must be encrypted under LMK pair 06-07.
	or 1 A + n A	For a Keyblock LMK, the 'ZPK' must comply with the following: Key Usage: 'P0', '72'; Algorithm: 'D', 'T'; Mode of Use: 'B', 'D', 'N'
PVK		The PVK used to verify the PIN.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.
	or 1 A + n A	For a Keyblock LMK, the 'PVK' must comply with the following: Key Usage: 'V1'; Algorithm: 'D', 'T'; Mode of Use: 'C', 'V', 'N'
Maximum PIN Length	2 N	Value '12'.
PIN block	16 H	The PIN block encrypted under the ZPK.
PIN block format code	2 N	One of the valid PIN block format codes.
Check Length	2 N	The minimum PIN length.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
Decimalization Table	16 N or 16 H or 1 A + 3 H or 1 A + 32 H	16 N when using Plaintext decimalization tables. 16 H when using Encrypted decimalization tables and a Variant LMK or 3-DES Keyblock 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 Keyblock LMK.
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 account number; 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'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'EB'.
Error Code	2 A	'00' : No error '01' : PIN verification failure '02' : Warning PVK not single length (See notes at start of this section.) '10' : ZPK parity error '11' : PVK 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 Diebold Method

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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		The TPK under which the PIN block is encrypted.
	16 H or 1 A + 32/48 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 1 A + n A	For a Keyblock LMK, the 'TPK' must comply with the following: **Key Usage**: 'P0', '71' **Algorithm**: 'D', 'T' **Mode of Use**: '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	The PIN block encrypted under the TPK.
PIN block format code	2 N	One of the valid PIN block format codes.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
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 account number. The data must be right-justified and padded with F.

Field	Length & Type	Details
Offset	4 N	PIN offset.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 '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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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		The ZPK under which the PIN block is encrypted.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'ZPK' must be encrypted under LMK pair 06-07.
	or 1 A + n A	For a Keyblock LMK, the 'ZPK' must comply with the following: **Key Usage**: 'P0', '72'; **Algorithm**: 'D', 'T'; **Mode of Use**: '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	The PIN block encrypted under the ZPK.
PIN block format code	2 N	One of the valid PIN block format codes.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
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 account number. The data must be right-justified and padded with F.
Offset	4 N	PIN offset.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be

Field	Length & Type	Details
		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 '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 VISA Method

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: Verify a PIN from a local ATM (or PIN pad etc.) using the VISA 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		The TPK under which the PIN block is encrypted.
	16 H or 1 A + 32/48 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 1 A + n A	For a Keyblock LMK, the 'TPK' must comply with the following: **Key Usage**: 'P0', '71'; **Algorithm**: 'D', 'T'; **Mode of Use**: 'B', 'D', 'N'
PVK Pair		The two PVKs, used to generate the PVV.
	32 H or 1 A + 32 H	For a Variant LMK, each PVK in the 'PVK Pair' must be encrypted under LMK pair 14-15 variant 0.
	or 1 A + n A	For a Keyblock LMK, the 'PVK Pair' is a double-length key, and must comply with the following: **Key Usage**: 'V2'; **Algorithm**: 'T'; **Mode of Use**: 'C', 'V', 'N'
PIN block	16 H	The PIN block encrypted under the TPK.
PIN block format code	2 N	One of the valid PIN block format codes.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
PVKI	1 N	The PVKI (should be between '0' and '6').
PVV	4 N	The PVV for the PIN.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 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 VISA Method

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: Verify a PIN from interchange using the VISA PVV method.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'EC'.
ZPK		The ZPK under which the PIN block is encrypted.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'ZPK' must be encrypted under LMK pair 06-07.
	or 1 A + n A	For a Keyblock LMK, the 'ZPK' must comply with the following: **Key Usage**: 'P0', '72'; **Algorithm**: 'D', 'T'; **Mode of Use**: 'B', 'D', 'N'
PVK Pair		The two PVKs, used to generate the PVV.
	32 H or 1 A + 32 H	For a Variant LMK, each PVK in the 'PVK Pair' must be encrypted under LMK pair 14-15 variant 0.
	or 1 A + n A	For a Keyblock LMK, the 'PVK Pair' is a double-length key, and must comply with the following: **Key Usage**: 'V2'; **Algorithm**: 'T'; **Mode of Use**: 'C', 'V', 'N'
PIN block	16 H	The PIN block encrypted under the ZPK.
PIN block format code	2 N	One of the valid PIN block format codes.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
PVKI	1 N	The PVKI (should be between '0' and '6').
PVV	4 N	The PVV for the PIN.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 '27' : PVK not double length '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 Comparison Method

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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		The TPK under which the PIN block is encrypted.
	16 H or 1 A + 32/48 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 1 A + n A	For a Keyblock LMK, the 'TPK' must comply with the following: **Key Usage**: 'P0', '71'; **Algorithm**: 'D', 'T'; **Mode of Use**: 'B', 'D', 'N'
PIN block	16 H	The PIN block containing the PIN for verification; encrypted under the TPK.
PIN block format code	2 N	One of the valid PIN block format codes.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
PIN	L N or L H or 1 A + 32 H	The PIN from the host database, encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' followed by 32 hex digits.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: Verify a PIN received from interchange 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 'BE'.
ZPK		The ZPK under which the PIN block is encrypted.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'ZPK' must be encrypted under LMK pair 06-07.
	or 1 A + n A	For a Keyblock LMK, the 'ZPK' must comply with the following: **Key Usage**: 'P0', '72'; **Algorithm**: 'D', 'T'; **Mode of Use**: 'B', 'D', 'N'
PIN block	16 H	The PIN block containing the PIN for verification; encrypted under the ZPK.
PIN block format code	2 N	One of the valid PIN block format codes.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
PIN	L N or L H or 1 A + 32 H	The PIN from the host database, encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' followed by 32 hex digits.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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.

PIN Translation Commands

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 payShield 9000 HSM provides the following host commands to support PIN translation operations:

Command	Page
Translate a PIN from One ZPK to Another (CC)	113
Translate a PIN from TPK to ZPK/BDK (3-DES DUKPT) Encryption (CA)	115
Translate a PIN from ZPK to LMK Encryption (JE)	118
Translate a PIN from TPK to LMK Encryption (JC)	120
Translate a PIN from LMK to ZPK Encryption (JG)	122
Translate PIN Algorithm (BQ)	124
Translate Account Number for LMK-encrypted PIN (QK)	125
Translate a PIN from BDK to BDK or ZPK Encryption (3-DES DUKPT) (G0)	321

Translate a PIN from One ZPK to Another

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'CC'.
Source ZPK		The ZPK under which the PIN block is currently encrypted.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'Source ZPK' must be encrypted under LMK pair 06-07.
	or 1 A + n A	For a Keyblock LMK, the 'Source ZPK' must comply with the following: **Key Usage**: 'P0', '72'; **Algorithm**: 'D', 'T'; **Mode of Use**: 'B', 'D', 'N'
Destination ZPK		Destination ZPK under which the PIN block is to be encrypted.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'Destination ZPK' must be encrypted under LMK pair 06-07.
	or 1 A + n A	For a Keyblock LMK, the 'Destination ZPK' must comply with the following: **Key Usage**: 'P0', '72'; **Algorithm**: 'D', 'T'; **Mode of Use**: 'B', 'E', 'N'
Maximum PIN Length	2 N	Value '12'.
Source PIN block	16 H	The source PIN block encrypted under the source ZPK.
Source PIN block format	2 N	The format code for the source PIN block.
Destination PIN block format	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 Chapter 10 of the General Information Manual on PCI HSM Compliance.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by

Field	Length & Type	Details
		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 '68' : Command disabled '69' : PIN Block format has been disabled or a standard error code.
PIN Length	2 N	Length of the returned PIN.
Destination PIN block	16 H	The destination PIN block encrypted under the destination ZPK.
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 (3-DES DUKPT) Encryption

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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.

Notes: The PIN block format may also be changed.
The ANSI X9.24-1:2009 method for DUKPT PIN Key derivation is used.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'CA'.
Source TPK		The TPK under which the PIN block is currently encrypted.
	16 H or 1 A + 32/48 H	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".
	or 1 A + n A	For a Keyblock LMK, the 'Source TPK' must comply with the following: **Key Usage**: 'P0', '71' **Algorithm**: 'D', 'T' **Mode of Use**: 'B', 'D', '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. Value '~' (X'7E). Optional; if present, this flag indicates that the destination key is a BDK-2.

Field	Length & Type	Details
Destination Key		The key under which the PIN block is to be encrypted. Three types of keys are supported: ZPK, BDK-1 and BDK-2.
	16/32 H or 1 A + 16/32/48 H	For a Variant LMK: If 'Destination Key Flag' is not present, then this key must be a ZPK, encrypted under LMK 06-07. If 'Destination Key Flag' is '*', then this key must be a BDK-1, encrypted under LMK 28-29. If 'Destination Key Flag' is '~', then this key must be a BDK-2, encrypted under LMK 28-29/6.
	or 1 A + n A	For a Keyblock LMK: This key must be either a ZPK or BDK-1 or BDK-2, and comply with the following: Key Usage: 'P0', '72'; Algorithm: 'D', 'T'; Mode of Use: 'B', 'E', 'N' Key Usage: '80', '41'; Algorithm: 'T'; Mode of Use: '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	The source PIN block encrypted under the source TPK.
Source PIN block format	2 N	The format code for the source PIN block.
Destination PIN block format	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 Chapter 10 of the General Information Manual on PCI HSM Compliance.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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.

Field	Length & Type	Details
Response Code	2 A	Value 'CB'.
Error Code	2 A	'00' : No error '10' : Source TPK parity error '11' : Destination ZPK parity error '68' : Command disabled '69' : PIN Block format has been disabled or a standard error code.
PIN Length	2 N	Length of the returned PIN.
Destination PIN block	16 H	The destination PIN block encrypted under the destination ZPK.
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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: Translate a PIN from encryption under a ZPK to encryption under the LMK.

Notes: 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.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'JE'.
Source ZPK		The ZPK under which the PIN block is currently encrypted.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'Source ZPK' must be encrypted under LMK pair 06-07.
	or 1 A + n A	For a Keyblock LMK, the 'Source ZPK' must comply with the following: **Key Usage**: 'P0', '72'; **Algorithm**: 'D', 'T'; **Mode of Use**: 'B', 'D', 'N'
PIN block	16 H	The source PIN block encrypted under the ZPK.
PIN block format code	2 N	One of the valid PIN block format codes.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 1 A + 32 H	The PIN encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: Translate a PIN from encryption under a TPK to encryption under the LMK.

Notes: 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. Thus the LMK-encrypted PIN changes when the account number is changed.

Field	Length & Type	Details
		COMMAND MESSAGE
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'JC'.
Source TPK		The TPK under which the PIN block is currently encrypted.
	16 H or 1 A + 32/48 H	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".
	or 1 A + n A	For a Keyblock LMK, the 'Source TPK' must comply with the following: Key Usage: 'P0', '71'; Algorithm: 'D', 'T'; Mode of Use: 'B', 'D', 'N'
PIN block	16 H	The source PIN block encrypted under the TPK.
PIN block format code	2 N	One of the valid PIN block format codes.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 1 A + 32 H	The PIN encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC024 or LIC025**	
Authorization: **Not required**	

Function: Translate a PIN from encryption under the LMK to encryption under a ZPK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'JG'.
Destination ZPK		The ZPK under which the PIN block is to be encrypted.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'Destination ZPK' must be encrypted under LMK pair 06-07.
	or 1 A + n A	For a Keyblock LMK, the 'Destination ZPK' must comply with the following: Key Usage: 'P0', '72'; Algorithm: 'D', 'T'; Mode of Use: 'B', 'E', 'N'
PIN block format code	2 N	One of the valid PIN block format codes.
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
PIN	L N or L H or 1 A + 32 H	The PIN encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' followed by 32 hex digits.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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	The 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.

Translate PIN Algorithm

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 3-DES Keyblock 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'.
Account Number	12 N	The 12 right-most digits of the account number, 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 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
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: 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.

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 1 A + 32 H	The PIN encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' followed by 32 hex digits.
Old Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the old account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the old account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
New Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the new account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the new account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 '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 1 A + 32 H	The PIN encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' 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.

PIN Mailer Printing Commands

The payShield 9000 HSM 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 9000 returns check data to the Host to give confidence that the data printed on the mailer is correct (i.e., the payShield 9000 has performed the correct cryptographic functions).

To configure the printer, use the CP (Configure Printer) console command.

The payShield 9000 HSM provides the following host commands to support PIN mailer printing operations:

Command	Page
Print PIN/PIN and Solicitation Data (PE)	128
Print a PIN Solicitation Mailer (OA)	130
Verify PIN/PIN and Solicitation Mailer Cryptography (PG)	132
Verify Solicitation Mailer Cryptography (RC)	133
Print TMK Mailer (TA)	134

Print PIN/PIN and Solicitation Data

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC027**	
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 9000. 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
Account Number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN	L N or L H or 1 A + 32 H	The PIN encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' 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 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.
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 ☑	Keyblock LMK ☑
License: **HSM9-LIC027**	
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 9000. 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 '0A'.
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.
Account Number	12 N	The 12 right-most digits of the account number, 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 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 '0B'.
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.
RESPONSE MESSAGE (after printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value '0Z'.
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.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify PIN/PIN and Solicitation Mailer Cryptography

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
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'.
Account Number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN	L N or L H or 1 A + 32 H	The PIN encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' 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 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.

Field	Length & Type	Details

Verify Solicitation Mailer Cryptography

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
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'.
Account Number	12 N	The 12 right-most digits of the account number, 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 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.

Print TMK Mailer

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC027**	
Authorization: **Required** Activity: **command.ta.host**	

Function: Print the TMK at the HSM-attached terminal.

Notes: A printer must be attached to the HSM, and the print format must have been defined.
The clear TMK will be positioned in the mailer at the location of the '^P' symbol defined by the print format.

This command uses an extended specification of Print Formatting Symbols to provide up to 32 different fields:

^00 = Insert Print Field #0

^01 = Insert Print Field #1

…

^1F = Insert Print Field #31

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'TA'.
TMK	16 H or 1 A + 32/48 H	The Terminal Master 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 LMK pair 36-37 variant 8 if the setting has the value "Y".
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 in 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 the '%' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'TB'.
Error Code	2 A	'00' : No error '10' : TMK 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.
RESPONSE MESSAGE (after printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'TZ'.
Error Code	2 A	'00' : No error '16' : Printer time out '68' : Command disabled or a standard error code.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.

PIN Solicitation Data Processing Commands

The payShield 9000 HSM provides the following host commands to support solicitation data entry operations:

Command	Page
Load Solicitation Data to User Storage (QA)	137
Final Load of Solicitation Data to User Storage (QC)	139

Load Solicitation Data to User Storage

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
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 using the CS Console command or the HSM Manager *Initial Settings* dialogue box. 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
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.

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 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.

Clear PIN Commands

CAUTION!

THE USE OF CLEAR PIN FACILITIES PRESENTS A SIGNIFICANT SECURITY RISK.

The payShield 9000 HSM provides the following host commands to support clear PIN operations:

Command	Page
Encrypt a Clear PIN (BA)	142
Decrypt an Encrypted PIN (NG)	143

Encrypt a Clear PIN

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC024** or **LIC025**	
Authorization: **Required** Activity: **pin.clear.host**	

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 X'F to the maximum PIN length L. Value set with the CS (Configure Security) console command (range 5 – 13).
Account Number	12 N	The 12 right-most digits of the account number, excluding the check digit.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 1 A + 32 H	The PIN encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
Authorization: **Required** Activity: **pin.clear.host**	

Function: Decrypt an encrypted PIN and return a reference number.

Notes: The command is available only if selected during configuration by enabling the setting "*Select clear PINs?*" (CS Console command) or "*Enable clear PINs?*" (HSM Manager Initial Settings).
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'.
Account Number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN	L N or L H or 1 A + 32 H	The PIN encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' followed by 32 hex digits.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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'.
Reference number	12 N	The reference number derived by encrypting the account number 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.

Watchword Commands

The payShield 9000 HSM provides the following host commands to support general Watchword operations:

Command	Page
Verify a Watchword Response (FU)	145
Generate a Decimal MAC (LK)	147
Verify a Decimal MAC (LM)	149

Verify a Watchword Response

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC005**	
Authorization: **Not required**	

Function: Verify a Watchword response.

Notes: The cipher scheme used depends upon the key length.
Single length WWK – Cipher scheme code 0
Double length WWK – Cipher scheme code 1
Triple length WWK – Cipher scheme code 2

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FU'.
WWK		The Watchword Key, used to generate the response.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'WWK' must be encrypted under LMK pair 22-23.
	or 1 A + n A	For a Keyblock LMK, the 'WWK' must comply with the following: **Key Usage**: '01'; **Algorithm**: 'D', 'T'; **Mode of Use**: 'C', 'V', 'N'
Flag	1 N	'1' : response for PIN 1 '2' : response for PIN 2.
Challenge	7 N	Watchword challenge.
Response	7 N	Watchword response.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'FV'.
Error Code	2 A	'00' : No error '01' : Watchword Response verification failure '10' : WWK 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.

Generate a Decimal MAC

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC005**	
Authorization: **Not required**	

Function: Generate a Decimal MAC on data.

Notes: This command assumes that the data on which the MAC is to be generated consists of characters only.
The cipher scheme used depends upon the key length.
Single length TAK – Cipher scheme code 0 (X9.9 MAC)
Double length TAK – Cipher scheme code 1 (X9.19 MAC)

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'LK'.
TAK		The Terminal Authentication Key, used to generate the MAC.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'TAK' must be encrypted under LMK pair 16-17.
	or 1 A + n A	For a Keyblock LMK, the 'TAK' must comply with one of the following: **Key Usage** / **Algorithm** / **Mode of Use** 'M1' / 'D' / 'C', 'G', 'N' 'M3' / 'T' / 'C', 'G', 'N'
MAC Length	1 H	Number of characters required in Decimal MAC (range 1 to 12).
Data	0 - n	The data on which a MAC is to be generated, n = 16K Must not contain a '~' 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 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 'LL'.
Error Code	2 A	'00' : No error '10' : TAK parity error '68' : Command disabled or a standard error code.
MAC	n N	The calculated decimal MAC with a length as specified in the 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.

Verify a Decimal MAC

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC005**	
Authorization: **Not required**	

Function: To verify a decimal MAC of user defined length

Notes: This command assumes that the data on which the MAC is to be generated consists of characters only
The cipher scheme used depends upon the key length.
Single length TAK – Cipher scheme code 0 (X9.9 MAC)
Double length TAK – Cipher scheme code 1 (X9.19 MAC)

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'LM'.
TAK		The Terminal Authentication Key, used to verify the MAC.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'TAK' must be encrypted under LMK pair 16-17.
	or 1 A + n A	For a Keyblock LMK, the 'TAK' must comply with one of the following: **Key Usage** / **Algorithm** / **Mode of Use** 'M1' / 'D' / 'C', 'V', 'N' 'M3' / 'T' / 'C', 'V', 'N'
MAC length	1 H	The number of characters in the Decimal MAC (range 1 – 12).
MAC	n N	The MAC to be verified.
Data	0 - n	The data on which the MAC to be verified was calculated, n = 16K Must not contain a '~' 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 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 'LN'.
Error Code	2 A	'00' : No error '01' : MAC verification failure '10' : TAK 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.

Message Authentication Code Commands

The payShield 9000 HSM 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 9000 HSM provides the following host commands to support generic MAC operations:

Command	Page
Generate MAC (M6)	152
Verify MAC (M8)	155
Verify and Translate MAC (MY)	158

Note: Other (legacy) MAC commands exist – see Legacy Commands (page 385).

Generate MAC

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC008**	
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.

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.

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' … '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

Field	Length & Type	Details
		with length, pad with 0x00). For MAC Algorithm values '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) For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
Key	16 H or 1 A + 32/48 H or 1 A + n A	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. For a Keyblock LMK, the 'Key' must comply with one of the following:

Key Usage	Algorithm	Mode of Use
'M1'	'D'	'C', 'G', 'N'
'M3'	'T'	'C', 'G', 'N'
'M5', 'M6'	'A'	'C', 'G', 'N'

IV	16 H or 32 H	The intermediate IV. When MACing the middle or final blocks of a series of blocks, this should be the IV returned from MACing the previous block. If using a DES/3-DES 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 or n A	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. 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 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/3-DES 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	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 ☑	Keyblock LMK ☑
License: **HSM9-LIC008**	
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.

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.

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' … '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.

Field	Length & Type	Details
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). For MAC Algorithm values '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) For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
Key		The Message Authentication Key, used in conjunction with the IV, if appropriate, to verify the MAC.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'Key' is either a TAK or ZAK, as specified above.
	or 1 A + n A	For a Keyblock LMK, the 'Key' must comply with one of the following: Key Usage: 'M1' — Algorithm: 'D' — Mode of Use: 'C', 'V', 'N' Key Usage: 'M3' — Algorithm: 'T' — Mode of Use: 'C', 'V', 'N' Key Usage: 'M5', 'M6' — Algorithm: 'A' — Mode of Use: 'C', 'V', 'N'
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/3-DES 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		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:
	n B or	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.
	n H or	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.
MAC	8 H or 16 H	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'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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	'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.
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/3-DES 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'.
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 ☑	Keyblock LMK ☑
License: **HSM9-LIC008**	
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.

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.

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.)

Field	Length & Type	Details
		'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). For Source MAC Algorithm values '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 Keyblock LMK: This field is ignored; should be set to 'FFF'.
Source Key		The Source Message Authentication Key, used in conjunction with the Source IV, if appropriate, to verify the supplied MAC.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'Source Key' is either a TAK or ZAK, as specified above.
	or 1 A + n A	For a Keyblock LMK, the 'Source Key' must comply with one of the following: <table><tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr><tr><td>'M1'</td><td>'D'</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></table>
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). For Destination MAC Algorithm values '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:

Field	Length & Type	Details
		'003' : TAK (encrypted under LMK pair 16-17) '008' : ZAK (encrypted under LMK pair 26-27)
		For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
Destination Key		The Destination Message Authentication Key, used in conjunction with the Destination IV, if appropriate, to generate the new MAC.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'Destination Key' is either a TAK or ZAK, as specified above.
	or 1 A + n A	For a Keyblock LMK, the 'Destination Key' must comply with one of the following: Key Usage: 'M1', 'M3', 'M5', 'M6' Algorithm: 'D', 'T', 'A' Mode of Use: '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/3-DES 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/3-DES 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.
Message		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:
	n B or	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.
	n H or	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.
	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.
Source MAC	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.

Field	Length & Type	Details
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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/3-DES 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/3-DES 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.

Message Encryption Commands

The payShield 9000 HSM provides the following host commands to support message encryption operations:

Command	Page
Encrypt Data Block (M0)	164
Decrypt Data Block (M2)	168
Translate Data Block (M4)	172

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 latest revision of the DUKPT standard (X9.24-1:2009) 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 type-1 BDK supports 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 type-2 BDK supports the unidirectional method.
  - A further BDK type (type-3) is supported, in which case the data encryption or decryption key is derived from the BDK using the 'PIN verification' variant.

  The differences between the types of BDKs are summarised in the table below.

  Further Information about DUKPT and its implementation on the payShield 9000 can be found in:

  - Chapter 4 of 1270A542 payShield 9000 Host Programmer's Manual
  - Chapter 13 of 1270A593 payShield 9000 General Information Manual.

BDKs used with Message Encryption Commands

<table>
<tr><th colspan="2">BDK Type</th><th>Description</th></tr>
<tr><td rowspan="2">Type-1</td><td>For a Variant LMK, the BDK is encrypted under LMK 28-29.</td><td rowspan="2">Variants are applied to the derived transaction key as follows:
<table>
<tr><th>Key function</th><th>Variant</th></tr>
<tr><td>Decrypting "request" data</td><td>00 00 00 00 00 FF 00 00</td></tr>
<tr><td>Encrypting "response" data</td><td>00 00 00 00 00 FF 00 00</td></tr>
</table>
Note that this method will produce bidirectional encryption keys.</td></tr>
<tr><td>For a Keyblock LMK, the BDK must have Key Usage = 'B0'.</td></tr>
<tr><td rowspan="2">Type-2</td><td>For a Variant LMK, the BDK is encrypted under LMK 28-29 variant 6.</td><td rowspan="2">Variants are applied to the derived transaction key as follows:
<table>
<tr><th>Key function</th><th>Variant</th></tr>
<tr><td>Decrypting "request" data</td><td>00 00 00 00 00 FF 00 00</td></tr>
<tr><td>Encrypting "response" data</td><td>00 00 00 FF 00 00 00 00</td></tr>
</table>
Note that this method will produce unidirectional encryption keys.</td></tr>
<tr><td>For a Keyblock LMK, the BDK must have Key Usage = '41'.</td></tr>
<tr><td rowspan="2">Type-3</td><td>For a Variant LMK, the BDK is encrypted under LMK 28-29 variant 8.</td><td rowspan="2">Variants are applied to the derived transaction key as follows:
<table>
<tr><th>Key function</th><th>Variant</th></tr>
<tr><td>Decrypting "request" data</td><td>00 00 00 00 00 00 00 FF</td></tr>
<tr><td>Encrypting "response" data</td><td>00 00 00 00 00 00 00 FF</td></tr>
</table>
Note that this method will produce bidirectional encryption keys.</td></tr>
<tr><td>For a Keyblock LMK, the BDK must have Key Usage = '42'.</td></tr>
</table>

Encrypt Data Block

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC008**	
Authorization: **Not required**	

Function: Encrypt a block of data.

Notes: The encryption key may be a BDK. This command supports type-1 BDKs, type-2 BDKs and type-3 BDKs. Note that a BDK must be a double-length key.

If a BDK is supplied, then the DUKPT method (as defined in X9.24-1:2009) will be used to determine the encryption key. This command supports both bidirectional and unidirectional encryption keys, but always assumes that the data is "response" data.For further information on the use of BDKs with message encryption commands, please refer to the table on page 163.

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.

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.

Note: 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.

Note: No padding is applied – the input message must be a multiple of 8 (or 16 for hex-encoded messages).

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	Describes the encryption mode: '00' : ECB '01' : CBC (requires IV) '02' : CFB8 (requires IV) '03' : CFB64 (requires IV).
Input Format Flag	1 N	Describes the format of the input message: '0' : Binary '1' : Hex-Encoded Binary '2' : Text.

<table>
<tr><th>Field</th><th>Length & Type</th><th>Details</th></tr>
<tr><td>Output Format Flag</td><td>1 N</td><td>Describes the format of the output message:
'0' : Binary
'1' : Hex-Encoded Binary.</td></tr>
<tr><td>Key Type</td><td>3 H</td><td>For a Variant LMK:
Indicates the key type of the key to be used. The following key types are permitted:
'009' : type-1 BDK (encrypted under LMK pair 28-29)
'609' : type-2 BDK (encrypted under LMK pair 28-29/6)
'809' : type-3 BDK (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)
For a Keyblock LMK:
This field is ignored; should be set to 'FFF'.</td></tr>
<tr><td>Key</td><td></td><td>The encryption Key, used in conjunction with the IV, if appropriate, to encrypt the supplied Message.</td></tr>
<tr><td></td><td>16 H
or
1 A + 16/32/48 H</td><td>For a Variant LMK, the 'Key' is a BDK, ZEK, DEK or TEK, as specified above.</td></tr>
<tr><td></td><td>or
1 A + n A</td><td>For a Keyblock LMK, the 'Key' must comply with one of the following:
<table>
<tr><th>Key Usage</th><th>Algorithm</th><th>Mode of Use</th></tr>
<tr><td>'B0', '41', '42'</td><td>'T'</td><td>'B', 'E', 'N'</td></tr>
<tr><td>'D0', '21', '22', '23'</td><td>'D', 'T', 'A'</td><td>'B', 'E', 'N'</td></tr>
</table></td></tr>
<tr><td>KSN Descriptor</td><td>3 H</td><td>The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information.
Only present if Key Type is a BDK.</td></tr>
<tr><td>Key serial number</td><td>12 - 20 H</td><td>The KSN supplied by the PIN pad, including the transaction counter. See the Host Programmer Manual for further information.
Only present if Key Type is a BDK.</td></tr>
<tr><td>IV</td><td>16 H
or
32 H</td><td>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/3-DES 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' or '03'.</td></tr>
<tr><td>Message Length</td><td>4 H</td><td>The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes.
This must be a multiple of 8 for binary and text formatted messages, or a multiple of 16 for hex-encoded binary messages.</td></tr>
</table>

Field	Length & Type	Details
Message		The message to be encrypted. The length & type of the field will depend on the value of the Input Format Flag:
	n B or	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..
	n H or	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..
	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 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	'00' : No error '02' : Invalid Mode Flag field '03' : Invalid Input Format Flag field '04' : Invalid Output Format Flag field '05' : Invalid Key Type field '06' : Invalid Message Length field '10' : Encryption Key Parity Error '35' : Illegal Message Format '67' : Command not licensed '68' : Command disabled or a standard error code.
IV	16 H or 32 H	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/3-DES 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 or 03.
Message Length	4 H	The length of the following field, in bytes.
Encrypted Message		The encrypted message. The length & type of the field will depend on the value of the Output Format Flag:
	n B or	Output 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..
	n H	Output 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..
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 ☑	Keyblock LMK ☑
License: **HSM9-LIC008**	
Authorization: **Not required**	

Function: Decrypt a block of data.

Notes: The decryption key may be a BDK. This command supports type-1 BDKs, type-2 BDKs and type-3 BDKs. Note that a BDK must be a double-length key.

If a BDK is supplied, then the DUKPT method (as defined in X9.24-1:2009) of key derivation will be used to determine the decryption key. This command supports both bidirectional and unidirectional decryption keys, but always assumes that the data is "request" data.

For further information on the use of BDKs with message encryption commands, please refer to the table on page 163.

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.
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.
Note: 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.

Note: No padding is applied – the input message must be a multiple of 8 (or 16 for hex-encoded messages).

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	Describes the decryption mode: '00' : ECB '01' : CBC (requires IV) '02' : CFB8 (requires IV) '03' : CFB64 (requires IV).

Field	Length & Type	Details
Input Format Flag	1 N	Describes the format of the input message: '0' : Binary '1' : Hex-Encoded Binary
Output Format Flag	1 N	Describes the format of the output message: '0' : Binary '1' : Hex-Encoded Binary '2' : Text.
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' : type-1 BDK (encrypted under LMK pair 28-29) '609' : type-2 BDK (encrypted under LMK pair 28-29/6) '809' : type-3 BDK (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). For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
Key		The decryption Key, used in conjunction with the IV, if appropriate, to decrypt the supplied Message.
	16 H or 1 A + 16/32/48 H	For a Variant LMK, the 'Key' is a BDK, ZEK, DEK or TEK, as specified above.
	or 1 A + n A	For a Keyblock LMK, the 'Key' must comply with one of the following: Key Usage: 'B0', '41', '42' — Algorithm: 'T' — Mode of Use: 'B', 'D', 'N' Key Usage: 'D0', '21', '22', '23' — Algorithm: 'D', 'T', 'A' — Mode of Use: 'B', 'D', 'N'
KSN Descriptor	3 H	The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information. Only present if Key Type is 'a BDK.
Key serial number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information. Only present if Key Type is a BDK.
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/3-DES 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' or '03'.
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes. This must be a multiple of 8 for binary formatted messages, or a multiple of 16 for hex-encoded binary messages.
Encrypted Message		The encrypted message. The type of the message will depend on the value of the Input Format Flag field:

Field	Length & Type	Details
	n B or n H	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..
Delimiter LMK Identifier	1 A 2 N	Value '%'. Optional; if present, the following field must 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 'M3'.
Error Code	2 A	'00' : No error '02' : Invalid Mode Flag field '03' : Invalid Input Format Flag field '04' : Invalid Output Format Flag field '05' : Invalid Key Type field '06' : Invalid Message Length field '10' : Decryption Key Parity Error '35' : Illegal Message Format '67' : Command not licensed '68' : Command disabled 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/3-DES 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 or 03.
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 = '1' or '2', then n = multiple of 8 when using a DES key, or a multiple of 16 when using an AES key.. Output 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.. Output 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..
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.

Field	Length & Type	Details
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate Data Block

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC008**	
Authorization: **Not required**	

Function: Translate a block of data from encryption under one key, to encryption under another key.

Notes: 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.
Either the source key or the destination key (but not both) may be a BDK. This command supports type-1 BDKs, type-2 BDKs and type-3 BDKs. Note that a BDK must be a double-length key.

If the source key is a BDK, then the DUKPT (as defined X9.24-1:2009) 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 163.

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	'00' : ECB '01' : CBC (requires IV) '02' : CFB8 (requires IV) '03' : CFB64 (requires IV).
Destination Mode Flag	2 N	'00' : ECB '01' : CBC (requires IV) '02' : CFB8 (requires IV) '03' : CFB64 (requires IV).

Field	Length & Type	Details
Input Format Flag	1 N	'0' : Binary '1' : Hex-Encoded Binary.
Output Format Flag	1 N	'0' : Binary '1' : Hex-Encoded Binary.
Source Key Type	3 H	For a Variant LMK: Indicates the source (decryption) key type of the key to be used. The following key types are permitted: '009' : type-1 BDK (encrypted under LMK pair 28-29) '609' : type-2 BDK (encrypted under LMK pair 28-29/6) '809' : type-3 BDK (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).
		For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
Source Key		The Source (decryption) Key, used in conjunction with the IV, if appropriate, to decrypt the supplied Message.
	16 H or 1 A + 16/32/48 H	For a Variant LMK, the 'Source Key' is a BDK, ZEK, DEK or TEK, as specified above.
	or 1 A + n A	For a Keyblock LMK, the 'Source Key' must comply with one of the following: Key Usage: 'B0', '41', '42'; Algorithm: 'T'; Mode of Use: 'B', 'D', 'N' Key Usage: 'D0', '21', '22', '23'; Algorithm: 'D', 'T', 'A'; Mode of Use: 'B', 'D', '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 Source Key Type is a BDK.
Source Key serial number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information. Only present if Source Key Type is a BDK.
Destination Key Type	3 H	For a Variant LMK: Indicates the destination (encryption) key type of the key to be used. The following key types are permitted: '009' : type-1 BDK (encrypted under LMK pair 28-29) '609' : type-2 BDK (encrypted under LMK pair 28-29/6) '809' : type-3 BDK (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)
		For a Keyblock LMK: This field is ignored; should be set to 'FFF'.
Destination Key		The Destination (encryption) Key, used in conjunction with the IV, if appropriate, to re-encrypt the decrypted Message.
	16 H or 1 A + 16/32/48 H	For a Variant LMK, the 'Destination Key' is a BDK, ZEK, DEK or TEK, as specified above.
	or 1 A + n A	For a Keyblock LMK, the 'Destination Key' must comply with one of the following: Key Usage: 'B0', '41', '42'; Algorithm: 'T'; Mode of Use: 'B', 'E', 'N' Key Usage: 'D0', '21', '22', '23'; Algorithm: 'D', 'T', 'A'; Mode of Use: 'B', 'E', 'N'

Field	Length & Type	Details
Destination KSN Descriptor	3 H	The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information. Only present if Destination Key Type is a BDK.
Destination Key serial number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information. Only present if Destination Key Type is a BDK.
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/3-DES 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/3-DES 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'.
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes. This must be a multiple of 8 for binary formatted messages, or a multiple of 16 for hex-encoded binary messages.
Encrypted Message		The message to be translated. The length & type of the field will depend on the value of the Input Format Flag:
	n B	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..
	n H	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..
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 Mode Flag 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/3-DES 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/3-DES 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'.
Message Length	4 H	The length of the following field, in bytes.
Translated Message		The translated message. The length & type of the field will depend on the value of the Output Format Flag:
	n B	Output 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..
	n H	Output 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..
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.

HMAC Commands

The payShield 9000 HSM provides the following host commands to support generic HMAC operations:

Command	Page
Generate an HMAC Secret Key (LO)	177
Generate an HMAC on a Block of Data (LQ)	180
Verify an HMAC on a Block of Data (LS)	182
Import an HMAC key under a ZMK (LU)	184
Export an HMAC key under a ZMK (LW)	188
Translate a HMAC Key from Old LMK to New LMK (LY)	191

Generate an HMAC Secret Key

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC005**	
Variant LMK	Authorization: **Determined by KTT(G)** Activity: **generate.hmac.host**
Keyblock 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 Keyblock 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 Keyblock 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 ≤ key length), where L is the size of the hash function output (so L = 20 in the case of SHA-1). See Note above.

Field	Length & Type	Details
COMMAND MESSAGE		
HMAC Key Format	2 N	Defines the format of the stored key. For a Variant LMK: '00' : Thales HMAC Key format. For a Keyblock LMK: '04' : Thales HMAC Keyblock format.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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.
Applies only when generating a keyblock.		
Delimiter	1 A	Value '#'. Required when generating a keyblock. If present, the following fields must be present.
Key Usage	2 A	Key Usage field, to be included in the keyblock 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 keyblock 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 keyblock 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 Chapter 5 of the General Information Manual.
Key Version Number	2 N	Key Version Number field, to be included in the keyblock 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 keyblock header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in Chapter 5 of the General Information Manual.
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	For a Variant LMK: Length (in bytes) of the next field.
	or 4 H	For a Keyblock LMK: This field is reserved, and set to 'FFFF'.
HMAC Key	n B or n A	The new HMAC Key. Note: the key is *not* 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 Keyblock 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC005**	
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 'LG'.
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 Keyblock 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 ≤ t ≤ 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 Keyblock LMK: '04' : Thales HMAC Keyblock format.
HMAC Key Length	4 N	For a Variant LMK: Length (in bytes) of the next field.
	or 4 H	For a Keyblock 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 *not* 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 Keyblock LMK, the 'HMAC Key' must comply with the following: **Key Usage**: '61' – '65'; **Algorithm**: 'H'; **Mode of Use**: 'C', 'G', 'N'
Delimiter	1 A	Value ';'.
Data Length	5 N	Length of message to be authenticated

Field	Length & Type	Details
COMMAND MESSAGE		
Message Data	n B	Data to be authenticated
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC005**	
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 Keyblock 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 ≤ t ≤ 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 Keyblock LMK: '04' : Thales HMAC Keyblock format.
HMAC Key Length	4 N	For a Variant LMK: Length (in bytes) of the next field.
	or 4 H	For a Keyblock LMK: This field is ignored; should be set to 'FFFF'.
HMAC Key	n B or n A	The HMAC Key, used to verify the supplied HMAC. Note: the key is *not* prefixed with a key scheme character.
		For a Variant LMK, the 'HMAC Key' is encrypted under the LMK pair 34-35 variant 1.

Field	Length & Type	Details
COMMAND MESSAGE		
		For a Keyblock LMK, the 'HMAC Key' must comply with the following: Key Usage: '61' – '65'; Algorithm: 'H'; Mode of Use: 'C', 'V', 'N'
Delimiter	1 A	Value ';'.
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 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC005**	
Variant LMK	Authorization: **Determined by KTT(I)** Activity: **import.10C.host**
Keyblock LMK	Authorization: **If import from non-KB** Activity: **import.10C.host**

Function: Import an HMAC under a Zone Master Key (ZMK).

Notes: The HMAC Key encrypted under the ZMK must be a multiple of 8 bytes. The HSM will extract the HMAC Key from the input key, ignoring any padding.
Transport Formats 01, 02 (PKCS#11) and 03 (X9.17) are only permitted if enabled using the console CS (Configure Security) command.

If Transport Format 03 (X9.17) is used then the plaintext HMAC Key must be an exact multiple of 8 bytes.

Importing an HMAC from Transport Format 04 (Thales Keyblock) is only permitted when using a Keyblock LMK.

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)'.
	16 / 32 H or 1 A + 32/48 H	For a Variant LMK, the 'ZMK' is encrypted under the LMK pair 04-05.
	or 1 A + n A	For a Keyblock LMK, the 'ZMK' must comply with the following: **Key Usage**: 'K0', '52'; **Algorithm**: 'D', 'T'; **Mode of Use**: 'B', 'D', 'N'
HMAC Key (ZMK) Length	4 N or 4 H	If Transport Format ≠ '04', this field specifies the length (in bytes) of the next field. If Transport Format = '04', this field is ignored; should be set to 'FFFF'.
HMAC Key (ZMK)	n B or n A	The HMAC Key to be imported, encrypted under the ZMK. Note: the key is *not* prefixed with a key scheme character.

Field	Length & Type	Details
COMMAND MESSAGE		
		If in Thales Keyblock format (Transport Format '04'), the 'HMAC Key (ZMK)' must comply with the following: Key Usage: '61' – '65'; Algorithm: 'H'; Mode of Use: 'C', 'G', 'V', 'N'
Delimiter	1 A	Value ';'. Only present if using a Variant LMK.
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 Keyblock format (not permitted for variant LMK).
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 Keyblock LMK: '04' : Thales HMAC Keyblock format.
Hash Identifier	2 N or 2 H	Only present if using a Variant LMK. 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 or 2 H	Only present if using a Variant LMK. Only present if Transport Format = '01', '02' or '03'. HMAC Key Usage value: '01' : HMAC Generation '02' : HMAC Verification '03' : HMAC Generation and Verification.
HMAC Key Length	4 N	Only present if using a Variant LMK. 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 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			
Applies only when generating a keyblock.	Delimiter	1 A	Value '#'. Required when importing to Thales keyblock 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 keyblock 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 keyblock 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 Chapter 5 of the General Information Manual.
	Key Version Number	2 N	Key Version Number field, to be included in the keyblock 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 keyblock header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in Chapter 5 of the General Information Manual. 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 Keyblock LMK: This field is reserved, and set to 'FFFF'.
HMAC Key (under LMK)	n B or n A	The imported HMAC key. Note: the key is *not* 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 Keyblock 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.

Export an HMAC key under a ZMK

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC005**	
Authorization: **Not required**	

Function: Export an HMAC under a Zone Master Key (ZMK).

Notes: The HMAC Key encrypted under the ZMK must be a multiple of 8 bytes. The HSM will add any necessary padding.
Transport Formats 01, 02 (PKCS#11) and 03 (X9.17) are only permitted if enabled using the Configure Security ("CS") command.

If Transport Format 03 (X9.17) is used then the HMAC Key Length must be an exact multiple of 8 bytes.

Exporting an HMAC to Transport Format 04 (Thales Keyblock) is only permitted when using a Keyblock LMK.

Field	Length & Type	Details
		COMMAND MESSAGE
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'LW'.
ZMK		The Zone Master Key, used to encrypt the 'HMAC Key'.
	16 / 32 H or 1 A + 32/48 H	For a Variant LMK, the 'ZMK' is encrypted under the LMK pair 04-05.
	or 1 A + n A	For a Keyblock LMK, the 'ZMK' must comply with the following: **Key Usage**: 'K0', '52'; **Algorithm**: 'D', 'T'; **Mode of Use**: '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 Keyblock LMK: '04' : Thales HMAC Keyblock format.
Transport Format	2 N	Format of plaintext 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 Keyblock format (not permitted for variant LMK).
HMAC Key (LMK) Length	4 N	For a Variant LMK: Length (in bytes) of the next field.
	or 4 H	For a Keyblock 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 *not* prefixed with a key scheme character.

Field	Length & Type	Details
COMMAND MESSAGE		
		For a Variant LMK, the 'HMAC Key' is encrypted under the LMK pair 34-35 variant 1. For a Keyblock LMK, the 'HMAC Key' must comply with the following: **Key Usage**: '61' - '65'; **Algorithm**: 'H'; **Mode of Use**: 'C', 'G', 'V', 'N'
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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.
$Keyblock_{LMK} \rightarrow Keyblock_{ZMK}$: Delimiter	1 A	Value '&'. Optional; can only be present when the exported key is keyblock; if present, the following field must be present.
$Keyblock_{LMK} \rightarrow Keyblock_{ZMK}$: 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.
HMAC Key (ZMK) Length	4 N or 4 H	If Transport Format ≠ '04', this field specifies the length (in bytes) of the next field. If Transport Format = '04', this field is ignored; should be set to 'FFFF'.
HMAC Key (ZMK)	n B or n A	The HMAC Key, encrypted under the ZMK, in the format defined by 'Transport Format'. Note: the key is *not* 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 ≤ key length, where L is the size of the hash function output (so L = 20 in the case of SHA-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.

Translate a HMAC Key from Old LMK to New LMK

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC005**	
Authorization: **Not required**	

Function: Translate an HMAC Key from encryption under an old LMK, held in key change storage, to encryption under a new LMK.

Notes: This command can also be used to change the format of the stored HMAC Key.

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 Keyblock LMK: '04' : Thales HMAC Keyblock 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 Keyblock LMK: '04' : Thales HMAC Keyblock format.
HMAC Key Length	4 N	For an old Variant LMK: Length (in bytes) of the next field.
	or 4 H	For an old Keyblock 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 *not* 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 Keyblock LMK, the 'HMAC Key' must comply with the following: Key Usage: '61' - '65'; Algorithm: 'H'; Mode of Use: 'C', 'G', 'V', 'N'
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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			
Applies only when translating from variant to keyblock.	Delimiter	1 A	Value '#'. Required when translating to Thales keyblock format. If present, the following fields must be present.
	Key Usage	2 A	Key Usage field, to be included in the keyblock 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 translating a key from format '00', this field must be compatible with the Hash Identifier of the input key.
	Mode of Use	1 A	Mode of Use field, to be included in the keyblock 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 Chapter 5 of the General Information Manual.
	Key Version Number	2 N	Key Version Number field, to be included in the keyblock 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 keyblock header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in Chapter 5 of the General Information Manual.
	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 'LZ'.
Error Code	2 A	'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.
HMAC Key Length	4 N	For a current Variant LMK: Length (in bytes) of the next field. For a current Keyblock LMK: This field is reserved, and set to 'FFFF'.
HMAC Key	n B or n A	The translated HMAC key, encrypted under the current LMK. Note: the key is *not* prefixed with a key scheme character. For a current Variant LMK, the 'HMAC Key' is encrypted under the LMK pair 34-35 variant 1. For a current Keyblock 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.

User Storage Commands

The payShield 9000 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 9000 HSM provides the following host commands to support user storage operations:

Command	Page
Load Data to User Storage (LA)	195
Read Data from User Storage (LE)	197
Verify the Diebold Table in User Storage (LC)	199

Load Data to User Storage

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
Authorization: **Not required**	

Function: Load data to user storage.

Notes: See Chapter 16 of the *payShield 9000 General Information Manual* for a decription of the User Storage capability.
Where the security setting *User storage key length* has been set to one of the Fixed Length values (S(ingle)=16 characters, D(ouble)=32 characters, or T(riple)=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 to fill the block.
Where the security setting *User storage key length* has been set to variable length (V(ariable)), 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'.
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.

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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
Authorization: **Not required**	

Function: Read data from user storage.

Notes: See Chapter 16 of the *payShield 9000 General Information Manual* for a decription of the User Storage capability.

Where the security setting *User storage key length* has been set to one of the Fixed Length values (S(ingle)=16 characters, D(ouble)=32 characters, or T(riple)=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 (V(ariable)), 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 S(ingle), D(ouble), or T(riple). 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 V(ariable).]*
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 'LF'.
Error Code		2 A	'00' : No error '68' : Command disabled or a standard error code.
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.
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 ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
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.
  - 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 '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 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.

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 9000. 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 *Print Formatting Symbols* section of the payShield 9000 Host Programmer's Manual.

The payShield 9000 HSM provides the following host commands to support print output formatting operations:

Command	Page
Load Formatting Data to HSM (PA)	201
Load Additional Formatting Data to HSM (PC)	202
Load a PIN Text String (LI)	203

Load Formatting Data to HSM

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC027**	
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 Print Formatting Symbols Tables in the *payShield 9000 Host Programmer's 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 '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 ☑	Keyblock LMK ☑
License: **HSM9-LIC027**	
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 Print Formatting Symbols Tables in the *payShield 9000 Host Programmer's 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 '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 ☑	Keyblock LMK ☑
License: **HSM9-LIC027**	
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.

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 storage of the old LMK within the HSM. This storage location is known as "Key Change Storage".

When the old LMK has been saved in key change storage, and the new LMK is loaded in the standard LMK 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 9000 HSM provides the following host commands to support LMK translation operations:

Command	Page
Translate a PIN and PIN Length (BG)	205
Translate Keys from Old LMK to New LMK (BW)	207
Erase the Key Change Storage (BS)	211

Translate a PIN and PIN Length

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC024** or **LIC025**	
Authorization: **Not required**	

Function: Translate a PIN and/or PIN length from encryption under the LMK pair held in "key change storage" to encryption under the current LMK. Also, translate the PIN length if a new value has been selected.

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 L_2N for PIN encryption algorithm A, and L_2H 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'.
Account Number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN	L_1 N or L_1 H	The PIN encrypted under the old LMK, where L_1 is the old encrypted PIN length.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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	The PIN encrypted under the current LMK, where L_2 is the new encrypted 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.

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

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
Authorization: **Not required**	

Function: This command can perform either or both of the following functions:

- Translate keys from encryption under the LMK held in "key change storage" to encryption under a new LMK.
- 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' Keyblock 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.
- See the table in Chapter 10 of the payShield 9000 General Information 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.

Field	Length & Type	Details
		COMMAND MESSAGE
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'BW'.
Key Type code	2 N	For an old Variant LMK: Indicates the LMK under which the key is encrypted: '00' : LMK pair 04-05 '01' : LMK pair 06-07 '02' : LMK pair 14-15 '03' : LMK pair 16-17 '04' : LMK pair 18-19 '05' : LMK pair 20-21 '06' : LMK pair 22-23 '07' : LMK pair 24-25 '08' : LMK pair 26-27 '09' : LMK pair 28-29 '0A' : LMK pair 30-31 '0B' : LMK pair 32-33 '10' : Variant 1 of LMK pair 04-05 '42' : Variant 4 of LMK pair 14-15 '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". It is not required to enter any LMK into 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 key type specified after delimiter.
	or 2 H	For an old Keyblock LMK: This field is reserved, and should be set to 'FF'.
Key length flag	1 N	For an old Variant LMK: '0' : for single-length key '1' : for double-length key '2' : for triple-length key.
	or 1 H	For an old Keyblock LMK: This field is reserved, and should be set to 'F'.
Key		The Key to be translated from old LMK to new LMK and/or migrated to new key type.
	16 / 32 H or 1 A + 32/48 H	For an old Variant LMK, the 'Key' is encrypted under the old LMK (pair/variant as defined by 'Key Type Code' above).
	or 1 A + n A	For an old Keyblock LMK, the 'Key' is encrypted under the old LMK.
Delimiter	1 A	Optional. Only present if the following field is present. Value ';'.

Field	Length & Type	Details
COMMAND MESSAGE		
Key Type	3 H	For an old Variant LMK: Where 'FF' was entered for 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 Chapter 4 of the General Information Manual. 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)
		For an old Keyblock 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'.
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 at Appendix C of the payShield 9000 General Information Manual.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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.
Variant$_{\text{Old LMK}}$ → Keyblock$_{\text{Current LMK}}$ only: Delimiter	1 A	Value '#'. Optional; Must be present when translating a key from an old Variant LMK to a current Keyblock 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 Chapter 5 of the General Information Manual.
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 Chapter 5 of the General Information Manual.
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'.

Field	Length & Type	Details
COMMAND MESSAGE		
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 '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		The translated Key, encrypted under the current LMK.
	16 / 32 H or 1 A + 32/48 H	For a new Variant LMK, the 'Key' will be encrypted under the appropriate LMK pair/variant, determined by the 'Key Type'.
	or 1 A + n A	For a new Keyblock LMK, the 'Key' will be 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.

Erase the Key Change Storage

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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 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.

Miscellaneous Commands

The payShield 9000 HSM provides the following host commands to support miscellaneous operations:

Command	Page
Echo Command (B2)	213
Cancel Authorized Activities (RA)	214
Generate a Key Check Value (BU)	216
Set HSM Response Delay (LG)	219
Translate Decimalization Table from Old to New LMK (LO)	220
Command Chaining (NK)	221
Modify Keyblock Header (CS)	224
Generate a Random Value (N0)	226

Echo Command

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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 authorized 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

Field	Length & Type	Details
		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 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 '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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
Variant LMK	Authorization: **See text** Activity: **generate.{*keytype*}.host**
Keyblock LMK	Authorisation: **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.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'BU'.
Key Type Code	2 N	For a Variant LMK: Indicates the LMK under which the key is encrypted: '00' : LMK pair 04-05 '01' : LMK pair 06-07 '02' : LMK pair 14-15 '03' : LMK pair 16-17 '04' : LMK pair 18-19 '05' : LMK pair 20-21 '06' : LMK pair 22-23 '07' : LMK pair 24-25 '08' : LMK pair 26-27 '09' : LMK pair 28-29 '0A' : LMK pair 30-31 '0B' : LMK pair 32-33 '10' : Variant 1 of LMK pair 04-05 '1C' : Variant 1 of LMK pair 34-35 '42' : Variant 4 of LMK pair 14-15 'FF' : Use Key Type field, specified after Delimiter (below).

Field	Length & Type	Details
	or 2 H	For a Keyblock LMK: This field is reserved, and should be set to 'FF'.
Key length flag	1 N	For a Variant LMK: '0' : for single-length key '1' : for double-length key '2' : for triple-length key. '3' : for HMAC key
	or 1 H	For a Keyblock LMK: This field is reserved, and should be set to 'F'.
Key		The Key for which a Key Check Value is required.
	16 / 32 H or 1 A + 32/48 H	For a Variant LMK, the 'Key' is encrypted under the LMK (pair/variant as defined by 'Key Type Code' above).
	or 1 A + n A	For a Keyblock LMK, the 'Key' must comply with the following: **Key Usage**: Any valid value; **Algorithm**: Any valid value; **Mode of Use**: 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.
Key Type	3 H	For a Variant LMK: This is the 3-digit key type code of the key being translated. For a list of key type codes, see Key Type Codes in Chapter 4 of the General Information Manual.
		For a Keyblock 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.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 '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 / 6 H	Result of encrypting 64 binary zeroes with the 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
Authorization: **Not required**	

Function: Set the delay for which the HSM waits before it responds to a command

Notes: The command enables the Host to delay HSM output. This is for Host ports that are half duplex and require time to reconfigure from output to input mode.
The delay duration is from 0 to 255ms (the value is treated as MOD 256, so a setting of 256 results in a delay of 0).
The delay is not implemented until after the response to this command.
If the HSM is configured to any host communication other than asynchronous, this command has no effect.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'LG'.
Delay	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 ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
Authorization: **Not required**	

Function: Translate an Encrypted Decimalization Table from Encryption under an LMK in Key Change Storage, to a new LMK.

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 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 1 A + 32 H	16 H when using a Variant LMK or 3-DES Keyblock LMK. 'L' + 32 H when using an AES Keyblock LMK.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 1 A + 32 H	16 H when using a Variant LMK or 3-DES Keyblock LMK. 'L' + 32 H when using an AES Keyblock 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 ☑	Keyblock LMK ☑
License: **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 a 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 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.

Field	Length & Type	Details
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 Keyblock Header

Variant LMK ☒	Keyblock LMK ☑
License: **HSM9-LIC001**	
Authorization: **Optional** Activity: **misc.host**	

Function: To modify certain fields in a Thales keyblock.

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	1 A + n A	Keyblock whose header is to be modified; the key scheme character must be 'S'.
Change Field	1 N	Indicates which field in the keyblock 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 keyblock (must not include a '%' character).
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 keyblock '68' : Command disabled or a standard error code.
Modified Keyblock	1 A + n A	Modified keyblock
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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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 Length	3 N	Random Number Length, taken from Command
Random Value	n B	Random Value with length as defined by Random Number Length (maximum of 256 Bytes)
Random Value Delimiter	1 A	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.

Diagnostic Commands

The payShield 9000 HSM provides the following host commands to support diagnostic operations:

Command	Page
Perform Diagnostics (NC)	228
HSM Status (NO)	229
Return Network Information (NI)	231
Get HSM Loading (J2)	234
Get Host Command Volumes (J4)	236
Reset Utilization Statistics (J6)	238
Get Health Check Accumulated Counts (J8)	239
Reset Health Check Accumulated Counts (JI)	241
Get Instantaneous Health Check Status (JK)	242

Perform Diagnostics

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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.
The Host system should time the NC command and generate an appropriate system message if a response is not received within 5 seconds. If an error is detected in the processor, HSM functions are suspended, and no message is returned to the Host.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'NC'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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 'N0'.
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	2 N	Number of TCP sockets configured (maximum 64).
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 ***not*** one of these.
Reserved	10A	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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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 Host connections is not currently provided

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
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 '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).
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
….	….	….

Field	Length & Type	Details
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 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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.

Notes: See Chapter 8 of the payShield 9000 General Information Manual for an overview of the payShield 9000 Utilization Data capabilities.

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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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 Chapter 8 of the payShield 9000 General Information Manual for an overview of the payShield 9000 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 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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 Chapter 8 of the payShield 9000 General Information Manual for an overview of the payShield 9000 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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 Chapter 9 of the payShield 9000 General Information Manual for an overview of the payShield 9000 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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: See Chapter 9 of the payShield 9000 General Information Manual for an overview of the payShield 9000 Health Check Data capabilities. 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
Authorization: **Not required**	

Function: To return the current status of various health-related items.

Notes: See Chapter 9 of the payShield 9000 General Information Manual for an overview of the payShield 9000 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.

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
HSM Manager state	1 N	Whether the service to process Local or Remote 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 – not running 2 – running 3 – not configured
Async link state	1 N	Whether the async link is running. 0 – unknown 1 – running 2 – not running 3 – not configured
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
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' keyblock
Algorithm	1 N	The algorithm used by the LMK: 0 = 3-DES2Key, 1 = 3-DES3Key 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.

Auditing Commands

The payShield 9000 HSM provides the following host commands to support audit operations:

Command	Page
Translate Audit Record MAC key (Q0)	245
Retrieve Audit Record (Q2)	247
Archive (Print) Audit Record (Q4)	248
Delete Audit Record (Q6)	249
Audit Record Verification (Q8)	250

Translate Audit Record MAC key

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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 'QO'.
MAC key		The MAC key to be translated.
	'U' + 32 H	For an old Variant LMK, the 'MAC Key' must be encrypted under LMK pair 22-23 variant 7.
	'S' + 32 H	For an old Keyblock 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	1 A + 32 H	The translated MAC Key, 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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 Appendix B for details.
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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001**	
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 Appendix B for 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 '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.

Card Verification Code/Value Commands

The payShield 9000 HSM provides the following host commands to support card verification code/value operations:

Command	Page
Generate a Card Verification Code/Value (CW)	252
Verify a Card Verification Code/Value (CY)	254
Generate a Dynamic CVV (QY)	256
Verify a Dynamic CVV/CVC	258
Calculate Card Security Codes (RY)	263
Verify Card Security Codes (RY)	265

Generate a Card Verification Code/Value

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
Authorization: **Not required**	

Function: Generate a VISA CVV or MasterCard CVC.

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		The CVK A / B key, used to calculate the CVV/CVC.
	32 H or 1 A + 32 H	For a Variant LMK, the 'CVK A/B' must be encrypted under LMK pair 14-15 variant 4.
	or 1 A + n A	For a Keyblock LMK, the 'CVK A/B' must comply with the following: **Key Usage**: 'C0', '12', '13' **Algorithm**: 'T' **Mode of Use**: 'C', 'G', 'N'
Primary account number	n N	The primary account number for the card.
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 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.

Verify a Card Verification Code/Value

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: Verify a VISA CVV or MasterCard CVC.

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 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 A / B		The CVK A / B key, used to verify the supplied CVV/CVC.
	32 H or 1 A + 32 H	For a Variant LMK, the 'CVK A/B' must be encrypted under LMK pair 14-15 variant 4.
	or 1 A + n A	For a Keyblock LMK, the 'CVK A/B' must comply with the following: **Key Usage**: 'C0', '12', '13' **Algorithm**: 'T' **Mode of Use**: 'C', 'V', 'N'
CVV	3 N	CVV for verification.
Primary account number	n N	The primary account number for the card.
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 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not Required**	

Function: Generate a Dynamic Card Verification Value (dCVV).

Notes: The only scheme currently supported is Visa dCVV (Scheme ID = 0). This command will 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' … '9' : Reserved for future use.
MK-DCVV		Master Key from which card-unique key is derived.
	32 H or 1 A + 32/48 H	For a Variant LMK: For scheme ID = '0', the 'MK-DCVV' must be a MK-AC, encrypted under LMK 28-29 variant 1.
	or 1 A + n A	For a Keyblock LMK: For scheme ID = '0', the 'MK-DCVV' must comply with the following: Key Usage: 'E0'; Algorithm: 'T'; Mode of Use: '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.
PAN	n N	The Primary Account Number for the card. The maximum PAN Length for Scheme 0 (Visa) is 16 digits.
Delimiter	1 A	Value ';'. Identifies the end of the PAN field.
Scheme '0' (Visa dCVV) 1) Expiration Date	4 N	The Card Expiry Date.
Scheme '0' (Visa dCVV) 2) Service Code	3 N	The Service Code to be used for dCVV generation. NOTE: must be '998' for Scheme 0 (Visa).
Scheme '0' (Visa dCVV) 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.

Field	Length & Type	Details
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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' : MK-DCVV Parity Error or a standard error code.
dCVV	3 N	The calculated dCVV
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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Optional (see text)** Activity: **diag.host**	

Function: Verify a Dynamic Card Verification Value (dCVV) or Card Verification Code (dCVC).

Notes: 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 *DK-AC*.

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

The PAN sequence number is assumed to be zero for the calculation of the *DK-CVC3*. This command will append a zero to the supplied PAN when generating the *DK-CVC3.* Optionally, the command will also allow the PAN sequence number to be provided so that the calculation of the UDK can be based on supplied PAN and PAN sequence numbers.

Verification of the CVC3 requires the IVCVC3 which is a MAC calculated over the static part of $Track_1$ or $Track_2$ 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.

PINCVC3 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.

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' … '9' : Reserved for future use.
Version	1 N	For Scheme ID = '0': '0' : Visa DCVV verification. 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. For Scheme ID = '2': '0' : American Express ExpressPay verification as defined in ExpressPay 2.0 specifications. For Scheme ID = '3': '0' : Discover ZIP DCVV '1' : Discover ZIP DCVV Plus. Other values are RFU.
MK-DCVV		Master Key from which card-unique key is derived.
	32 H or 1 A + 32/48 H	For a Variant LMK: For scheme ID = '0' or '2', the 'MK-DCVV' must be a MK-AC, encrypted under LMK 28-29 variant 1. For Scheme ID = '1' or '3', the 'MK-DCVV' must be a MK-CVC3, encrypted under LMK 28-29 variant 7.
	or 1 A + n A	For a Keyblock LMK: For scheme ID = '0' or '2', the 'MK-DCVV' must comply with the following: **Key Usage**: 'E0'; **Algorithm**: 'T'; **Mode of Use**: 'N' For scheme ID = '1' or '3', the 'MK-DCVV' must comply with the following: **Key Usage**: 'E6', '32'; **Algorithm**: 'T'; **Mode of Use**: 'N'

Field			Length & Type	Details
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. Discover specific methods for deriving unique key from Master Key (only valid if Scheme ID = '3'): '2': 16-byte Account Unique Key for DCVV (AUKDCVV) '3': 24-byte Account Unique Key for DCVV (AUKDCVV)
PAN			n N	The Primary Account Number for the card. The maximum PAN Length for Scheme 0 (Visa) is 16 digits. The maximum PAN Length for Scheme 1 (MasterCard) is 19 digits. If Key Derivation Method = '2' or '3': Concatenation of the 16-digit Primary Account Number and 4-digit Expiration Date for the card.
Delimiter			1 A	Value ';'. Identifies the end of the PAN field.
PAN Sequence No.			2 N	The Sequence Number for the card. If the Sequence Number is not available it should be specified as '00'. Only present for: • Scheme '1' & Version '1' • Scheme '1' & Version '2' • Scheme '2'
Scheme '0' (Visa DCVV)	Expiration Date		4 N	The Card Expiry Date.
	Service Code		3 N	The Card's Track 2 Service Code.
	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.
	DCVV		3 N	Dynamic CVV to be validated.
Scheme '1' (MasterCard Paypass)	Versions '0' and '1'	IVCVC3	5 N	The issuer proprietary static data element. Max value '65535' (2 byte field).
	Versions '2' and '3'	Track Data Length	3 N	The length of the following field.
		Track Data	n B	Static Track (1 or 2) Data.
	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).
	ATC		5 N	Decimal value of Application Transaction Counter. Max value '65535' (2 byte field).

Field		Length & Type	Details
	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).
Scheme '2' (ExpressPay)	Transaction Data Length	2 H	Length of the following field. Can be any length from '01' (1) to 'FF' (255) bytes.
	Transaction Data	n B	Variable length data. If the data supplied is not a multiple of 8 bytes, additional zero padding is added.
	Delimiter	1 A	Delimiter, to indicate the end of Transaction Data, value ';'.
	Cryptogram	5 N	The Cryptogram to be validated.
Scheme '3' (Discover)	ATC	4 N	Decimal value of Application Transaction Counter.
	Unpredictable Number	2 N	Value of random number provided to the card by the terminal during a transaction.
	Extended Unpredictable Number	6 N	Value of Extended Unpredictable Number, in BCD format, right-justified and zero-filled. Only present for Version = '1'.
	DCVV	3 N	The DCVV to be verified. Only present for Version = '0'.
	DCVV Plus Length	1 N	Length of DCVV Plus. Only present for Version = '1'.
	DCVV Plus	n N	DCVV Plus. Length is determined by preceding field. Only present for Version = '1'.
Delimiter		1 A	Value '%'. Optional; if present, the following field must 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' : DCVV verification failure '05' : Unrecognized Scheme, Version ID or Key Derivation Method '10' : MK-DCVV Parity Error '68' : Command disabled or a standard error code.
Diagnostic Data	3 N or 5 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. For Scheme-ID '0' & Version '0', this is a 3N field containing the correct dCVV. For Scheme-ID '1' & Version '0, '1', or '2', this is a 5N field containing the correct CVC3. For Scheme-ID '1' & Version '3', this is a 5N field containing the correct PINCVC3. For Scheme-ID '2' & Version '0', this is a 5N field containing the correct Cryptogram. For Scheme-ID '3' & Version '0', this is a 3N field containing the correct DCVV. For Scheme-ID '3' & Version '1', this is an nN field containing the correct DCVV Plus (where n is specified by the input field "DCVV Plus 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.

Calculate Card Security Codes

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC024**	
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		The CSCK used to calculate the Card Security Code.
	32 H or 1 A + 32 H	For a Variant LMK, the 'CSCK' must be encrypted under LMK pair 14-15 variant 4.
	or 1 A + n A	For a Keyblock LMK, the 'CSCK' must comply with the following: **Key Usage**: 'C0', '11'; **Algorithm**: 'T'; **Mode of Use**: 'C', 'G', 'N'
Account Number	19 N	The full account number, 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.

Field	Length & Type	Details
COMMAND MESSAGE		
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 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.

Verify Card Security Codes

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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		The CSCK used to verify the Card Security Code.
	32 H or 1 A + 32 H	For a Variant LMK, the 'CSCK' must be encrypted under LMK pair 14-15 variant 4.
	or 1 A + n A	For a Keyblock LMK, the 'CSCK' must comply with the following: Key Usage: 'C0', '11'; Algorithm: 'T'; Mode of Use: 'C', 'V', 'N'
Account Number	19 N	The full account number, 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

Field	Length & Type	Details
COMMAND MESSAGE		
5-digit CSC/iCSC	5 N	Authenticating Code (2 digits). Only present if Flag = '0' or '2'. 5-digit Card Security Code. Ignored if set to 'FFFFF'.
4-digit CSC/iCSC	4 N	Only present if Flag = '0' or '2'. 4-digit Card Security Code. Ignored if set to 'FFFF'.
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'. If Flag = '3' this field will contain the 3-digit iCSC or AEVV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 '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.

EMV Chip Card Commands

This section describes the payShield 9000 HSM 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	VSDC / UKIS name used	Europay / MasterCard name used
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 9000 HSM provides the following host commands to support EMV chip card operations:

Command	Page
ARQC Verification and/or ARPC Generation (EMV 3.1.1) (KQ)	268
Data Authentication Code and Dynamic Number Verification (EMV 3.1.1) (KS)	271
Generate Secure Message (EMV 3.1.1) (KU)	273
Generate Secure Message (EMV 4.x) (KY)	277
ARQC Verification and/or ARPC Generation (EMV 4.x) (KW)	283
Decrypt Encrypted Counters (EMV 4.x) (KO)	286
Verify Truncated Application Cryptogram (MasterCard CAP) (K2)	289

ARQC Verification and/or ARPC Generation (EMV 3.1.1)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC026**	
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 18)	'0'
MasterCard M/Chip (CVN 10 or 11)	'1'
American Express AEIPS (CVN 01)	'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	Identifier of the EMV scheme: '0' : Visa VIS '1' : MasterCard M/Chip '2' : American Express AEIPS.
MK-AC		The Issuer Master Key for generating and verifying Application Cryptograms.

Field	Length & Type	Details
MK-SMI	32 H or 1 A + 32 H	For a Variant LMK, the 'MK-AC' must be encrypted under LMK pair 28-29 variant 1.
	or 1 A + n A	For a Keyblock LMK, the 'MK-AC' must comply with the following: Key Usage: 'E0'; Algorithm: 'T'; Mode of Use: 'N'
		The Issuer Master Key for Secure Message with Integrity. Only present if Mode = '3' or '4', and Scheme ID is 'O'.
	32 H or 1 A + 32 H	For a Variant LMK, the 'MK-SMI' must be encrypted under LMK pair 28-29 variant 2.
	or 1 A + n A	For a Keyblock LMK, the 'MK-AC' must comply with the following: Key Usage: 'E1'; Algorithm: 'T'; Mode of Use: '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 'O'.
Transaction Data Length	2 H	Length of next field. Can be any length from 1 to 255 bytes. Only present if Mode is 'O', '1', '3' or '4'.
Transaction Data	n B	Variable length data. Only present if Mode is 'O', '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 'O', '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 = 'O'.
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 = 'O'.
Discretionary Data	n B	Discretionary Data over which the MAC was generated. Only present if Mode is '3' or '4' and Scheme ID = 'O'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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	'00' : No error '01' : ARQC/TC/AAC verification failed '03' : Mode = 3 or 4 but Scheme ID ≠ 0 '04' : Invalid Mode value '05' : Unrecognized Scheme ID '06' : 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.
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.

Data Authentication Code and Dynamic Number Verification (EMV 3.1.1)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC026**	
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		The Issuer Master Key for calculating and verifying Data Authentication Codes. Only present only for Mode '0'.
	32 H or 1 A + 32 H	For a Variant LMK, the 'MK-DAC' must be encrypted under LMK pair 28-29 variant 4.
	or 1 A + n A	For a Keyblock LMK, the 'MK-DAC' must comply with the following: **Key Usage**: 'E3' **Algorithm**: 'T' **Mode of Use**: 'N'
MK-DN		The Issuer Master Key for calculating and verifying Dynamic Numbers. Only present only for Mode '1'.
	32 H or 1 A + 32 H	For a Variant LMK, the 'MK-DN' must be encrypted under LMK pair 28-29 variant 5.
	or 1 A + n A	For a Keyblock LMK, the 'MK-DN' must comply with the following: **Key Usage**: 'E4' **Algorithm**: 'T' **Mode of Use**: '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 be present.

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.
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' : 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.

Generate Secure Message (EMV 3.1.1)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC026**	
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'

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.
MK-SMI		The Master Key for Secure Messaging with Integrity, used to generate a MAC on the message.

Field	Length & Type	Details
	32 H or 1 A + 32 H	For a Variant LMK, the 'MK-SMI' must be encrypted under LMK pair 28-29 variant 2.
	or 1 A + n A	For a Keyblock LMK, the 'MK-SMI' must comply with the following: Key Usage: 'E2'; Algorithm: 'T'; Mode of Use: 'N'
PAN/PAN Sequence No	8 B	Pre-formatted PAN/PAN Sequence number.
Integrity Session Data	8 B	Used for Integrity Session Key Generation: For Scheme ID = '0' and '2' (Visa/UKIS and AEIPS) this will be the 2 byte ATC right justified and padded on the left with 6 zero bytes. For Scheme ID = '1' (Europay/MasterCard) this is an 8 byte random number, RANDi.
Plaintext Message Data Length	4 H	Length in bytes of data in next field.
Plaintext Message	n B	Plaintext Message Data.
Delimiter	1 A	Delimiter of previous field, ';'.
MK-SMC		The Master Key for Secure Messaging with Confidentially, used to encrypt the message. Only present if Mode Flag = '2' or '4'.
	32 H or 1 A + 32 H	For a Variant LMK, the 'MK-SMC' must be encrypted under LMK pair 28-29 variant 3.
	or 1 A + n A	For a Keyblock LMK, the 'MK-SMC' must comply with the following: Key Usage: 'E1'; Algorithm: 'T'; Mode of Use: 'N'
TK		The Transport Key, used to decrypt the supplied message. Only present if Mode Flag = '1' or '2'.
	32 H or 1 A + 32 H	For a Variant LMK, the 'TK' must be encrypted under LMK pair 30-31.
	or 1 A + n A	For a Keyblock LMK, the 'TK' must comply with the following: Key Usage: 'D0', '22'; Algorithm: 'T'; Mode of Use: 'B', 'D', 'N'
Confidentiality Session Data	8 B	Used for Confidentiality Session Key Generation. For Scheme ID = '0' or '2' (Visa/UKIS or AEIPS) 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. Only present if Mode Flag = '1', '2', '3' or '4'.
Offset	4 H	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). Only present if Mode Flag = '1', '2', '3' or '4'. If Mode Flag = '3' or '4', this is used to specify the new PIN Block position.
Cipher Text Message Data Length	4 H	Length in bytes of data in next field. For the standard model HSM the maximum size is 32 bytes ('0020' in hex). Must be a multiple of 8 bytes (i.e. 8, 16, 24 or 32).

Field	Length & Type	Details
		If Mode Flag = '3' or '4', this is used for the New PIN Block. If Destination PIN Block Type = 42, this is used for Current PIN Block concatenated with New PIN Block. Only present if Mode Flag = '1', '2', '3' or '4'.
Cipher Text Message Data	n B	Cipher Text Message supplied encrypted using a Transport Key (TK). It must be a multiple of 8 bytes long. Note that no additional padding is performed on the decrypted message before the re-encryption process. Only present if Mode Flag = '1', '2', '3' or '4'. If Mode Flag = '3' or '4', this is used for the New PIN Block. If Destination PIN Block Type = 42, this is used for Current PIN Block concatenated with New PIN Block.
Delimiter	1 A	Delimiter of previous field, ";". Only present if Mode Flag = '1', '2', '3' or '4'.
Source PIN Encryption Key Type		Only present if Mode Flag = '3' or '4'.
	1 N	For a Variant LMK: Type of PIN Encryption Key: '0' : ZPK '1' : TPK.
	or 1 H	For a Keyblock LMK: This field is ignored; should be set to 'F'.
Source PIN Encryption Key		The source PIN Encryption Key, used to decrypt the supplied PIN block. Only present if Mode Flag = '3' or '4'.
	16 H or 1 A + 32/48 H	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".
	or 1 A + n A	For a Keyblock LMK, the 'Source PIN Encryption Key' must comply with the following: Key Usage: 'P0', '71', '72' Algorithm: 'D', 'T' Mode of Use: 'B', 'D', 'N'
Source PIN Block Format code	2 N	The format code for the source PIN block. Only present if Mode Flag = '3' or '4'.
Destination PIN Block format code	2 N	The format code for the destination PIN block: '34' : Standard EMV PIN Block '35' : Europay / Mastercard Pay Now & Pay Later '41' : Visa / Amex Format Without Using Current PIN '42' : Visa / AmexFormat using Current PIN. Only present if Mode Flag = '3' or '4'.
Account Number	12 N or 18 H	Only present if Mode Flag = '4'. This field is used for PIN block translation. For a Source PIN Block Format Code ≠ '04', this field has length 12 N, and specifies the 12 right most digits of the account number, excluding the check digit. For a Source PIN Block Format Code = '04', this field has

Field	Length & Type	Details
MK-AC		length 18 H, and specifies the entire 18 digit account number, excluding the check digit, padded with 'F' on the left. Only present if Mode Flag = '3' or '4' 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.
	32 H or 1 A + 32 H	For a Variant LMK, the 'MK-AC' must be encrypted under LMK pair 28-29 variant 1.
	or 1 A + n A	For a Keyblock LMK, the 'MK-AC' must comply with the following: Key Usage: 'E0' Algorithm: 'T' Mode of Use: 'N'
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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	'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 '68' : Command disabled '69' : PIN Block format has been disabled or a standard error code.
MAC	8 B	The calculated 64 bit MAC.
Re-encrypted ciphertext Data Length	4 H	Length in bytes of data in next field. Only present for modes '1', '2', '3' or '4'.
Re-encrypted ciphertext message Data	n B	Re-encrypted Ciphertext message data. Only present for modes '1', '2', '3' or '4'.
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 ☑	Keyblock LMK ☑
License: **HSM9-LIC026**	
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:

Application	Scheme ID
Visa VIS (CVN 14)	'0'
MasterCard M/Chip (CVN 12 or 13) (EMV 2000)	'1'
MasterCard M/Chip (CVN 14 or 15) (EMV CSK)	'6'
Discover D-PAS (05 or 06)	'6'
Indonesian National Standard Chip Card Specification (NSICCS)	'5'

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	The following modes define the operation of the Function: '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. 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. For Mode = 0, EMV 4.x Option A ICC Master Key Derivation

Field	Length & Type	Details
		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.
Scheme ID	1 N	Only present for Mode Flag = '2', '4' or '5'. Identifier for the card Scheme: '0' : Visa VIS using EMV 4.x Option A ICC Master Key Derivation and EMV2000 Session Key Derivation '1' : MasterCard M/Chip using EMV 4.x Option A ICC Master Key Derivation and EMV2000 Session Key Derivation '2' : Reserved for future use '3' : Reserved for future use '4' : CCD using EMV 4.x Option B ICC Master Key Derivation and EMV2000 Session Key Derivation '5' : Visa VIS using EMV 4.x Option A ICC Master Key Derivation and EMV Common Session Key Derivation and Indonesian National Standard Chip Card Specification (NSICCS) '6' : MasterCard M/Chip and Discover D-PAS using EMV 4.x Option A ICC Master Key Derivation and EMV Common Session Key Derivation '7' : CCD using EMV 4.x Option B ICC Master Key Derivation and EMV Common Session Key Derivation Used to specify the padding and Key Derivation Methods to use. Note: For Mode Flag = '5', this field only specifies the key derivation method as padding is not relevant.
MK-SMI		The Master Key for Secure Messaging with Integrity, used to generate a MAC on the message.
	32 H or 1 A + 32 H	For a Variant LMK, the 'MK-SMI' must be encrypted under LMK pair 28-29 variant 2.
	or 1 A + n A	For a Keyblock LMK, the 'MK-SMI' must comply with the following: Key Usage: 'E2' Algorithm: 'T' Mode of Use: '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' or '7'. Number of bytes in PAN/PAN Sequence Number field. Valid values '01' … '99'. *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.*
PAN/PAN Sequence No	8 B or n B	For Mode = '0' or when 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). *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.* For Mode <> '0' and Scheme ID = '4' or '7', this field contains the PAN/PSN (in BCD format). The field length is specified (in bytes) by the PAN length field.

Field	Length & Type	Details
		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. *Note: If PAN length <= 8 bytes EMV Option A will be used, and the HSM will pad appropriately to 8 bytes if necessary.*
Delimiter	1 A	Only present for Scheme ID '4' or '7'. 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'. The ATC from the card. This is used for Session Key Generation.
Application Cryptogram	8 B	Only present for Scheme ID = '5', '6' or '7'. 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	Plaintext Message Data.
Delimiter	1 A	Delimiter of previous field, ';'.
MK-SMC		The Master Key for Secure Messaging with Confidentially, used to encrypt the message. Only present if Mode Flag = '2' or '4'.
	32 H or 1 A + 32 H	For a Variant LMK, the 'MK-SMC' must be encrypted under LMK pair 28-29 variant 3.
	or 1 A + n A	For a Keyblock LMK, the 'MK-SMC' must comply with the following: Key Usage: 'E1'; Algorithm: 'T'; Mode of Use: '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		The Transport Key, used to decrypt the supplied message. Only present if Mode Flag = '2'.
	32 H or 1 A + 32 H	For a Variant LMK, the 'TK' must be encrypted under LMK pair 30-31.
	or 1 A + n A	For a Keyblock LMK, the 'TK' must comply with the following: Key Usage: '00', '22'; Algorithm: 'T'; Mode of Use: '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. (ie if length of Plaintext data is '0039', and Offset is '0039', then the Ciphertext data is placed at the end of the plaintext

Field	Length & Type	Details
		message. If Mode Flag = '4', this is used to specify the New PIN Block position.
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'. Cipher Text Message supplied encrypted using a Transport Key (TK). It must be a multiple of 8 bytes long. Note that no additional padding is performed on the decrypted message before the re-encryption process. If Mode Flag = '4', this is used for the New PIN Block. If Destination PIN Block Type = 42 this is used for Current PIN Block concatenated with New PIN Block.
Delimiter	1 A	Only present if Mode Flag = '2' or '4'. Delimiter of previous field, ';'.
Source PIN Encryption Key Type		Only present if Mode Flag = '4'.
	1 N	For a Variant LMK: Type of PIN Encryption Key: '0' : ZPK '1' : TPK.
	or 1 H	For a Keyblock LMK: This field is ignored; should be set to 'F'.
Source PIN Encryption Key		The source PIN Encryption Key, used to decrypt the supplied PIN block. Only present if Mode Flag = '4'.
	16 H or 1 A + 32/48 H	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".
	or 1 A + n A	For a Keyblock LMK, the 'Source PIN Encryption Key' must comply with the following: Key Usage: 'P0', '71', '72'; Algorithm: 'D', 'T'; Mode of Use: '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'. The format code for the destination PIN block: '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.
Account Number	12 N or 18 H	Only present if Mode Flag = '3' or '4'. This field is used for PIN block translation. For a Source PIN Block Format ≠ '04', this field has length 12

Field	Length & Type	Details
MK-AC		N, and specifies the 12 right most digits of the account number, excluding the check digit. For a Source PIN Block Format = '04', this field has length 18 H, and specifies the entire 18 digit account number, excluding the check digit, padded with 'F' on the left. Only present if Mode Flag = '4' 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.
	32 H or 1 A + 32 H	For a Variant LMK, the 'MK-AC' must be encrypted under LMK pair 28-29 variant 1.
	or 1 A + n A	For a Keyblock LMK, the 'MK-AC' must comply with the following: Key Usage: 'E0'; Algorithm: 'T'; Mode of Use: 'N'
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 '52' : Invalid Branch/Height '68' : Command disabled '69' : PIN Block format has been disabled or a standard error code.
MAC	8 B	The calculated 64 bit MAC.
Re-encrypted ciphertext Data Length	4 H	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.

ARQC Verification and/or ARPC Generation (EMV 4.x)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC026**	
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
Visa VIS (CVN 14)	'0'
Visa VIS (CVN 18)	'2' or '3'
MasterCard M/Chip (CVN 12 or 13) (EMV 2000)	'0'
MasterCard M/Chip (CVN 14 or 15) (EMV CSK)	'2'
Discover D-PAS (05 or 06)	'2'
Indonesian National Standard Chip Card Specification (NSICCS)	'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 'KW'.
Mode Flag	1 H	Mode of operation: '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

Field	Length & Type	Details
		generation '6' : Perform D-PAS Method 1 ARPC generation only.
Scheme ID	1 N	Specifies the Key Derivation Methods to use '0' : Option A ICC Master Key Derivation and EMV2000 Session Key Derivation '1' : Option B ICC Master Key Derivation and EMV2000 Session Key Derivation '2' : Option A ICC Master Key Derivation and EMV Common Session Key Derivation and Indonesian National Standard Chip Card Specification (NSICCS) '3' : Option B ICC Master Key Derivation and EMV Common Session Key Derivation
MK-AC		The Issuer Master Key for generating and verifying Application Cryptograms.
	32 H or 1 A + 32 H	For a Variant LMK, the 'MK-AC' must be encrypted under LMK pair 28-29 variant 1.
	or 1 A + n A	For a Keyblock LMK, the 'MK-AC' must comply with the following: Key Usage: 'E0'; Algorithm: 'T'; Mode of Use: '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' or '3'. Length in bytes of PAN/PAN Sequence Number field. Valid values '01' to '99'.
PAN/PAN Sequence No	8 B or n B	For Scheme ID = '0' or '2', this field will be fixed at 8 bytes, and should contain the pre-formatted PAN/PAN Sequence No. For Scheme ID = '1' or '3', the field length is specified by the "PAN Length" field. It is the responsibility of the host system to ensure that the PAN/PAN Sequence Number is appropriately padded.
Delimiter	1 A	Only present for Scheme ID = '1' or '3'. Delimiter, to indicate end of PAN/PAN Sequence No, value ';'.
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	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
Transaction Data Length	2 H	Only present for Mode Flag = '0', '1', '3' or '5'. 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' or '5'. 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	Only present for Mode Flag = '0', '1', '3' or '5'. Delimiter, to indicate end of Transaction Data, value ';'.

Field	Length & Type	Details
ARQC/TC/AAC	8 B	ARQC/TC/AAC to be validated and/or used for ARPC generation.
ARC	2 B	Only present for Mode Flag = '1' or '2'. Authorisation Response Code. Used in ARPC generation for VIS 1.x and M/Chip 4.x 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 5 and 6), the CSU is a 2-byte value and must be right-padded with 0s.
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 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' : ARQC/TC/AAC verification failure '04' : Unrecognized Mode Flag '05' : Unrecognized Scheme ID '10' : MK parity error '52' : Invalid Branch/Height '68' : Command disabled or a standard error code.
ARPC	8 B	Only present for Modes '1', '2', '3', '4', '5' and '6' if no error is encountered. The calculated ARPC.
Diagnostic data	8 B	Calculated ARQC/TC/AAC 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.

Decrypt Encrypted Counters (EMV 4.x)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC026**	
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 1 A + 32 H	For a Variant LMK, the 'MK-AC' must be encrypted under LMK pair 28-29 variant 1.
	or 1 A + n A	For a Keyblock LMK, the 'MK-AC' must comply with the following: Key Usage: 'E0'; Algorithm: 'T'; Mode of Use: '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'. *Note: This field indicates the number of bytes used to store*

Field	Length & Type	Details
COMMAND MESSAGE		
		the PAN/PSN. If the number of digits in the PAN/PSN is odd, an extra '0' digit must be inserted to the left.
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). 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. 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. 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. Note: If "PAN Length" <= 8 bytes, the HSM will pad to 8 bytes if necessary, according to EMV Option A.
Delimiter	1 A	Only present for Scheme ID = '1', '3' or '5'. Delimiter, to indicate end of PAN/PAN Sequence No, value ';'.
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.
UN	4 B	Only present for Scheme ID = '4' or '5'. Unpredictable Number.
Application Transaction Counter	2 B	The ATC from the card. This is used for Session Key Generation.
Encrypted Counters	8 B	The Encrypted Counter data, containing the OCTA and OCTN
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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.

Verify Truncated Application Cryptogram (MasterCard CAP)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC005**	
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.
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)		The Issuer Master Key for generating and verifying Application Cryptograms.
	32 H or 1 A + 32 H	For a Variant LMK, the 'MK-AC' must be encrypted under LMK pair 28-29 variant 1.
	or 1 A + n A	For a Keyblock LMK, the 'MK-AC' must comply with the following: Key Usage: 'E0'; Algorithm: 'T'; Mode of Use: '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'.

Field	Length & Type	Details
		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.
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). *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.* 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. *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.* *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.

Field	Length & Type	Details
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 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' : 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.

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 9000 HSM include key management in addition to MAC generation and verification.

The payShield 9000 HSM provides the following host commands to support RTKS operations:

Command	Page
Transaction Request With a PIN (T/AQ Key) (*when selected Transaction Key Scheme is Racal*) (RI)	294
Transaction Request With a PIN (T/AQ Key) *(when selected Transaction Key Scheme is Australian)* (HI)	297
Transaction Request Without a PIN (*when selected Transaction Key Scheme is Racal*)(RK)	298
Transaction Request Without a PIN (*when selected Transaction Key Scheme is Australian*) (HK)	300
Transaction Request With a PIN (T/CI Key) *(when selected Transaction Key Scheme is Racal)* (RU)	301
Transaction Request With a PIN (T/CI Key) *(when selected Transaction Key Scheme is Australian)* (HU)	303
Translate KEYVAL *(when selected Transaction Key Scheme is Racal)* (RW)	304
Translate KEYVAL *(when selected Transaction Key Scheme is Australian)* (HW)	306
Administration Request Message *(when selected Transaction Key Scheme is Racal)* (RM)	307
Administration Request Message *(when selected Transaction Key Scheme is Australian)* (HM)	309
Transaction Response with Auth Para from Card Issuer *(when selected Transaction Key Scheme is Racal)* (RO)	310
Transaction Response with Auth Para from Card Issuer (*when selected Transaction Key Scheme is Australian*) (HO)	312
Generate Auth Para and Transaction Response *(when selected Transaction Key Scheme is Racal)* (RQ)	313

Generate Auth Para and Transaction Response *(when selected Transaction Key Scheme is Australian)* (HQ)	315
Confirmation *(when selected Transaction Key Scheme is Racal)* (RS)	316
Confirmation *(when selected Transaction Key Scheme is Australian)* (HS)	318

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 using the CS (Configure Security) console command or HSM Manager Initial Settings. 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 9000.)

Transaction Request With a PIN (T/AQ Key) (*when selected Transaction Key Scheme is Racal*)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings). 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 Chapter 12 of the *payShield 9000 General Information 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		The Terminal Key Register, used to validate the MAC.
	16 H or 1 A + 32/48 H	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".
	or 1 A + n A	For a Keyblock LMK, the 'Terminal Key Register' must comply with the following: **Key Usage**: 'P0', '73'; **Algorithm**: 'D', 'T'; **Mode of Use**: 'N'
Account Number pointer	2 H	Value '00' if the account number starts at the first character in the message text field, and one value greater for each subsequent character into the field. The account number 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

Field	Length & Type	Details
COMMAND MESSAGE		
		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 account number starts at the first character in the message text field, and one value greater for each subsequent character into the field. The account number 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) characters and is formatted according to the ANSI X9.8 standard (PIN block format 01).
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 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		The TPK, used to decrypt a PIN block.
	16 H or 1 A + 32/48 H	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".

	or 1 A + n A	For a Keyblock LMK, the 'TPK' will comply with the following: **Key Usage**: '71' **Algorithm**: 'D', 'T' **Mode of Use**: '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.

Transaction Request With a PIN (T/AQ Key) *(when selected Transaction Key Scheme is Australian)*

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings) 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 9000.
  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 *payShield 9000 Australian Standards Reference 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 ø	Use the Rx variant of the command ø

  * As described in this manual
  ø As described in the *payShield 9000 Australian Standards Reference Manual*
  For further details, see Chapter 12 of the *payShield 9000 General Information 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings). 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 Chapter 12 of the *payShield 9000 General Information 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		The Terminal Key Register, used to validate the MAC.
	16 H or 1 A + 32/48 H	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".
	or 1 A + n A	For a Keyblock LMK, the 'Terminal Key Register' must comply with the following: Key Usage: 'P0', '73'; Algorithm: 'D', 'T'; Mode of Use: 'N'
Account Number pointer	2 H	Value '00' if the account number starts at the first character in the message text field, and one value greater for each subsequent character into the field. The account number 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.

Field	Length & Type	Details
Extended account number pointer	4 H	Optional. Only present if extended length messages are to be used. '0000' if the account number starts at the first character in the message text field, and one value greater for each subsequent character into the field. The account number 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 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 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings) 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 9000.

  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 *payShield 9000 Australian Standards Reference 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 Ø	Use the Rx variant of the command Ø

  * As described in this manual

  Ø As described in the *payShield 9000 Australian Standards Reference Manual*

  For further details, see Chapter 12 of the *payShield 9000 General Information 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings). 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 Chapter 12 of the *payShield 9000 General Information 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		The Terminal Key Register, used to validate the MAC.
	16 H or 1 A + 32/48 H	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".
	or 1 A + n A	For a Keyblock LMK, the 'Terminal Key Register' must comply with the following: Key Usage: 'P0', '73'; Algorithm: 'D', 'T'; Mode of Use: 'N'
Account Number pointer	2 H	Value '00' if the account number starts at the first character in the message text field, and one value greater for each subsequent character into the field. The account number 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.

Field	Length & Type	Details
Extended account number pointer	4 H	Optional. Only present if extended length messages are to be used. '0000' if the account number starts at the first character in the message text field, and one value greater for each subsequent character into the field. The account number 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 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 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 1 A + 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 3-DES Keyblock LMK, this field consists of an "S" followed by 32 hex digits. When using an AES Keyblock 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings) 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 9000.
  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 *payShield 9000 Australian Standards Reference 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 Ø	Use the Rx variant of the command Ø

* As described in this manual

Ø As described in the *payShield 9000 Australian Standards Reference Manual*

For further details, see Chapter 12 of the *payShield 9000 General Information 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings). 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 Chapter 12 of the *payShield 9000 General Information 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		The Zone PIN Key, used to encrypt the KEYVAL.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'ZPK' must be encrypted under LMK pair 06-07.
	or 1 A + n A	For a Keyblock LMK, the 'ZPK' must comply with the following: **Key Usage**: 'P0', '72'; **Algorithm**: 'D', 'T'; **Mode of Use**: 'B', 'E', 'N'
KEYVAL	16 H or 1 A + 32 H	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 3-DES Keyblock LMK, this field must consist of an "S" followed by 32 hex digits. When using an AES Keyblock LMK, this field must consist of an "N" followed by 32 hex digits.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings) 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 9000.
  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 *payShield 9000 Australian Standards Reference 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 Ø	Use the Rx variant of the command Ø

* As described in this manual

Ø As described in the *payShield 9000 Australian Standards Reference Manual*

For further details, see Chapter 12 of the *payShield 9000 General Information 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings). 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 Chapter 12 of the *payShield 9000 General Information 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		The Terminal Key Register, used to validate the MAC.
	16 H or 1 A + 32/48 H	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".
	or 1 A + n A	For a Keyblock LMK, the 'Terminal Key Register' must comply with the following: **Key Usage**: 'P0', '73'; **Algorithm**: 'D', 'T'; **Mode of Use**: '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

Field	Length & Type	Details
		characters are assumed to be the MAC.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings) 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 9000.
  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 *payShield 9000 Australian Standards Reference 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 ø	Use the Rx variant of the command ø

* As described in this manual

ø As described in the *payShield 9000 Australian Standards Reference Manual*

For further details, see Chapter 12 of the *payShield 9000 General Information Manual*.

Transaction Response with Auth Para from Card Issuer *(when selected Transaction Key Scheme is Racal)*

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings). 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 Chapter 12 of the *payShield 9000 General Information 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		The Terminal Key Register, used to generate the MAC.
	16 H or 1 A + 32/48 H	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".
	or 1 A + n A	For a Keyblock LMK, the 'Terminal Key Register' must comply with the following: **Key Usage**: 'P0', '73'; **Algorithm**: 'D', 'T'; **Mode of Use**: '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	The Zone PIN Key, or the single character 'L' to indicate that Auth Para is encrypted under the LMK (see next field).
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'ZPK' must be encrypted under LMK pair 06-07.
	or 1 A + n A	For a Keyblock LMK, the ZPK' must comply with the following: **Key Usage**: 'P0', '72'; **Algorithm**: 'D', 'T'; **Mode of Use**: '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.

Field	Length & Type	Details
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 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		The new Terminal Key Register, to replace the current one.
	16 H or 1 A + 32/48 H	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".
	or 1 A + n A	For a Keyblock LMK, the 'Terminal Key Register' will comply with the following: Key Usage: '73'; Algorithm: 'D', 'T'; Mode of Use: '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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings) 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 9000.
  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 *payShield 9000 Australian Standards Reference 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 ø	Use the Rx variant of the command ø

* As described in this manual

ø As described in the *payShield 9000 Australian Standards Reference Manual*

For further details, see Chapter 12 of the *payShield 9000 General Information 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings). 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 Chapter 12 of the *payShield 9000 General Information 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		The Terminal Key Register, used to generate the MAC.
	16 H or 1 A + 32/48 H	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".
	or 1 A + n A	For a Keyblock LMK, the 'Terminal Key Register' must comply with the following: **Key Usage**: 'P0', '73'; **Algorithm**: 'D', 'T'; **Mode of Use**: '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.

Field	Length & Type	Details
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 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		The new Terminal Key Register, to replace the current one.
	16 H or 1 A + 32/48 H	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".
	or 1 A + n A	For a Keyblock LMK, the 'Terminal Key Register' will comply with the following: **Key Usage**: '73' **Algorithm**: 'D', 'T' **Mode of Use**: '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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings) 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 9000.
  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 *payShield 9000 Australian Standards Reference 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 ø	Use the Rx variant of the command ø

* As described in this manual

ø As described in the *payShield 9000 Australian Standards Reference Manual*The command used to respond to requests from terminals at the acquirer Host.

For further details, see Chapter 12 of the *payShield 9000 General Information Manual*.

Confirmation *(when selected Transaction Key Scheme is Racal)*

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings). 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 Chapter 12 of the *payShield 9000 General Information 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		The Terminal Key Register, used to verify the MAC.
	16 H or 1 A + 32/48 H	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".
	or 1 A + n A	For a Keyblock LMK, the 'Terminal Key Register' must comply with the following: **Key Usage**: 'P0', '73'; **Algorithm**: 'D', 'T'; **Mode of Use**: '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

Field	Length & Type	Details
		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 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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 (using the CS Console command or HSM Manager Initial Settings) 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 9000.
  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 *payShield 9000 Australian Standards Reference 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 ø	Use the Rx variant of the command ø

* As described in this manual

ø As described in the *payShield 9000 Australian Standards Reference Manual*The command used to respond to requests from terminals at the acquirer Host.

For further details, see Chapter 12 of the *payShield 9000 General Information Manual*.

Derived Unique Key Per Transaction (X9.24-1) Commands

The payShield 9000 HSM provides the following host commands to support DUKPT operations:

Command	Page
Translate a PIN from BDK to BDK or ZPK Encryption (3-DES DUKPT) (G0)	321
Verify a PIN Using the IBM Method (3-DES DUKPT) (GO)	324
Verify a PIN Using the VISA PVV Method (3-DES DUKPT) (GQ)	328
Verify a PIN Using the Diebold Method (3-DES DUKPT) (GS)	331
Verify a PIN Using the Encrypted PIN Method (3-DES DUKPT) (GU)	334
Generate/Verify a MAC (3-DES DUKPT) (GW)	337

The above commands are used to acquire transactions from terminals that support the DUKPT key management scheme (as defined in X9.24-1). 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, please refer to Message Encryption Commands.

The latest revision of the DUKPT standard (X9.24-1:2009) 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 type-1 BDK 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 type-2 BDK supports the unidirectional method.

The differences between the two types of BDKs are summarised in the table below.

<table>
<tr><th colspan="2">BDK Type</th><th>Description</th></tr>
<tr><td rowspan="2">Type-1</td><td>For a Variant LMK, the BDK is encrypted under LMK 28-29.</td><td rowspan="2">Variants are applied to the derived transaction key as follows:
<table>
<tr><th>Key function</th><th>Variant</th></tr>
<tr><td>PIN verification</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>
</table>
Note that this method will produce bidirectional MAC keys.</td></tr>
<tr><td>For a Keyblock LMK, the BDK must have Key Usage = 'B0'.</td></tr>
<tr><td rowspan="2">Type-2</td><td>For a Variant LMK, the BDK is encrypted under LMK 28-29 variant 6.</td><td rowspan="2">Variants are applied to the derived transaction key as follows:
<table>
<tr><th>Key function</th><th>Variant</th></tr>
<tr><td>PIN verification</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>
</table>
Note that this method will produce unidirectional MAC keys.</td></tr>
<tr><td>For a Keyblock LMK, the BDK must have Key Usage = '41'.</td></tr>
</table>

Further Information about DUKPT and its implementation on the payShield 9000 can be found in:

- Chapter 4 of *1270A542 payShield 9000 Host Programmer's Manual*
- Chapter 13 of *1270A593 payShield 9000 General Information Manual*.

Translate a PIN from BDK to BDK or ZPK Encryption (3-DES DUKPT)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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.

Notes: The PIN block format may also be changed.
The command performs the same function as CA and CC, except the Host supplies the HSM with the information necessary to compute the current key. The source PIN Block and source KSN originate from the PIN Pad.
The ANSI X9.24-1:2009 method for DUKPT PIN Key derivation is used.

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 type-2 BDK.
Source Key		The key used to decrypt the source PIN block. Two types of BDK are supported: type-1 BDK and type-2 BDK.
	32 H or 1 A + 32 H	For a Variant LMK: If the 'Source Key Flag' is not present, this key must be a type-1 BDK, encrypted under LMK pair 28-29. If the 'Source Key Flag' is present, this key must be a type-2 BDK, encrypted under LMK pair 28-29 variant 6.
	or 1 A + n A	For a Keyblock LMK: This key must be a type-1 or type-2 BDK, and comply with the following: Key Usage: 'B0', '41'; Algorithm: 'T'; Mode of Use: '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. Value '~' (X'7E). Optional; if present, this flag indicates that the destination key is a BDK-2.

Field	Length & Type	Details
		COMMAND MESSAGE
Destination Key		The key used to re-encrypt the destination PIN block. Three types of keys are supported: ZPK, BDK-1 and BDK-2.
	16 H or 1 A + 16/32/48 H	For a Variant LMK: If 'Destination Key Flag' is not present, then this key must be a ZPK, encrypted under LMK 06-07. If 'Destination Key Flag' is '*', then this key must be a BDK-1, encrypted under LMK 28-29. If 'Destination Key Flag' is '~', then this key must be a BDK-2, encrypted under LMK 28-29/6
	or 1 A + n A	For a Keyblock LMK: This key must be either a ZPK or BDK-1 or BDK-2, and comply with the following: Key Usage: 'P0', '72'; Algorithm: 'D', 'T'; Mode of Use: 'B', 'E', 'N' Key Usage: 'B0', '41'; Algorithm: 'T'; Mode of Use: 'X', 'N'
Source KSN descriptor	3 H	The descriptor for the Source KSN (Key Serial Number - in the next field). See the Host Programmer Manual for further information. 1st digit: Source BDK Identifier Length ('0' – 'F') 2nd ¬digit: Reserved. Should be '0'. 3rd digit: Device Identifier Length ('0' – 'F')
Source Key Serial Number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information.
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).
Source encrypted PIN Block	16 H	The Source PIN Block, encrypted using the 'Source Key', supplied by the POS PIN terminal.
Source PIN Block format Code	2 N	The format code for the 'Source encrypted PIN Block'. For a list of possible values, see the list of PIN Block Formats in Chapter 6 of the General Information Manual.
Destination PIN block format code	2 N	The format code for the 'Destination PIN Block'. For a list of possible values, see the list of PIN Block Formats in Chapter 6 of the General Information Manual.
Account Number	12 N or 18 H	If Destination PIN Block format = '01': The 12 right-most digits of the PAN excluding the check digit. If Destination PIN Block format = '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.

Field	Length & Type	Details
COMMAND MESSAGE		
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'G1'.
Error Code	2 A	'00' : No error '10' : BDK parity error '11' : Interchange key parity error '27' : BDK not double or triple length '68' : Command disabled '69' : PIN Block format has been disabled or a standard error code.
PIN Length	2 N	Length of the translated PIN.
Destination Encrypted PIN Block	16 H	The PIN block encrypted under the 'Destination 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.

Verify a PIN Using the IBM Method (3-DES DUKPT)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: Verify a PIN using the IBM 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.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues verifying the PIN using 3-DES 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 3-DES Keyblock LMK) or 'L' + 32 hexadecimal digits (for an AES Keyblock 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)
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
BDK		The Base Derivation Key, used to decrypt the PIN block and optionally verify the MAC. Two types of BDK are supported: type-1 BDK and type-2 BDK.
	32 H or 1 A + 32 H	For a Variant LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' … '3', this key must be a type-1 BDK, encrypted under LMK pair 28 29. If Mode = '2', or if Mode = '1' and MAC Mode = 'A' … 'C', this key must be a type-2 BDK, encrypted under LMK pair 28-29 variant 6.
	or 1 A + n A	For a Keyblock LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' … '3', this key must be a type-1 BDK, and comply with the following: **Key Usage**: 'B0'; **Algorithm**: 'T'; **Mode of Use**: 'X', 'N' If Mode = '2', or if Mode = '1' and MAC Mode = 'A' … 'C', this key must be a type-2 BDK, and comply with the following: **Key Usage**: '41'; **Algorithm**: 'T'; **Mode of Use**: 'X', 'N'
PVK		The PIN Verification Key, used to verify the customer PIN.
	16 H or 1 A + 16/32/48 H	For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.
	or 1 A + n A	For a Keyblock LMK, the 'PVK' must comply with the following: **Key Usage**: 'V1'; **Algorithm**: 'D', 'T'; **Mode of Use**: 'C', 'V', 'N'
KSN descriptor	3 H	The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information.
Key serial number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information.
PIN Block	16 H	Encrypted PIN block received from the POS PIN terminal.
PIN Block Format Code	2 N	Restricted to the following:

Field	Length & Type	Details
		'01' : ANSI X9.8 Format 0 '04' : Plus format '05' : ISO 9564-1 Format 1, ANSI X9.8 Format 1 '47' : ISO 9564-1 Format 3
Check Length	2 N	Minimum PIN Length: 4..12
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
Decimalization Table	16 N or 16 H or 1 A + 3 H or 1 A + 32 H	16 N when using Plaintext decimalization tables. 16 H when using Encrypted decimalization tables and a Variant LMK or 3-DES Keyblock 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 Keyblock LMK.
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 account number; 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'.
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 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 '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 VISA PVV Method (3-DES DUKPT)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: Verify a PIN using the VISA PVV method.
This command can optionally verify a MAC using a DUKPT MAC Key.

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.
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.
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
BDK		The Base Derivation Key, used to decrypt the PIN block and optionally verify the MAC. Two types of BDK are supported: type-1 BDK and type-2 BDK.
	32 H or 1 A + 32 H	For a Variant LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' … '3', this key must be a type-1 BDK, encrypted under LMK pair 28 29. If Mode = '2', or if Mode = '1' and MAC Mode = 'A' … 'C', this key must be a type-2 BDK, encrypted under LMK pair 28-29 variant 6.

Field	Length & Type	Details
	or 1 A + n A	For a Keyblock LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' … '3', this key must be a type-1 BDK, and comply with the following: Key Usage: 'B0'; Algorithm: 'T'; Mode of Use: 'X', 'N' If Mode = '2', or if Mode = '1' and MAC Mode = 'A' … 'C', this key must be a type-2 BDK, and comply with the following: Key Usage: '41'; Algorithm: 'T'; Mode of Use: 'X', 'N'
PVK		The PIN Verification Key, used to verify the customer PIN.
	32 H or 1 A + 32/48 H	For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.
	or 1 A + n A	For a Keyblock LMK, the 'PVK' must comply with the following: Key Usage: 'V2'; Algorithm: 'T'; Mode of Use: 'C', 'V', 'N'
KSN descriptor	3 H	The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information.
Key serial number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information.
PIN Block	16 H	The encrypted PIN block received from the POS PIN terminal.
PIN Block Format Code	2 N	Restricted to the following: '01' : ANSI X9.8 Format 0 '04' : Plus format '05' : ISO 9564-1 Format 1, ANSI X9.8 Format 1 '47' : ISO 9564-1 Format 3
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
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'.
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 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 '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 (3-DES DUKPT)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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.
- 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)
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.

Field	Length & Type	Details
MAC Method	1 N	Present only for Mode = '1'. '1' : ANSI X9.19
BDK		The Base Derivation Key, used to decrypt the PIN block and optionally verify the MAC. Two types of BDK are supported: type-1 BDK and type-2 BDK.
	32 H or 1 A + 32 H	For a Variant LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' … '3', this key must be a type-1 BDK, encrypted under LMK pair 28 29. If Mode = '2', or if Mode = '1' and MAC Mode = 'A' … 'C', this key must be a type-2 BDK, encrypted under LMK pair 28-29 variant 6.
	or 1 A + n A	For a Keyblock LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' … '3', this key must be a type-1 BDK, and comply with the following: Key Usage: 'B0'; Algorithm: 'T'; Mode of Use: 'X', 'N' If Mode = '2', or if Mode = '1' and MAC Mode = 'A' … 'C', this key must be a type-2 BDK, and comply with the following: Key Usage: '41'; Algorithm: 'T'; Mode of Use: '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). See the Host Programmer Manual for further information.
Key serial number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information.
PIN Block	16 H	The encrypted PIN block received from the POS PIN terminal.
PIN Block Format Code	2 N	Restricted to the following: '01' : ANSI X9.8 Format 0 '04' : Plus format '05' : ISO 9564-1 Format 1, ANSI X9.8 Format 1 '47' : ISO 9564-1 Format 3
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
PIN validation	16 H	User-defined data consisting of hexadecimal characters, and the letter N, which indicates where the HSM is to insert the last five digits of the account number specified in the Host request message. (The digits must be left-justified).
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'.

Field	Length & Type	Details
		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 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 (3-DES DUKPT)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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.
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.

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)
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
BDK		The Base Derivation Key, used to decrypt the PIN block and optionally verify the MAC. Two types of BDK are supported: type-1 BDK and type-2 BDK.
	32 H or 1 A + 32 H	For a Variant LMK: If Mode = '0', or if Mode = '1' and MAC Mode = '1' … '3', this key must be a type-1 BDK, encrypted under LMK pair 28 29. If Mode = '2', or if Mode = '1' and MAC Mode = 'A' … 'C', this key must be a type-2 BDK, encrypted under LMK pair 28-29 variant 6.

Field	Length & Type	Details
	or 1 A + n A	For a Keyblock LMK: If Mode = 'O', or if Mode = '1' and MAC Mode = '1' … '3', this key must be a type-1 BDK, and comply with the following: Key Usage: 'BO'; Algorithm: 'T'; Mode of Use: 'X', 'N' If Mode = '2', or if Mode = '1' and MAC Mode = 'A' … 'C', this key must be a type-2 BDK, and comply with the following: Key Usage: '41'; Algorithm: 'T'; Mode of Use: 'X', 'N'
KSN descriptor	3 H	The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information.
Key serial number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information.
PIN Block	16 H	The encrypted PIN block received from the POS PIN terminal.
PIN Block Format Code	2 N	Restricted to the following: '01' : ANSI X9.8 Format 0 '04' : Plus format '05' : ISO 9564-1 Format 1, ANSI X9.8 Format 1 '47' : ISO 9564-1 Format 3
Account Number	12 N or 18 H	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the account number, excluding the check digit. For PIN Block format 04, this is an 18 digit field consisting of the account number, excluding the check digit, right-justified and padded with X'F on the left if necessary.
PIN	L N or L H or 1 A + 32 H	The PIN from the host database, encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' 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 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 (3-DES DUKPT)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
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.

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	Indicates the mode of operation: '1' & 'A' : Verify 8 byte MAC '2' & 'B' : Verify Approval MAC (4 leftmost bytes of MAC) '3' & 'C' : Verify Decline MAC (4 rightmost bytes of MAC) '4' & 'D' : Generate 8 byte MAC '5' & 'E' : Generate Approval MAC (4 leftmost bytes of MAC) '6' & 'F' : Generate Decline MAC (4 rightmost bytes of MAC) Use '1' … '6' when using bidirectional MAC keys. Use 'A' … 'F' when using unidirectional MAC keys.
MAC Method	1 N	Indicates the MAC algorithm: '1' : ANSI X9.19
BDK		The Base Derivation Key, used to derive the MAC key. Two types of BDK are supported: type-1 BDK and type-2 BDK.
	32 H or 1 A + 32 H	For a Variant LMK: For MAC Mode = '1' … '6', this key must be a type-1 BDK, encrypted under LMK pair 28 29. For MAC Mode = 'A' … 'F', this key must be a type-2 BDK, encrypted under LMK pair 28-29 variant 6.
	or 1 A + n A	For a Keyblock LMK: For MAC Mode = '1' … '6', this key must be a type-1 BDK, and comply with the following: Key Usage: 'B0'; Algorithm: 'T'; Mode of Use: 'X', 'N' For MAC Mode = 'A' … 'F', this key must be a type-2 BDK, and comply with the following: Key Usage: '41'; Algorithm: 'T'; Mode of Use: 'X', 'N'
KSN Descriptor	3 H	The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information.
Key Serial Number	12 – 20 H	The KSN supplied by the PIN Pad. See the Host Programmer

Field	Length & Type	Details
COMMAND MESSAGE		
		Manual for further information.
MAC	8 H or 16 H	Only present for MAC Mode = '1', '2', '3', 'A', 'B', or 'C'. 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	Length of next field in bytes. Must be multiple of 8 bytes
Message Data	n B	Data for which MAC is to be generated/verified.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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	Only present if MAC Mode is '4', '5', '6', 'D', 'E' or 'F'. The MAC generated on the Message Data: 16 H if MAC Mode is '4' or 'D'. 8 H if MAC Mode is '5', '6', 'E' or '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.

RSA Cryptosystem Commands

Use of the RSA cryptosystem requires the optional RSA license. To see full details refer to section 5 of the Host Programmers Manual.

The payShield 9000 HSM provides the following host commands to support RSA operations:

Command	Page
Generate a Public/Private Key Pair (EI)	340
Load a Private Key (EK)	343
Translate a Private Key (EM)	345
Import a Public Key (EO)	347
Validate a Public Key (EQ)	350
Validate a Certificate and Import the Public Key (ES)	352
Translate a Public Key (EU)	355
Generate an RSA Signature (EW)	357
Validate an RSA Signature (EY)	359
Import Key or data under an RSA Public Key (GI)	361
Export Key under an RSA Public Key (GK)	369
Hash a Block of Data (GM)	374

Generate a Public/Private Key Pair

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001** & **LIC002**	
Authorization: **Required** Activity: **generate.rsa.host**	

Function: Generate a public/private key pair.

Notes: Depending on key size, the function may take several seconds 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.

HSM9-LIC019 is required in order to generate keys with Key Type Indicator=4 to allow general purpose decryption/encryption of random data.

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

See: *payShield 9000 Host Programmer's Manual: The RSA Cryptosystem* for more information.

For Keyblock LMKs, the RSA Private Key is created in a keyblock format, with the following attributes:

Field	Value
Key Usage	'03'
Algorithm	'R'
Mode Of Use	Inferred from 'Key Type' parameter
Exportability	'N'
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	1 N	Key Type indicator: '0' : Signature only '1' : Key management only '2' : Both signature and key management '3' : Integrated Chip Card (ICC) Key '4' : allows general purpose decryption of data (e.g. TLS/SSL premaster secret) – requires HSM9-LIC019
Key length	4 N	Modulus length in bits. Range: '0320' … '2048'.
Public key encoding	2 N	Encoding rules for public key (must allow public key length to be inferred). '01' : DER encoding for ASN.1 Public Key (INTEGER uses unsigned representation). '02' : DER encoding for ASN.1 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 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.
For generating a Keyblock RSA private key only: Delimiter	1 A	Value '#'. Optional; must be present if using a Keyblock LMK; if present, the following fields must be present.
For generating a Keyblock RSA private key 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.
For generating a Keyblock RSA private key only: 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 generating a Keyblock RSA private key only: 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.		
For generating a Keyblock RSA private key only: Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.
For generating a Keyblock RSA private key only: 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.
For generating a Keyblock RSA private key only: 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 '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 '68' : Command disabled or a standard error code.
Public key	n B	Public key, encoded appropriately.
Private Key length	4 N	For a Variant LMK: Length (in bytes) of the next field.
	or 4 H	For a Keyblock LMK: This field is reserved, and set to 'FFFF'.
Private Key		The Private Key, encrypted under the LMK.
	n B	For a Variant LMK, the private key is encrypted under LMK pair 34-35.
	or 1 A + n B	For a Keyblock LMK, the private 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.

Load a Private Key

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001** & **LIC002**	
Authorization: **Not required**	

Function: Load a private key (encrypted under the LMK) into the HSM's tamper-protected 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.
See: *payShield 9000 Host Programmer's Manual: The RSA Cryptosystem* for more information.

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	For a Variant LMK: Length (in bytes) of the next field.
	or 4 H	For a Keyblock LMK: This field is ignored; should be set to 'FFFF'.
Private Key		The RSA Private Key to be loaded and stored inside the HSM.
	n B	For a Variant LMK, the 'Private Key' must be encrypted under LMK pair 34-35.
	or 1 A + n B	For a Keyblock LMK, the 'Private Key' must comply with the following: **Key Usage**: '03'; **Algorithm**: 'R'; **Mode of Use**: 'S', 'D', 'N'
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001** & **LIC002**	
Authorization: **Not required**	

Function: Translate a private key from encryption under the old LMK held in key change storage, to encryption under a new LMK.

Note: See: *payShield 9000 Host Programmer's Manual: The RSA Cryptosystem* for more information.

For translations from encryption under Variant LMK to a Keyblock LMK, the RSA Private Key is re-created in a keyblock format, with the following attributes:

Field	Value
Key Usage	'03'
Algorithm	'R'
Mode Of Use	Inferred from the input key's type
Exportability	'N'
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 Keyblock LMK: This field is ignored, and should be set to 'FFFF'.
Private key		The Private Key to be translated.
	n B	For a Variant LMK, the 'Private Key' must be encrypted under LMK pair 34-35.
	or 1 A + n B	For a Keyblock LMK, the 'Private Key' must comply with the following: Key Usage: '03'; Algorithm: 'R'; Mode of Use: 'S', 'D', 'N'
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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
For translation from variant LMK to keyblock LMK	Delimiter	1 A	Value '#'. Optional; must be present if translating the Private Key from encrypted under a Variant LMK to a Keyblock 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.
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 '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 Keyblock LMK: This field is reserved, and set to 'FFFF'.
Private key		The translated RSA Private Key.
	n B	For a Variant LMK, the 'Private Key' is encrypted under current LMK pair 34-35.
	or 1 A + n B	For a Keyblock 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001** & **LIC002**	
Authorization: **Required** Activity: **import.rsa.host**	

Function: Import a Public Key by either generating a MAC on it, using the LMK or by creating a keyblock.

Note: This command was previously named "Generate a MAC on an RSA Public Key".

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

WARNING: This command should not be used to generate a MAC/keyblock on a public key for which the corresponding private key exists encrypted under the LMK.

See: *payShield 9000 Host Programmer's Manual: The RSA Cryptosystem* for more information.

For Keyblock LMKs, the RSA Public Key is created in a keyblock format, with the following attributes:

Field	Value
Key Usage	'02'
Algorithm	'R'
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 'E0'.
Public Key Encoding		2 N	Encoding rules for public key (must allow public key length to be inferred). '01' : DER encoding for ASN.1 Public Key (INTEGER using unsigned representation). '02' : DER encoding for ASN.1 Public Key (INTEGER using 2's complement representation).
Public key		n B	Public key, DER encoded in ASN.1 format (sequence of modulus, exponent).
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. This field is used to terminate the previous two variable length fields.
Delimiter		1 A	Value '%'. Optional; if present, the following field must 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.
Applies only when using a Keyblock LMK.	Delimiter	1 A	Value '#'. Required when using a Keyblock LMK. If present, the following fields must be present.
	Mode of Use	1 A	Mode of Use field, to be included in the keyblock 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 Chapter 5 of the General Information Manual.
	Key Version Number	2 N	Key Version Number field, to be included in the keyblock 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 keyblock header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in Chapter 5 of the General Information Manual.
	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 or a standard error code.
Variant LMK: MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.
Public Key		The imported Public Key.
	n B	For a Variant LMK, the 'Public Key' is DER encoded in ASN.1 format (sequence of modulus, exponent).
	or 1 A + n B	For a Keyblock LMK, the 'Public Key' is stored (without encryption) in keyblock 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.

Validate a Public Key

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001** & **LIC002**	
Authorization: **Not required**	

Function: Validate a public key.

Note: See: *payShield 9000 Host Programmer's Manual: The RSA Cryptosystem* for more information.

Field		Length & Type	Details
COMMAND MESSAGE			
Message Header		m A	Subsequently returned to the Host unchanged.
Command Code		2 A	Value 'EQ'.
Variant LMK	MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.
Variant LMK	Public key	n B	The Public key; DER encoded in ASN.1 format (sequence of modulus, exponent).
Variant LMK	Authentication data	n B	Optional. Additional data included in the MAC calculation (must not include ';' or '~').
Variant LMK	Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present. Used to terminate all previous fields.
Keyblock LMK	Public Key	1 A + n B	The 'Public Key', in keyblock format; must comply with the following:

Key Usage	Algorithm	Mode of Use
'02'	'R'	'S', 'B', 'E', 'N'

Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001** & **LIC002**	
Authorization: **Not required**	

Function: Validate a certificate and import the public key contained within the certificate.

Notes: The command can (optionally) check whether the public key in the certificate corresponds to a private key encrypted under the LMK. See: *payShield 9000 Host Programmer's Manual: The RSA Cryptosystem* for more information.

Field		Length & Type	Details
COMMAND MESSAGE			
Message Header		m A	Subsequently returned to the Host unchanged.
Command Code		2 A	Value 'ES'.
Variant LMK	MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.
Variant LMK	Public Key	n B	The Public Key used to validate the certificate; DER encoded in ASN.1 format (sequence of modulus, exponent).
Variant LMK	Authentication data	n B	Optional. Additional data included in the MAC calculation (must not include ';' or '~').
Variant LMK	Delimiter	1 A	Value ';'. Used to indicate the end of the authentication data field.
Keyblock LMK	Public Key	1 A + n B	The Public Key used to validate the certificate; must be in keyblock format, and comply with the following: **Key Usage**: '02'; **Algorithm**: 'R'; **Mode of Use**: '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.

Field		Length & Type	Details
Pad mode identifier		2 N	Identifier of the pad mode used in certificate signature generation. '01' : PKCS#1 v1.5 method (EME-PKCS1-v1_5)
Public key encoding		2 N	Encoding rules for the public key contained in the certificate (must allow the public key length to be inferred).
Public key offset		4 N	Offset to the first byte of the public key field contained in the certificate
Variant LMK	Authentication data	n B	Optional. Additional data to be included in the MAC calculation (must not include ';').
Variant LMK	Delimiter	1 A	Value ';'. Used to indicate the end of the authentication data field.
Private Key length			Optional. Must be present if the Private Key field is present.
		4 N	For a Variant LMK: Length (in bytes) of the next field.
		or 4 H	For a Keyblock LMK: This field is ignored, and should be set to 'FFFF'.
Private Key			Optional. The Private Key that should correspond to the public key contained within the certificate.
		n B	For a Variant LMK, the 'Private Key' is encrypted under LMK pair 34-35.
		or 1 A + n B	For a Keyblock LMK, the 'Private Key' must comply with the following: Key Usage: '03'; Algorithm: 'R'; Mode of Use: 'S', 'D', 'N'
Delimiter		1 A	Value '%'. Optional; if present, the following field must 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.
Applies only when using a Keyblock LMK.	Delimiter	1 A	Value '#'. Required when using a Keyblock LMK. If present, the following fields must be present.
Applies only when using a Keyblock LMK.	Mode of Use	1 A	Mode of Use field, to be included in the keyblock 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 Chapter 5 of the General Information Manual. Note: The value supplied must be compatible with the Mode Of Use of the Private Key (if supplied).
Applies only when using a Keyblock LMK.	Key Version Number	2 N	Key Version Number field, to be included in the keyblock header; permitted values: '00' to '99'; must be present if the above Delimiter is present.
Applies only when using a Keyblock LMK.	Exportability	1 A	Exportability field, to be included in the keyblock header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in Chapter 5 of the General Information Manual.
Applies only when using a Keyblock LMK.	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.
Applies only when using a Keyblock LMK.	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.		
Applies only when using a Keyblock LMK.	Optional Block Identifier	2 A	Optional Block Identifier; any permitted value except 'PB'.

Field	Length & Type	Details
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 '85' : Invalid OAEP Mask Generation Function '86' : Invalid OAEP MGF Hash Function '87' : OAEP Parameter Error '88' : OAEP Error or a standard error code.
Variant LMK: MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.
Public key		The imported Public Key.
	n B	For a Variant LMK, the 'Public Key' is DER encoded in ASN.1 format (sequence of modulus, exponent).
	or 1 A + n B	For a Keyblock LMK, the 'Public Key' is stored (without encryption) in keyblock 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 ☑	Keyblock LMK ☑
License: **HSM9-LIC001** & **LIC002**	
Authorization: **Not required**	

Function: Translate a public key from an old LMK, held in key change storage, to a new LMK.

Note: See: *payShield 9000 Host Programmer's Manual: The RSA Cryptosystem* for more information.

Field		Length & Type	Details
COMMAND MESSAGE			
Message Header		m A	Subsequently returned to the Host unchanged.
Command Code		2 A	Value 'EU'.
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 '~').
Keyblock LMK	Public Key	1 A + n B	The Public Key; must be in keyblock format (using the old LMK), and comply with the following: **Key Usage**: '02'; **Algorithm**: 'R'; **Mode of Use**: 'S', 'B', 'E', 'N'
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 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.
Only when translating from an old variant LMK to a new keyblock LMK.	Delimiter	1 A	Value '#'. Required when using a Keyblock LMK. If present, the following fields must be present.
	Mode of Use	1 A	Mode of Use field, to be included in the keyblock 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 Chapter 5 of the General Information Manual.
	Key Version Number	2 N	Key Version Number field, to be included in the keyblock 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 keyblock header; any permitted value; must be present if the above Delimiter is present. For a list of possible values, see the Exportability Table in Chapter 5 of the General Information Manual.
	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.		

Field		Length & Type	Details
	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 '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.
Variant LMK	MAC	4 B	MAC on the public key and authentication data, calculated using the current LMK pair 36-37.
Keyblock LMK	Public key	1 A + n B	The translated Public Key, stored (without encryption) in keyblock 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.

Generate an RSA Signature

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC008** & **LIC002**	
Authorization: **Not required**	

Function: Generate a signature on a message using a private key.

Note:
- See: *payShield 9000 Host Programmer's Manual: The RSA Cryptosystem* for more information.
- Minimum private key lengths for use with the various Hash Identifiers are as follows:
  - '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
  - '07' : SHA-384 624 bits
  - '08' : SHA-512 752 bits

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 '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
Pad Mode identifier	2 N	Identifier of the padding mode used in signature generation. '01' : PKCS#1 v1.5 method (EME-PKCS1-v1_5)
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		Optional. Must be present if the Private key flag = '99'.

	4 N	For a Variant LMK: Length (in bytes) of the next field.
	or 4 H	For a Keyblock LMK: This field is ignored, and should be set to 'FFFF'.
Private Key		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.
	or 1 A + n B	For a Keyblock LMK, the 'Private Key' must comply with the following: Key Usage: '03'; Algorithm: 'R'; Mode of Use: 'S', 'N'
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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	'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 '85' : Invalid OAEP Mask Generation Function '86' : Invalid OAEP MGF Hash Function '87' : OAEP Parameter Error '88' : OAEP Error or a standard error code.
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 Signature

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC008** & **LIC002**	
Authorization: **Not required**	

Function: Validate a signature on a message using a public key.

Note: See: *payShield 9000 Host Programmer's Manual: The RSA Cryptosystem* for more information.

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
Pad mode identifier		2 N	Identifier of the pad mode used in signature generation. '01' : PKCS#1 v1.5 method (EME-PKCS1-v1_5)
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.
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.
Variant LMK	MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.
Variant LMK	Public Key	n B	The Public Key used to validate the signature; DER encoded in ASN.1 format (sequence of modulus, exponent).
Variant LMK	Authentication data	n B	Optional. Additional data included in the MAC calculation (must not include ';' or '~').
Variant LMK	Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present.

Field	Length & Type	Details
Keyblock LMK: Public Key	1 A + n B	The Public Key used to validate the signature; must be in keyblock format, and comply with the following: Key Usage: '02'; Algorithm: 'R'; Mode of Use: 'S', 'B', 'N'
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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	'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 '85' : Invalid OAEP Mask Generation Function '86' : Invalid OAEP MGF Hash Function '87' : OAEP Parameter Error '88' : OAEP 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.

Import Key or data under an RSA Public Key

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001** & **LIC002** (Optional: **LIC019**)	
Authorization: See Text Activity: **command.gi.host**	

Function: To translate a DES 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 a Type 4 RSA key pair: this requires optional license LIC019

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/No)
```

Refer to the Key Type Table in Chapter 4 of the General Information Manual for key types and restrictions on key import.

See: *payShield 9000 Host Programmer's Manual: The RSA Cryptosystem* for more information.

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 : OAEP (EME-OAEP-ENCODE).
Mask Generation Function	2 N	Identifier of the Mask Generation Function: '01' : MGF1 as defined in PKCS#1 v2.0 (see Reference 3). Optional, only present if Pad Mode Identifier is 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 is 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 is 02 (OAEP).

Field		Length & Type	Details
OAEP Encoding Parameters		n B	Optional, only present if Pad Mode Identifier is 02 (OAEP). If present, this field should be encoded according to Reference 1 section 11.2.1. 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 ';'. Optional, only present if Pad Mode Identifier is 02 (OAEP).
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' (requires LIC019), Key Type should have the value '3400'.
		or 4 H	For a Keyblock LMK: This field is ignored; should be set to 'FFFF'.
Only present when the 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 (EME-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.
	Variant LMK: MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.

Field			Length & Type	Details
		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.
	Keyblock LMK	Public Key	1 A + n B	The Public Key used to validate the signature; must be in keyblock format, and comply with the following: Key Usage: '02'; Algorithm: 'R'; Mode of Use: '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: the encrypted key, or the signed data block containing the encrypted key, or the data (e.g. TLS/SSL premaster secret) when RSA Key Type Indicator is '04' (requires LIC019).
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				Optional. Must be present if the Private key flag = '99'.
			4 N	For a Variant LMK: Length (in bytes) of the next field.
			or 4 H	For a Keyblock LMK: This field is ignored, and should be set to 'FFFF'.
Private Key				Optional. Must be present if the Private Key Flag = '99'. The Private Key, used to decrypt the imported key.
			n B	For a Variant LMK, the 'Private Key' is encrypted under LMK pair 34-35.
			or 1 A + n B	For a Keyblock LMK, the 'Private Key' must comply with the following: Key Usage: '03'; Algorithm: 'R'; Mode of Use: 'D', 'N'
Only supplied when importing a DES/3-DES Key	Delimiter		1 A	Only present if the following fields are also present. Value ';'.
	Reserved		1 A	Ignored. If present must be '0'. Only present if importing a DES/3-DES key. Field not required for data (e.g. TLS/SSL premaster) decryption when using RSA Key Type Indicator '04' (requires LIC019)
	Key Scheme LMK		1 A	Key Scheme for imported key when encrypted under LMK. Only present if importing a DES/3-DES key. Field not required for data (e.g. TLS/SSL premaster) decryption when using RSA Key Type Indicator '04' (requires LIC019).

Field		Length & Type	Details
	Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV Only present if importing a DES/3-DES key. Field not required for data (e.g.TLS/SSL premaster) decryption when using RSA Key Type Indicator '04' (requires LIC019).
Only supplied when importing an HMAC key	Delimiter	1 A	Only present if the following HMAC fields are also present. For a Variant LMK: Value '#' or '|' (ASCII X'7C). For a Keyblock LMK: Value '|' (ASCII X'7C).
	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.
	HMAC Key Usage	2 N	Key Usage value identifier: '01' : HMAC Generation '02' : HMAC Verification '03' : HMAC Generation and Verification
	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 Keyblock LMK: '04' : Thales Keyblock format.
Delimiter		1 A	Value '='. Only present if the Key Block Type follows. Note: The '=' delimiter is used to distinguish from the normal ';' delimiter.
Key Block Type		2 N	'01' : Key Block format supported in existing firmware. '02' : Key Block Template (format of template is specified below). '03' : Unformatted Key Block. '04' : ASN.1 Encoded Key Block. Key Block Types '01', '02', and '03' may be used for importing DES keys. Key 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 Block Type will be '01'.
Key Block Template Length		4 N	Length of Key Block data. Only present if Key Block Type = '02'.
Key Block Template		n H	Key Block, DER encoded in ASN.1 format. Key data zero filled. Only present if Key Block Type = '02'.

Field		Length & Type	Details
Delimiter		1 A	Value ';'. Only present if Key Block Type = '02'.
Key Length		2 A	Length of the Key within the Key Block. Only present if Key Block Type is '02'.
Key Offset		4 N	Offset to the location of the Key within the Key Block. Only present if Key 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 Block Type = '02' then Check Value is expected at position indicated by Check Value Offset. Only present when importing DES keys and if Key Block Type = '02'.
Check value offset		4 N	Offset to the location of the check value within the Key Block. If Check Value length is '00' then this field is ignored. Only present when importing DES keys and if Key Block Type = '02'.
Delimiter		1 A	Value '%'. Optional; if present, the following field must 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 importing a DES/3-DES key to keyblock format	Delimiter	1 A	Value '#'. Optional; can only be present when importing a DES/3-DES key, and returning it in keyblock 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 Chapter 5 of the General Information Manual.
	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 Chapter 5 of the General Information Manual.
	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.
HMAC key to keyblo	Delimiter	1 A	Value '#'. Optional; can only be present when importing an HMAC key, and returning it in keyblock format; if present, the following fields must be 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 '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	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		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'GJ'.
Error Code	2 A	'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 keyblock 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 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 '88' : OAEP Error or a standard error code.

Field		Length & Type	Details
When importing a DES/3-DES key	Initialization value	16 H	Initialization value for the DES key. Optional. Only present if Key Block Type = '01'.
	DES Key		The imported DES Key, encrypted under the LMK.
		16 / 32 H or 1 A + 32/48 H	For a Variant LMK, the 'Key' is encrypted under the appropriate LMK pair/variant (as defined by the 'Key Type').
		or 1 A + n A	For a Keyblock LMK, the 'Key' is encrypted under the LMK.
	Key Check Value	16 / 6 H	Result of encrypting 64 binary zeros with the 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	HMAC Key Length	4 N	For a Variant LMK: Length (in bytes) of the next field.
		or 4 H	For a Keyblock LMK: This field is reserved, and set to 'FFFF'.
	HMAC Key		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 Keyblock LMK, the 'HMAC Key' is encrypted under the LMK.
Note 1	TLS Data Length	4 N	Data or TLS/SSL clear-text premaster length (requires LIC019)
	TLS Data	n B	Data or TLS/SSL clear-text premaster (requires LIC019)
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.

Notes:

1. These fields are provided when importing data (e.g. TLS/SSL premaster secret) using RSA Key Type Indicator '04' (requires Optional License LIC019).

Export Key under an RSA Public Key

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC001** & **LIC002**	
Authorization: **Not required**	

Function: Translate a DES 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: This command does not require Authorized state, but uses the Key Type Table to determine whether the key can be exported.
See: *payShield 9000 Host Programmer's Manual: The RSA Cryptosystem* for more information.

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' : OAEP (EME-OAEP-ENCODE)
Mask Generation Function	2 N	Identifier of the mask generation function: '01' : MGF1 as defined in PKCS#1 v2.0 (see Reference 3). Optional, only present if Pad Mode Identifier is 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 Reference 1 section 11.2.1. 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 ';'. Optional, only present if Pad Mode Identifier = '02' (OAEP).

Field		Length & Type	Details
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 Keyblock LMK: This field is ignored; should be set to 'FFFF'.
Only present 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 (EME-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	n B	Block of data to be pre-pended to the encrypted key, prior to signing.
	Delimiter	1 A	Value ';'.
	Footer Data Block Length	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	n B	Block of data to be appended to the encrypted key, prior to signing.
	Delimiter	1 A	Value ';'.
	Private Key Flag	2 N	Flag to indicate location of the private key; '00' … '20' : index of stored private key '99' : use private key provided with command
	Private Key Length		Optional. Must be present if Private Key Flag = '99'.
		4 N	For a Variant LMK: Length (in bytes) of the next field.
		or 4 H	For a Keyblock LMK: This field is ignored, and should be set to 'FFFF'.
	Private Key		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
		or 1 A + n B	For a Keyblock LMK, the 'Private Key' must comply with the following: Key Usage: '03'; Algorithm: 'R'; Mode of Use: 'S', 'N'
	Delimiter	1 A	Optional. Must be present if the Private Key Flag = '99'. Value ';'.
When exporting a DES/3-DES 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
		1 A	For a Keyblock LMK: This field is ignored, and should be set to 'F'.
	DES Key (under LMK)		The DES key to be exported, encrypted under the LMK.
		16 / 32 H or 1 A + 32/48 H	For a Variant LMK, the 'Key' must be encrypted under the appropriate LMK pair/variant (as defined by the 'Key Type').
		or 1 A + n A	For a Keyblock LMK, the 'Key' must be encrypted under the LMK.
	Check Value	16 H	Check value on DES key.
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.
			For a Keyblock LMK: '04' : Thales Keyblock format.
	HMAC Key Length	4 N	For a Variant LMK: Length (in bytes) of the next field.
		or 4 H	For a Keyblock LMK: This field is reserved, and set to 'FFFF'.
	HMAC Key (under LMK)		The HMAC key to be exported, 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 Keyblock LMK, the 'HMAC Key' is encrypted under the LMK.
	Delimiter	1 A	Value ';'.
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 '~').
Keyblock LMK	Public Key	1 A + n B	The Public Key used to encrypt the key to be exported; must be in keyblock format, and comply with the following: Key Usage: '02'; Algorithm: 'R'; Mode of Use: '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' : Key Block format supported in existing 5.05 firmware. '02' : Key Block Template (format of template is specified below). '03' : Unformatted Key Block. '04' : ASN.1 Encoded Key Block. Key Block Types '01', '02', and '03' may be used for exporting DES keys. Key Block Types '02', '03', and '04' may be used for exporting HMAC keys. This field is optional. When not present, the value of Key Block Type will be '01'.
Key Block Template Length	4 N	Length of Key Block data. Optional, only present if Key Block Type = '02'.
Key Block Template	n H	Key Block, DER encoded in ASN.1 format. Key data and Check Value data (if present) zero filled. Optional, only present if Key Block Type = '02'.
Delimiter	1 A	Value ';'. Optional, only present if Key Block Type = '02'.
Key Offset	4 N	Offset to the position within the Key Block to insert the key. Optional, only present if Key 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 Block, inserted at the position indicated by Check Value Offset. Optional, only present when exporting DES keys and if Key Block Type = '02'.
Check Value Offset	4 N	Offset to the position within the Key Block to insert a check value. If Check Value length = '00', then this field is ignored. Optional, only present when exporting DES keys and if Key Block Type = '02'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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	'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 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 Block length error '78' : Private key length error '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 '88' : OAEP Error or a standard error code.
Initialization value	16 H	Initialization value for DES key. Only present when exporting a DES/3-DES key using Key Block Type '01'.
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.

Hash a Block of Data

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC008**	
Authorization: **Not required**	

Function: Hash a block of data.

Notes: See: *payShield 9000 Host Programmer's Manual: The RSA Cryptosystem* for more information.

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	Length of the message data to be hashed.
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.

VISA Cash Commands

The payShield 9000 HSM provides the following host commands to support the VISA Cash functions:

Notes:

The use of the $ALGL_{IEP}$ and VKL_{IEP} fields in following commands deserves special mention as these fields are optional. There are three scenarios controlled by these fields.

Scenario	Applicable Visa Cash cards	Single or Double length KDL used	Additional Notes
Neither VKL_{IEP} or $ALGL_{IEP}$ supplied to HSM	Version 1.5 and earlier DES cards	Single	May be used with cards which do not report VKL_{IEP} or $ALGL_{IEP}$. Backwards compatible with earlier versions of firmware
Only VKL_{IEP} supplied to HSM	Version 1.6 DES cards and Public Key cards	Double	May be used with later cards. Host must determine the value of $ALGL_{IEP}$ and supply VKL_{IEP} if required. Backwards compatible with earlier versions of firmware
Both VKL_{IEP} and $ALGL_{IEP}$ supplied to HSM	Any card.	Single if $ALGL_{IEP}$ has value 01, double if $ALGL_{IEP}$ has value 04	Allows host to send both $ALGL_{IEP}$ and VKL_{IEP} without concern about their values. VKL_{IEP} must always be supplied as a placeholder even if its value is not relevant (ie when $ALGL_{IEP}$ is of value 01)

This set of scenarios accommodates all relevant combinations of Visa Cash cards and allows the host application to operate in one of two modes.

Host makes the decision about what $ALGL_{IEP}$ is relevant for the current transaction and either supplies VKL_{IEP} if $ALGL_{IEP}$ is of value 04, or does not supply VKL_{IEP} if $ALGL_{IEP}$ is of value 01. $ALGL_{IEP}$ itself is not sent to the HSM. Thus the first and second scenarios in the above table can be used to cater for all cards in use. This mode of operation is used by some (earlier) host systems and therefore must be supported for backwards compatibility. Note that earlier Visa Cash cards do not report a value of $ALGL_{IEP}$ and so the host may have to determine this in other ways. Reference 4 discusses this point.

Host simply passes values of $ALGL_{IEP}$ and VKL_{IEP} to HSM as supplied in the current transaction. Thus if a card does not supply $ALGL_{IEP}$ or VKL_{IEP} no values are passed to the HSM and vice versa. Thus the first and third scenarios in the above table will be used. In this mode of operation the host is not required to make any decisions about the transaction; these are left to the HSM.

If Visa specifies alternative processing requirements in the future (and hence values of $ALGL_{IEP}$ other than 1 or 4) the HSM will be upgraded to accommodate them.

The earlier Visa Cash cards which do not report $ALGL_{IEP}$ or VKL_{IEP} will all eventually expire making the first scenario in the above table redundant.

The payShield 9000 HSM provides the following host commands to support VISA Cash operations:

Command	Page
Verify Load Signature S1 and Generate Load Signature S2 (DM)	377
Verify Load Completion Signature S3 (DO)	379
Verify Unload Signature S1 and Generate Unload Signature S2 (DQ)	381
Verify Unload Completion Signature S3 (DS)	383

Verify Load Signature S_1 and Generate Load Signature S_2

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC028**	
Authorization: **Not required**	

Function: Verify Load Signature S_1 and generate Load Signature S_2 .

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DM'.
KML	32 H or 1 A + 32/48 H	KML, encrypted under Variant 2 of LMK pair 04-05.
BIN_{IEP}	6 H	IEP Issuer Visa assigned BIN.
ID_{EP}	10 H	IEP Serial number.
$DEXP_{IEP}$	6 H	IEP Expiration date (YYMMDD format).
NT_{IEP}	4 H	IEP Transaction counter.
M_{LDA}	8 H	Amount to be loaded.
$CURR_{LDA}$	4 H	Load device currency code.
$CEXP_{LDA}$	2 H	Load device currency exponent.
BAL_{IEP}	8 H	IEP Current balance.
ID_{ACQ}	8 H	Acquirer BIN.
R	8 H	Random number.
S_1	16 H	Load request signature for validation.
VKL_{IEP}	2 H	Optional. Load Key version. If present but $ALGL_{IEP}$ not present, then a double length KDL will be used; see Notes in Introduction. Must be present if $ALGL_{IEP}$ is present.
$ALGL_{IEP}$	2 H	Optional. Load Algorithm. Can only take the values '01' and '04'. If set to '01' a single length KDL is used and VKL_{IEP} is ignored. If '04', a double length KDL is used and VKL_{IEP} is used.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'DN'.
Error Code	2 A	'00' : No error '01' : S_1 verification failure '03' : Invalid $ALGL_{IEP}$ '10' : KML parity error '68' : Command disabled or a standard error code.
S_2	16 H	Returned load 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.

Verify Load Completion Signature S_3

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC028**	
Authorization: **Not required**	

Function: Verify Load Completion Signature S_3 .

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'D0'.
KML	32 H or 1 A + 32/48 H	KML, encrypted under Variant 2 of LMK pair 04-05.
BIN_{IEP}	6 H	IEP Issuer Visa assigned BIN.
ID_{IEP}	10 H	IEP Serial number.
$DEXP_{IEP}$	6 H	IEP Expiration date (YYMMDD format).
NT_{IEP}	4 H	IEP Transaction counter.
ID_{ACQ}	8 H	Acquirer BIN.
R	8 H	Random number.
CC_{IEP}	4 H	Completion code.
S_3	16 H	Load completion signature for validation.
VKL_{IEP}	2 H	Optional. Load Key version. If present but $ALGL_{IEP}$ not present, then a double length KDL will be used; see Notes in Introduction. Must be present if $ALGL_{IEP}$ is present.
$ALGL_{IEP}$	2 H	Optional. Load Algorithm. Can only take the values '01' and '04'. If set to '01' a single length KDL is used and VKL_{IEP} is ignored. If '04', a double length KDL is used and VKL_{IEP} is used.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'DP'.
Error Code	2 A	'00' : No error '01' : S_3 verification failure '03' : Invalid $ALGL_{IEP}$ '10' : KML 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.

Verify Unload Signature S_1 and Generate Unload Signature S_2

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC028**	
Authorization: **Not required**	

Function: Verify Unload Signature S_1 and generate Unload Signature S_2 .

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DQ'.
KML	32 H or 1 A + 32/48 H	KML, encrypted under Variant 2 of LMK pair 04-05.
BIN_{EP}	6 H	IEP Issuer Visa assigned BIN.
ID_{EP}	10 H	IEP Serial number.
$DEXP_{IEP}$	6 H	IEP Expiration date (YYMMDD format).
NT_{IEP}	4 H	IEP Transaction counter.
M_{LDA}	8 H	Amount to be unloaded.
$CURR_{LDA}$	4 H	Load device currency code.
$CEXP_{LDA}$	2 H	Load device currency exponent.
BAL_{EP}	8 H	IEP Current balance.
ID_{ACQ}	8 H	Acquirer BIN.
R	8 H	Random number.
S_1	16 H	Unload request signature for validation.
VKL_{IEP}	2 H	Optional. Load Key version. If present but $ALGL_{IEP}$ not present, then a double length KDL will be used; see Notes in Introduction. Must be present if $ALGL_{IEP}$ is present.
$ALGL_{IEP}$	2 H	Optional. Load Algorithm. Can only take the values '01' and '04'. If set to '01' a single length KDL is used and VKL_{IEP} is ignored. If '04', a double length KDL is used and VKL_{IEP} is used.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'DR'.
Error Code	2 A	'00' : No error '01' : S_1 verification failure '03' : Invalid $ALGL_{IEP}$ '10' : KML parity error '68' : Command disabled or a standard error code.
S_2	16 H	Returned unload 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.

Verify Unload Completion Signature S3

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC028**	
Authorization: **Not required**	

Function: Verify Unload Completion Signature S_3.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DS'.
KML	32 H or 1 A + 32/48 H	KML, encrypted under Variant 2 of LMK pair 04-05.
BIN_{IEP}	6 H	IEP Issuer Visa assigned BIN.
ID_{EP}	10 H	IEP Serial number.
$DEXP_{IEP}$	6 H	IEP Expiration date (YYMMDD format).
NT_{EP}	4 H	IEP Transaction counter.
ID_{ACQ}	8 H	Acquirer BIN.
R	8 H	Random number.
CC_{IEP}	4 H	Completion code.
S_3	16 H	Unload completion signature for validation.
VKL_{IEP}	2 H	Optional. Load Key version. If present but $ALGL_{IEP}$ not present, then a double length KDL will be used; see Notes in Introduction. Must be present if $ALGL_{IEP}$ is present.
$ALGL_{IEP}$	2 H	Optional. Load Algorithm. Can only take the values '01' and '04'. If set to '01' a single length KDL is used and VKL_{IEP} is ignored. If '04', a double length KDL is used and VKL_{IEP} is used.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'DT'.
Error Code	2 A	'00' : No error '01' : S_3 verification failure '03' : Invalid $ALGL_{IEP}$ '10' : KML 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.

Legacy Commands

The commands in this category exist in the software for legacy reasons. They have been superseded by newer (usually more generic) commands – refer to the individual commands for details. Whilst there are no plans to withdraw these commands from the payShield 9000, it is strongly recommended that new application software use the newer commands.

The payShield 9000 HSM provides the following host commands to support legacy operations:

Command	Page
Generate a CVK Pair (AS)	388
Generate and Print a TMK, TPK or PVK (OE) *	390
Generate a Pair of PVKs (FG) *	392
Generate a Watchword Key (FO)	395
Generate ZEK/ZAK (FI)	397
Generate a ZPK (IA)	399
Form a ZMK from Three ZMK Components (GG)	401
Form a ZMK from 2 to 9 ZMK Components (GY)	403
Generate and Print a ZMK Component (OC)	405
Translate a CVK Pair from Old LMK to New LMK Encryption (AY)	407
Translate a CVK Pair from LMK to ZMK Encryption (AU)	409
Translate a CVK Pair from ZMK to LMK Encryption (AW)	411
Translate a TMK, TPK or PVK (AA) *	413
Translate a TMK, TPK or PVK from LMK to ZMK Encryption (FE) *	415
Translate a TMK, TPK or PVK from ZMK to LMK Encryption (FC) *	417
Translate a TAK (AC)	419
Translate a TAK from LMK to ZMK Encryption (MG)	421
Translate a TAK from ZMK to LMK Encryption (MI)	423
Translate a Watchword Key from LMK to ZMK Encryption (FQ)	425
Translate a Watchword Key from ZMK to LMK Encryption (FS)	427

Command	Page
Translate a ZEK/ZAK from LMK to ZMK Encryption (FM)	429
Translate a ZEK/ZAK from ZMK to LMK Encryption (FK)	431
Translate a ZPK (KC)	433
Translate a ZPK from LMK to ZMK Encryption (GC)	435
Translate a ZPK from ZMK to LMK Encryption (FA)	437
Translate a ZMK (GE)	439
Generate a Key Check Value (Not Double-Length ZMK) (KA) *	441
Generate a CSCK (RY)	443
Export a CSCK (RY)	445
Import a CSCK (RY)	447
Generate a BDK (BI)	449
Translate a BDK from ZMK to LMK Encryption (DW)	450
Translate a BDK from LMK to ZMK Encryption (DY)	452
Generate and Export a KML (DI)	454
Import a KML (DK)	456
Generate a MAC (MA)	458
Verify a MAC (MC)	460
Verify and Translate a MAC (ME)	462
Generate MAC (MAB) for Large Message (MQ)	464
Generate MAC (MAB) using ANSI X9.19 Method for a Large Message (MS)	466
Generate a Binary MAC (MK)	468
Verify a Binary MAC (MM)	470
Verify and Translate a Binary MAC (MO)	472
Translate a PIN from BDK to ZPK Encryption (DUKPT) (CI)	474
Verify a PIN Using the IBM Method (DUKPT) (CK)	476

Command	Page
Verify a PIN Using the VISA PVV Method (DUKPT) (CM)	480
Verify a PIN Using the Diebold Method (DUKPT) (CO)	482
Verify a PIN Using the Encrypted PIN Method (DUKPT) (CQ)	484

* These commands are disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value of "Y". They should be replaced with newer Host commands as follows:

Host Command		Replaced by	
AA	Translate a TMK, TPK or PVK	BW	Translate Keys from Old LMK to New LMK
FC	Translate a TMK, TPK or PVK from ZMK to LMK Encryption	A6	Import a Key
FE	Translate a TMK, TPK or PVK from LMK to ZMK Encryption	A8	Export a Key
FG	Generate a pair of PVKs	A0	Generate a Key
KA	Generate a Key Check Value (Not Double-Length ZMK)	BU	Generate a Key Check Value
OE	Generate and Print a TMK, TPK or PVK	NE	Generate and Print a Key as Split Components

Generate a CVK Pair

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Generate a VISA CVK pair.
Output the key pair encrypted under a variant of LMK pair 14-15.

Note: This command is superseded by host command 'AO'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AS'.
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. If present must be 'O' or 'U'. For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible). Not available for keys generated using schemes. '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'AT'.
Error Code	2 A	'00' : No error '68' : Command disabled or a standard error code..
CVK Key scheme = 'O' or not specified		
CVK A	16 H	CVK A encrypted under variant 4 of LMK pair 14-15.
CVK B	16 H	CVK B encrypted under variant 4 of LMK pair 14-15.
CVK Key scheme not 'O'		
CVK A/B	1 A + 32 H	CVK A/B encrypted under variant 4 of LMK pair 14-15.
KCV Type = 'O' or not specified		
CVK A check value	16 H	The CVK A check value.
CVK B check value	16 H	The CVK B check value.
For KCV Type = '1'		
CVK A/B check value	6 H	The CVK A/B 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 and Print a TMK, TPK or PVK

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC027**	
Authorization: **Required** Activity: **genprint.{*keytype*}.host**	

Function: Generate a random key, return it encrypted under LMK pair 14-15 and print it at the payShield 9000 attached printer.

Notes:

- This command is superseded by host command 'NE'.
- A printer must be attached to one of the USB ports on the payShield 9000. Serial-to-USB and parallel-to-USB cables are available from Thales, on request.
- The HSM must have a print format already defined.
- The delimiter to separate optional fields is changed from ';' to '|'.
- This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value '0E'.
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	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 at Appendix C of the payShield 9000 General Information Manual.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 '0F'.
Error Code	2 A	'00' : No error '16' : Printer not ready/not connected '68' : Command disabled or a standard error code.
TMK, TPK or PVK	16 H or 1 A + 32/48 H	TMK, TPK or PVK encrypted under LMK pair 14-15.
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.
RESPONSE MESSAGE (after printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value '0Z'.
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 a Pair of PVKs

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Required** Activity: **generate.002.host**	

Function: Generate two random keys and return them each encrypted under LMK pair 14-15 and under a ZMK.

Notes:

- This command is superseded by host command 'AO'.
- The command is used to send the keys to another party.
- If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.
- This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FG'.
ZMK	16 / 32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
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 ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or 'O'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual. Default 'O'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or 'O'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual. Default 'O'.
KCV type	1 A	Optional. Key Check Value calculation method. Default 'O'. '0' : 16 digit KCV (backward compatible mode). Not available for keys generated using new schemes. '1' : 6 digit KCV. Only available for keys generated under new key schemes. '2' : 8 digit KCV. Only available for keys generated in backward compatibility mode.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be

Field	Length & Type	Details
COMMAND MESSAGE		
LMK Identifier	2 N	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
COMMAND MESSAGE		
Field	**Length & Type**	**Details**
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'FH'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '68' : Command disabled or a standard error code.
No LMK Scheme specified		
First TMK, TPK or PVK under LMK	16 H	First half of the new TMK, TPK or PVK, encrypted under LMK pair 14-15.
Second TMK, TPK or PVK under LMK	16 H	Second half of the new TMK, TPK or PVK, encrypted under LMK pair 14-15.
First TMK, TPK or PVK under ZMK	16 H	First half of the new TMK, TPK or PVK, encrypted under ZMK.
Second TMK, TPK or PVK under ZMK	16 H	Second half of the new TMK, TPK or PVK, encrypted under ZMK.
First KCV	16 / 8 / 6 H	Result of encrypting 64 binary zeros with the first half of the new TMK, TPK or PVK. The length is dependent upon the KCV Type. 16 H for KCV Type = '0'; 8 H for KCV Type = '1'; 6 H for KCV Type = '2'.
Second KCV	16 / 8 / 6 H	Result of encrypting 64 binary zeros with the second half of the new TMK, TPK or PVK. The length is dependent upon the KCV Type. 16 H for KCV Type = '0'; 8 H for KCV Type = '1'; 6 H for KCV Type = '2'.
LMK Scheme specified		
TMK, TPK or PVK under LMK	1 A + 32/48 H	New TMK, TPK or PVK; encrypted under LMK pair 14-15.
TMK, TPK or PVK under ZMK	1 A + 32/48 H	New TMK, TPK or PVK; encrypted under ZMK.
KCV	16 / 8 / 6 H	Result of encrypting 64 binary zeros with the new TMK, TPK or PVK. The length is dependent upon the KCV Type. 16 H for KCV Type = '0'; 8 H for KCV Type = '1'; 6 H for KCV Type = '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 a Watchword Key

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Generate a Watchword Key (WWK).

Notes: This command is superseded by host command 'AO'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FO'.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'. If an option is not required by the command fill with a valid value or '0'.
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'FP'.
Error Code	2 A	'00' : No error '68' : Command disabled or a standard error code.
WWK	16 H or 1 A + 32/48 H	Watchword Key encrypted under LMK pair 22-23.
Check value	16 / 6 H	Result of encrypting 64 binary zeroes with the WWK. 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.

Generate ZEK/ZAK

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Generate a ZEK or ZAK.

Notes: This command is superseded by host command 'AO'.

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 'FI'.
Flag	1 N	'0' : ZEK '1' : ZAK.
ZMK	16 / 32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
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 ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual. Default '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 at Appendix C of the payShield 9000 General Information Manual. Default '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'FJ'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '68' : Command disabled or a standard error code.
ZEK or ZAK for transmission	16 H or 1 A + 32/48 H	ZEK or ZAK encrypted under ZMK (ZEK when Flag is '0', ZAK when Flag is '1').
ZEK for storage	16 H or 1 A + 32/48 H	ZEK encrypted under LMK pair 30-31 (present only when Flag is '0').
ZAK for storage	16 H or 1 A + 32/48 H	ZAK encrypted under LMK pair 26-27 (present only when Flag is '1').
Check value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZEK/ZAK. 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.

Generate a ZPK

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Generate a random PIN key and return it to the Host encrypted under a ZMK for transmission to another party and under the LMK for storage on the Host database.

Notes: This command is superseded by host command 'AO'.

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 'IA'.
ZMK	16 / 32 H or 1 A + 32/48 H	The ZMK encrypted under LMK pair 04-05.
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 ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual. Default '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 at Appendix C of the payShield 9000 General Information Manual. Default '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'IB'.
Error Code	2 A	'00' : No error '10' : ZMK does not have odd parity '68' : Command disabled or a standard error code.
ZPK under ZMK	16 H or 1 A + 32/48 H	The ZPK encrypted under the ZMK.
ZPK under LMK	16 H or 1 A + 32/48 H	The ZPK encrypted under LMK pair 06-07.
Check value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZPK. 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.

Form a ZMK from Three ZMK Components

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Required** Activity: **component.000.host**	

Function: Form a ZMK from three encrypted components and return the ZMK encrypted under LMK pair 04-05, and the check value.

Notes: This command is superseded by host command 'A4'.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command. The encrypted components must be generated using the F or Z console commands.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'GG'.
First ZMK component	16 / 32 H	The first ZMK component encrypted under a variant of LMK 04-05.
Second ZMK component	16 / 32 H	The second ZMK component encrypted under a variant of LMK 04-05.
Third ZMK component	16 / 32 H	The third ZMK component encrypted under a variant of LMK 04-05.
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'GH'.
Error Code	2 A	'00' : No error '10' : Parity error in first component '11' : Parity error in second / third component '68' : Command disabled or a standard error code.
ZMK	16 / 32 H or 1 A + 32/48 H	The ZMK encrypted under LMK pair 04-05.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZMK. 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.

Form a ZMK from 2 to 9 ZMK Components

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Required** Activity: **component.000.host**	

Function: Form a ZMK from 2 to 9 encrypted components and return the ZMK encrypted under a variant of LMK pair 04-05, and the check value.

Notes: This command is superseded by host command 'A4'.
Use this command to provide inter-operation with non-Thales security equipment.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command. The encrypted components must be generated using the F or Z console commands.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'GY'.
Number of components	1 N	'2' – '9' : Number of components.
First ZMK component	16 / 32 H	The first ZMK component encrypted under a variant of LMK 04-05.
Second ZMK component	16 / 32 H	The second ZMK component encrypted under a variant of LMK 04-05.
…	…	…
Last ZMK component	16 / 32 H	The last ZMK component encrypted under a variant of LMK 04-05.
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'GZ'.
Error Code	2 A	'00' : No error '10' : Parity error in first component '11' : Parity error second to ninth components '68' : Command disabled or a standard error code.
ZMK	16 / 32 H or 1 A + 32/48 H	The ZMK encrypted under LMK pair 04-05.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZMK. 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.

Generate and Print a ZMK Component

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC027**	
Authorization: **Required** Activity: **genprint.000.host**	

Function: Generate a random ZMK component, print it at the payShield 9000 attached printer and return the encrypted value to the host.

Notes: This command is superseded by host command 'A2'.
A printer must be attached to one of the USB ports on the payShield 9000. Serial-to-USB and parallel-to-USB cables are available from Thales, on request.
The HSM must have a print format already defined.
If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.
The delimiter to separate optional fields is changed from ';' to '|'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value '0C'.
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	Optional. If present the following three fields must be present. Value '|'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual. Default '0'.
Reserved	1 A	Optional. If present, should be '0'.
Reserved	1 A	Optional. If present, should be '0'.
Delimiter	1 A	Value '~'. Optional; must be present if the '%' delimiter is present.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 '0D'.
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.
ZMK component	16 / 32 H or 1 A + 32/48 H	ZMK component encrypted under a variant of LMK pair 04-05.
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.
RESPONSE MESSAGE (after printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value '0Z'.
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.

Translate a CVK Pair from Old LMK to New LMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a CVK pair from encryption under a variant 4 of an old LMK pair 14-15 to encryption under a variant 4 of a new LMK pair 14-15.

Note: This command is superseded by host command 'BW'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AY'.
CVK A / B	32 H or 1 A + 32 H	CVK A / B pair encrypted under a variant 4 of the old LMK pair 14-15.
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'AZ'.
Error Code	2 A	'00' : No error '10' : CVK A or B parity error '11' : ZPK parity error '68' : Command disabled or a standard error code.
CVK A / B	32 H or 1 A + 32 H	CVK A / B encrypted under a variant of LMK pair 14-15.
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 CVK Pair from LMK to ZMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a CVK pair from encryption under a variant of LMK pair 14-15 to encryption under a ZMK.

Notes: This command is superseded by host command 'A8'.
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 'AU'.
ZMK	16 / 32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
CVK A / B	32 H or 1 A + 32 H	CVK A / B encrypted under a variant 4 of LMK pair 14-15.
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 ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual. Default '0'.
Reserved	1 A	Optional. If present must be '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0' : 16 digit KCV (backward compatible mode). Not available for keys generated using schemes. '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'AV'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '11' : CVK A or B parity error '68' : Command disabled or a standard error code.
CVK A / B	32 H or 1 A + 32 H	CVK A / B encrypted under ZMK.
KCV Type = 0 or not specified		
CVK A check value	6 H	The CVK A check value.
CVK B check value	6 H	The CVK B check value.
KCV Type = 1		
Key Check Value	6 H	Result of encrypting 64 binary zeros with the 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.

Translate a CVK Pair from ZMK to LMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a CVK pair from encryption under a ZMK to encryption under a variant of LMK pair 14-15.

Notes: This command is superseded by host command 'A6'.
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 'AW'.
ZMK	16 / 32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
CVK A / B	32 H or 1 A + 32 H	CVK A / B encrypted under the ZMK.
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode – not available for keys generated using schemes) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'AX'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '11' : CVK A or B parity error '68' : Command disabled or a standard error code.
CVK A / B	32 H or 1 A + 32 H	CVK A / B encrypted under a variant 4 of LMK pair 14-15.
KCV Type = '0' or not specified		
CVK A check value	6 H	The CVK A check value.
CVK B check value	6 H	The CVK B check value.
KCV Type = '1'		
Key Check Value	6 H	Result of encrypting 64 binary zeros with the 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.

Translate a TMK, TPK or PVK

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a TMK, TPK or PVK encrypted under the LMK pair held in "key change storage" to encryption under LMK pair 14-15.

Notes:

- This command is superseded by host command 'BW'.
- This command is disabled if the security setting “Enforce key type 002 separation for PCI HSM compliance” has the compliant value “Y”.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AA'.
TMK, TPK or PVK	16 H or 1 A + 32/48 H	The TMK, TPK or PVK encrypted under the LMK pair held in "key change storage".
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 at Appendix C of the payShield 9000 General Information Manual.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'AB'.
Error Code	2 A	'00' : No error '10' : TMK, TPK or PVK parity error '68' : Command disabled or a standard error code.
TMK, TPK or PVK	16 H or 1 A + 32/48 H	The TMK, TPK or PVK translated to encryption under LMK pair 14-15.
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 TMK, TPK or PVK from LMK to ZMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Required** Activity: **export.{*keytype*}.host**	

Function: Translate a TMK, TPK or PVK from encryption under the LMK to encryption under a ZMK.

Notes:

- This command is superseded by host command 'A8'.
- The command is used to send a key to another party.
- If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.
- This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FE'.
ZMK	16 / 32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
TMK, TPK or PVK	16 H or 1 A + 32/48 H	TMK, TPK or PVK encrypted under LMK pair 14-15.
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 ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual. Default '0'.
Reserved	1 A	Optional. If present must be '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'FF'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '11' : TMK, TPK or PVK parity error '68' : Command disabled or a standard error code.
TMK, TPK or PVK	16 H or 1 A + 32/48 H	Translated TMK, TPK or PVK encrypted under the ZMK.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the 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.

Translate a TMK, TPK or PVK from ZMK to LMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Required** Activity: **import.{*keytype*}.host**	

Function: Translate a TMK, TPK or PVK from encryption under a ZMK to encryption under the LMK.

Notes:

- This command is superseded by host command 'A6'.
- The command is used to receive a key from another party.
- If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.
- This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'FC'.
ZMK	16 / 32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
TMK, TPK or PVK	16 H or 1 A + 32/48 H	TMK, TPK or PVK encrypted under the ZMK.
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'FD'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '11' : TMK, TPK or PVK parity error '68' : Command disabled or a standard error code.
TMK, TPK or PVK	16 H or 1 A + 32/48 H	Translated TMK, TPK or PVK; encrypted under LMK pair 14-15.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the 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.

Translate a TAK

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a TAK encrypted under the LMK pair held in "key change storage" to encryption under LMK pair 16-17.

Note: This command is superseded by host command 'BW'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AC'.
TAK	16 H or 1 A + 32/48 H	The TAK encrypted under the LMK pair held in "key change storage".
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'AD'.
Error Code	2 A	'00' : No error '10' : TAK parity error '68' : Command disabled or a standard error code.
TAK	16 H or 1 A + 32/48 H	The TAK translated to encryption 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.

Translate a TAK from LMK to ZMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a TAK from encryption under the LMK to encryption under a ZMK.

Used to send a key to another party.

Notes: This command is superseded by host command 'A8'.

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 'MG'.
ZMK	16 / 32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
TAK	16 H or 1 A + 32/48 H	TAK encrypted under LMK pair 16-17.
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 ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual. Default '0'.
Reserved	1 A	Optional. If present must be '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'MH'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '11' : TAK parity error '68' : Command disabled or a standard error code.
TAK	16 H or 1 A + 32/48 H	TAK encrypted under the ZMK.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the TAK. 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.

Translate a TAK from ZMK to LMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a TAK from encryption under a ZMK to encryption under the LMK.

Used to receive a key from another party.

Notes: This command is superseded by host command 'A6'.

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 'MI'.
ZMK	16 / 32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
TAK	16 H or 1 A + 32/48 H	TAK encrypted under ZMK.
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'MJ'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '11' : TAK parity error '68' : Command disabled or a standard error code.
TAK	16 H or 1 A + 32/48 H	TAK encrypted under LMK pair 16-17.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the TAK. 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.

Translate a Watchword Key from LMK to ZMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a Watchword Key from encryption under the LMK to encryption under a ZMK.

Notes: This command is superseded by host command 'A8'.

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 'FQ'.
ZMK	16 / 32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
WWK	16 H or 1 A + 32/48 H	Watchword encrypted under LMK pair 22-23.
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 ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual. Default '0'.
Reserved	1 A	Optional. If present must be '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'FR'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '11' : ZPK parity error '68' : Command disabled or a standard error code.
WWK	16 H or 1 A + 32/48 H	WWK encrypted under ZMK.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the WWK. 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.

Translate a Watchword Key from ZMK to LMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a Watchword Key from encryption under a ZMK to encryption under the LMK.

Notes: This command is superseded by host command 'A6'.

If using a 32-character ZMK, 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 'FS'.
ZMK	16 / 32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
WWK	16 H or 1 A + 32/48 H	Watchword encrypted under ZMK.
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'FT'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '11' : Imported key all zero '68' : Command disabled or a standard error code.
WWK	16 H or 1 A + 32/48 H	WWK encrypted under LMK pair 22-23.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the WWK. 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.

Translate a ZEK/ZAK from LMK to ZMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a ZEK or ZAK.

Notes: This command is superseded by host command 'A8'.

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 'FM'.
Flag	1 N	'0' : ZEK '1' : ZAK.
ZMK	16 / 32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
ZEK	16 H or 1 A + 32/48 H	ZEK encrypted under LMK pair 30-31 (present only when Flag is '0').
ZAK	16 H or 1 A + 32/48 H	ZAK encrypted under LMK pair 26-27 (present only when Flag is '1').
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 ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual. Default '0'.
Reserved	1 A	Optional. If present must be '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'FN'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '11' : ZEK/ZAK parity error '68' : Command disabled or a standard error code.
ZEK/ZAK	16 H or 1 A + 32/48 H	ZEK or ZAK encrypted under ZMK (ZEK when Flag is '0', ZAK when Flag is '1').
Check value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZEK/ZAK. 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.

Translate a ZEK/ZAK from ZMK to LMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a ZEK or ZAK from ZMK to LMK.

Notes: This command is superseded by host command 'A6'.

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 'FK'.
Flag	1 N	'0' : ZEK '1' : ZAK.
ZMK	16 / 32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
ZEK/ZAK	16 H or 1 A + 32/48 H	ZEK or ZAK encrypted under ZMK (ZEK when Flag is '0', ZAK when Flag is '1').
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'FL'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '68' : Command disabled or a standard error code.
ZEK	16 H or 1 A + 32/48 H	ZEK encrypted under LMK pair 30-31 (present only when Flag is '0').
ZAK	16 H or 1 A + 32/48 H	ZAK encrypted under LMK pair 26-27 (present only when Flag is '1').
Check value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZEK/ZAK. 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.

Translate a ZPK

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a ZPK encrypted under the LMK pair held in "key change storage" to encryption under LMK pair 06-07.

Note: This command is superseded by host command 'BW'.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'KC'.
ZPK	16 H or 1 A + 32/48 H	The ZPK encrypted under the LMK pair held in "key change storage".
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 at Appendix C of the payShield 9000 General Information Manual.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'KD'.
Error Code	2 A	'00' : No error '10' : ZPK parity error '68' : Command disabled or a standard error code.
ZPK	16 H or 1 A + 32/48 H	The ZPK translated to encryption under LMK pair 06-07.
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 ZPK from LMK to ZMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a ZPK from encryption under the LMK to encryption under a ZMK.

Used to transmit a ZPK to another party.

Notes: This command is superseded by host command 'A8'.

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 'GC'.
ZMK	16 / 32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
ZPK	16 H or 1 A + 32/48 H	ZPK encrypted under LMK pair 06-07.
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 ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual. Default '0'.
Reserved	1 A	Optional. If present must be '0'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'GD'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '11' : ZPK parity error '68' : Command disabled or a standard error code.
ZPK	16 H or 1 A + 32/48 H	Translated ZPK; encrypted under the ZMK.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZPK. 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.

Translate a ZPK from ZMK to LMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a ZPK from encryption under a ZMK to encryption under the LMK.

Used to receive a ZPK from another party.

Notes: This command is superseded by host command 'A6'.
The command does not require the ZPK to have odd parity, but odd parity is forced on the encrypted output. Unlike other commands, if error 01 is returned, it does not inhibit the return of subsequent fields.
The command tests the ZPK, after decrypting it from under the ZMK, to ensure the key (including the parity bits) is not zero (i.e., X'0000 0000 0000 0000). If the key is zero, the HSM returns error code 11 (all zero ZPK with even parity) and terminates processing.

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 'FA'.
ZMK	16 / 32 H or 1 A + 32/48 H	The ZMK encrypted under LMK pair 04-05.
ZPK	16 H or 1 A + 32/48 H	ZPK encrypted under the ZMK.
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.

Field	Length & Type	Details
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 'FB'.
Error Code	2 A	'00' : No error '01' : ZPK parity error; advice only '10' : ZMK parity error '11' : All zero ZPK with even parity '68' : Command disabled or a standard error code.
ZPK	16 H or 1 A + 32/48 H	Translated ZPK; encrypted under LMK pair 06-07.
Check value	16 / 6 H	Result of encrypting 64 binary zeroes with the ZPK. 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.

Translate a ZMK

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a ZMK encrypted under the LMK pair held in "key change storage" to encryption under LMK pair 04-05.

Notes: This command is superseded by host command 'BW'.

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 'GE'.
ZMK	16 / 32 H or 1 A + 32/48 H	The ZMK encrypted under the LMK pair held in "key change storage".
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 at Appendix C of the payShield 9000 General Information Manual.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'GF'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '68' : Command disabled or a standard error code.
ZMK	16 / 32 H or 1 A + 32/48 H	The ZMK translated to encryption under LMK pair 04-05.
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 (Not Double-Length ZMK)

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Generate a key check value for one of the following:
ZMK (single-length), ZPK, TMK, TPK, PVK, TAK

Notes:
- This command is superseded by host command 'BU'.
- The command can be used to verify a key received from another party. The HSM generates the value by encrypting 64 binary zeroes under the key.
- This command does not support the use of double-length ZMKs.
- This command is disabled if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the compliant value "Y".

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'KA'.
Key	16 H or 1 A + 32/48 H	One of the following: ZMK, ZPK, TMK, TPK, PVK or TAK encrypted under the relevant LMK pair.
Key Type code	2 N	The key type identifier: '00' : ZMK '01' : ZPK '02' : TMK, TPK or PVK '03' : TAK.
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.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'KB'.
Error Code	2 A	'00' : No error '10' : Encrypted key parity error '68' : Command disabled or a standard error code.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeroes with the 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.

Generate a CSCK

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Generate a random dual-length CSCK and encrypt it under LMK 14-15 variant 4.

Note: This command is superseded by host command 'AO'.

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 '0'.
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 '68' : Command disabled or a standard error code.
Mode	1 N	Value '0'.
CSCK	32 H or 1 A + 32 H	The CSCK encrypted under LMK 14-15 variant 4.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeros with the CSCK. 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.

Export a CSCK

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Decrypt a CSCK from under LMK 14-15 variant 4 and re-encrypt it under a supplied ZMK.

Note: This command is superseded by host command 'A8'.

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 '1'.
ZMK	32 H or 1 A + 32/48 H	The Zone Master Key, encrypted under LMK 04-05.
CSCK	32 H or 1 A + 32 H	The CSCK encrypted under LMK 14-15 variant 4.
Atalla variant	1 / 2 N	Optional.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'. If an option is not required by the command fill with a valid value or 0.
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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' : ZMK parity error '11' : CSCK parity error '27' : CSCK not double length '68' : Command disabled or a standard error code.
Mode	1 N	Value '1'.
CSCK encrypted for export	32 H or 1 A + 32 H	The CSCK encrypted under the supplied ZMK.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeros with the CSCK. 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.

Import a CSCK

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Decrypt a CSCK from under a supplied ZMK and re-encrypt it under LMK 14-15 variant 4.

Notes: This command is superseded by host command 'A6'.
Parity on the incoming CSCK is ignored, but odd parity will be forced before re-encryption. Error Code '01' will be returned if the incoming key did not have odd parity.
If the incoming key is found to be all zeros, Error Code 02 is returned and the key is not translated.

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 '2'.
ZMK	32 H or 1 A + 32/48 H	The Zone Master Key, encrypted under LMK 04-05.
CSCK	32 H or 1 A + 32 H	The CSCK, encrypted under the ZMK.
Atalla variant	1 / 2 N	Optional.
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 16 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 '01' : Incoming key did not have odd parity '02' : Incoming key was all zero '10' : ZMK parity error '27' : CSCK not double length '68' : Command disabled or a standard error code.
Mode	1 N	Value '2'.
CSCK	32 H or 1 A + 32 H	The CSCK encrypted under LMK 14-15 variant 4.
Key Check Value	16 / 6 H	Result of encrypting 64 binary zeros with the CSCK. 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.

Generate a BDK

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Determined by KTT(G)** Activity: **generate.bdk.host**	

Function: Generate a BDK and encrypt it under LMK pair 28-29 for Host storage.

Notes: This command is superseded by host command 'AO'.
This command is fully backward compatible with the BI command in payShield 9000 base software version 1.0.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'BI'.
Delimiter	1 A	Value ';'. Optional. If present the following three fields must be present.
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 at Appendix C of the payShield 9000 General Information Manual.
Reserved	1 A	Optional. If present must be '0'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'BJ'.
Error Code	2 A	'00' : No error '68' : Command disabled or a standard error code.
BDK	32 H or 1 A + 32 H	The BDK encrypted under LMK pair 28-29.
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 BDK from ZMK to LMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a BDK from encryption under a ZMK to encryption under LMK pair 28-29.

Notes: This command is superseded by host command 'A6'.
The command ignores the S/D (single/double length) parameter set by the CS (Configure Security) console command – the ZMK cannot be single length.
A key check value (KCV) is produced for the BDK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DW'.
ZMK	32 H or 1 A + 32/48 H	The ZMK encrypted under LMK pair 04-05.
BDK	32 H or 1 A + 32 H	The BDK encrypted under the ZMK.
Atalla variant	1 / 2 N	Optional. For use in networks that use a ZMK variant.
Delimiter	1 A	Value ';'. Optional. If present the following three fields must be present.
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 8 digit KCV (backward compatible mode) '1' : 6 digit KCV '2' : 8 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'DX'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '11' : BDK parity error '27' : BDK not double length '68' : Command disabled or a standard error code.
BDK	32 H or 1 A + 32 H	The BDK encrypted under LMK pair 28-29.
Key Check Value	6 / 8 H	Result of encrypting 64 binary zeros with the BDK.
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 BDK from LMK to ZMK Encryption

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a BDK from encryption under LMK pair 28-29 to encryption under ZMK.

Notes: This command is superseded by host command 'A8'.
The command ignores the S/D (single/double length) parameter set by the CS (Configure Security) console command – the ZMK cannot be single length.
A key check value (KCV) is produced for the BDK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DY'.
ZMK	32 H or 1 A + 32/48 H	The ZMK encrypted under LMK pair 04-05.
BDK	32 H or 1 A + 32 H	The BDK encrypted under LMK pair 28-29.
Atalla variant	1 / 2 N	Optional. For use in networks that use a ZMK variant.
Delimiter	1 A	Value ';'. Optional. If present the following three fields must be present.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or '0'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual.Default '0'.
Reserved	1 A	Optional. If present must be 0.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default '0'. '0' : 8 digit KCV (backward compatible mode) '1' : 6 digit KCV '2' : 8 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'DZ'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '11' : BDK parity error '27' : BDK not double length or triple length '68' : Command disabled or a standard error code.
BDK	32 H or 1 A + 32 H	The BDK encrypted under the ZMK.
Key Check Value	6 / 8 H	Result of encrypting 64 binary zeros with the 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 Export a KML

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Generate a double-length Master Load Key (KML) and return it encrypted under Variant 2 of LMK pair 04-05, and also under a double length Zone Master Key (ZMK).

Notes: This command is superseded by host command 'AO'.
A check value for the KML is also returned.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DI'.
ZMK	32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
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 ';'.
Key Scheme (ZMK)	1 A	Optional. Key scheme for encrypting key under ZMK (or 'O'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual. Default 'O'.
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or 'O'). For a list of key schemes, see the Key Scheme Table at Appendix C of the payShield 9000 General Information Manual. Default 'O'.
Key Check Value Type	1 A	Optional. Key Check Value calculation method. Default 'O'. 'O' : 6 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'DJ'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '68' : Command disabled or a standard error code.
KML (ZMK)	32 H or 1 A + 32/48 H	KML, encrypted under ZMK.
KML (under LMK)	32 H or 1 A + 32/48 H	KML, encrypted under Variant 2 of LMK pair 04-05.
KML check value	6 H	Check value formed by encrypting a block of 64 binary zeros with the KML and returning the 24 left-most bits of the result.
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 KML

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Translate a double-length Master Load Key (KML) from encryption under a ZMK to encryption under Variant 2 of LMK pair 04-05.

Notes: This command is superseded by host command 'A6'.
A check value for the KML is also returned.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'DK'.
ZMK	32 H or 1 A + 32/48 H	ZMK encrypted under LMK pair 04-05.
KML	32 H or 1 A + 32/48 H	KML, encrypted under ZMK.
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 at Appendix C of the payShield 9000 General Information Manual.
Key Check Value Type	1 A	Optional. Key Check Value calculation method: '0' : 6 digit KCV (backward compatible mode) '1' : 6 digit KCV.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'DL'.
Error Code	2 A	'00' : No error '10' : ZMK parity error '11' : KML parity error '68' : Command disabled or a standard error code.
KML	32 H or 1 A + 32/48 H	KML, encrypted under Variant 2 of LMK pair 04-05.
KML check value	6 H	Check value formed by encrypting a block of 64 binary zeros with the KML and returning the left-most 24 bits of the result.
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 MAC

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Generate a MAC on a given block of data using a TAK.

Notes: This command is superseded by host command 'M6'.

The MAC algorithm used is ANSI X9.9 using zero padding.

The value n given for Data is the recommended maximum value; it can be increased up to 32Kbytes with consideration for the overall buffer size compared to the size of the complete HSM command message.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MA'.
TAK	16 H or 1 A + 32/48 H	TAK encrypted under LMK pair 16-17.
Data	0 - n	The data on which a MAC is to be generated, n = 16K. Must not contain a '~' 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 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 'MB'.
Error Code	2 A	'00' : No error '10' : TAK parity error '68' : Command disabled or a standard error code.
MAC	8 H	The calculated 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.

Verify a MAC

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Verify a MAC on given block of data using a TAK.

Notes: This command is superseded by host command 'M8'.

The MAC algorithm used is ANSI X9.9 using zero padding.

The value n given for Data is the recommended maximum value; it can be increased toward 32Kbytes with consideration for the overall buffer size compared to the size of the complete HSM command message.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MC'.
TAK	16 H or 1 A + 32/48 H	TAK encrypted under LMK pair 16-17.
MAC	8 H	The MAC to be verified.
Data	0 - n	The data on which the MAC to be verified was calculated, n = 16K. Must not contain a '~' 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 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 'MD'.
Error Code	2 A	'00' : No error '01' : MAC verification failure '10' : TAK 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.

Verify and Translate a MAC

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Verify a MAC on a block of data using a TAK and, if successful, generate a MAC on the same block of data with a different TAK.

Notes: This command is superseded by host command 'MY'.

The MAC algorithm used is ANSI X9.9 using zero padding.

The value n given for Data is the recommended maximum value; it can be increased toward 32Kbytes with consideration for the overall buffer size compared to the size of the complete HSM command message.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'ME'.
Source TAK	16 H or 1 A + 32/48 H	The source TAK encrypted under LMK pair 16-17.
Destination TAK	16 H or 1 A + 32/48 H	The destination key encrypted under LMK pair 16-17.
MAC	8 H	The MAC generated with the source key.
Data	0 - n	The data on which to verify and generate a MAC, n = 16K. Must not contain a '~' 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 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 'MF'.
Error Code	2 A	'00' : No error '01' : MAC verification failure '10' : Source TAK parity error '11' : Destination TAK parity error '68' : Command disabled or a standard error code.
MAC	8 H	The MAC generated using the destination TAK.
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 MAC (MAB) for Large Message

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Generate a MAC (MAB) for a large message using a ZAK.

Notes: When using 8 hex-digit MACs, this command is superseded by host command 'M6'.

The MAC algorithm used is ANSI X9.9 using zero padding.

The command operates on binary data. If the HSM is set for Async/ASCII operation, ensure that:

The Host port has been set for 8 data bit operation by the CH (Configure Host) command.

The data for which the MAC is to be generated does not contain either EM (X'19) or ETX (X'03).

The value n given for Data is the recommended maximum value; it can be increased toward 32Kbytes with consideration for the overall buffer size compared to the size of the complete HSM command message.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MQ'.
Message block number	1 N	'0' : The only block. '1' : The first block. '2' : A middle block. '3' : The last block.
ZAK	16 H or 1 A + 32/48 H	ZAK encrypted under LMK pair 26-27
IV	16 H	Initialization value, present only when Message block number is '2' or '3'.
Message length	3 H	Message length in bytes.
Message block	n B	The clear text message block.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'MR'.
Error Code	2 A	'00' : No error '02' : ZAK not single length '05' : Invalid message block number '10' : ZAK parity error '68' : Command disabled or a standard error code.
MAB	16 H	Used as IV for next block when Message block number is '1' or '2'. Used as message authenticator when Message block number is '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 MAC (MAB) using ANSI X9.19 Method for a Large Message

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: To generate a MAB for a large message using a TAK or ZAK.

Notes:
When using 8 hex-digit MACs, this command is superseded by host command 'M6'.
The MAC algorithm used is ANSI X9.19 using zero padding.
The command can operate on binary data or expanded Hex. If the HSM is set for Async/ASCII operation and binary data used ensure that:
The host port has been set for 8 data bit operation by the CH (Configure Host) console command.
The data for which the MAC is to be generated does not contain either EM (X'19) or ETX(X'03).
Expanded Hex mode uses 2 hexadecimal characters for each binary byte.
If the message block is the first or a middle block it must be a multiple of 8 bytes.

Consideration to the buffer size of the HSM must be made before the value n message length is selected.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MS'.
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).
Key Length	1 N	Key length: 0 : Single Length DES Key 1 : Double Length DES Key.
Message Type	1 N	Message Type: '0' : Message data is binary '1' : Message data is expanded Hex.

Field	Length & Type	Details
Key	16 H or 1 A + 32/48 H	Key, encrypted under appropriate LMK pair. TAK under LMK pair 16 – 17 ZAK under LMK pair 26 – 27.
IV	16 H	Initialization value, present only when Message block number is '2' or '3'.
Message Length	4 H	Length of message to be MAC'd (length of following field if message type binary; half the length of the following field if expanded hex).
Message Block	n B or H	The message block either in binary or as expanded Hex.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'MT'.
Error Code	2 A	'00' : No error '03' : Invalid Message Type Code '04' : Invalid Key Type Code '05' : Invalid Message Block Number '06' : Invalid Key Length Code '68' : Command disabled or a standard error code.
MAB	16 H	Used as IV for next block when message block number is 1 or 2. Used as message authenticator when message block is 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 a Binary MAC

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Generate a MAC on a binary message using a TAK.

Note: This command is superseded by host command 'M6'.
The MAC algorithm used is ANSI X9.9 using zero padding.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MK'.
TAK	16 H or 1 A + 32/48 H	The TAK used to generate the MAC, encrypted under LMK 16-17.
EITHER		
For Binary Communications Modes:		
Data length	3 H	'001' … '320' indicating the length of the data field (in hex).
Data	n B	Data to be MACed. 1 to 800 bytes.
OR		
For Normal Async Modes:		
Data length	3 H	'002' … '320' indicating the length of the data field (in hex).
Data	n H	Data to be MACed. 2 to 800 hexadecimal characters representing 1 to 400 bytes.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'ML'.
Error Code	2 A	'00' : No error '10' : TAK parity error '68' : Command disabled or a standard error code.
MAC	8 H	The computed 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.

Verify a Binary MAC

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Verify a MAC on a binary message using a TAK.

Note: This command is superseded by host command 'M8'.
The MAC algorithm used is ANSI X9.9 using zero padding.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MM'.
TAK	16 H or 1 A + 32/48 H	The TAK used to generate the MAC, encrypted under LMK 16-17.
MAC	8 H	The MAC to be verified.
EITHER		
For Binary Communications Modes:		
Data length	3 H	'001' … '320' indicating the length of the data field (in hex).
Data	n B	Data to be MACed. 1 to 800 bytes.
OR		
For Normal Async Modes:		
Data length	3 H	'002' … '320' indicating the length of the data field (in hex).
Data	n H	Data to be MACed. 2 to 800 hexadecimal characters representing 1 to 400 bytes.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'MN'.
Error Code	2 A	'00' : No error '01' : MAC did not verify '10' : TAK 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.

Verify and Translate a Binary MAC

Variant LMK ☑	Keyblock LMK ☒
License: **HSM9-LIC029**	
Authorization: **Not required**	

Function: Verify a MAC on a binary message using a TAK, and if successful, generate a MAC on the same message with a different TAK.

Notes: This command is superseded by host command 'MY'.

The MAC algorithm used is ANSI X9.9 using zero padding.

If the verify fails no destination MAC is computed.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MO'.
Source TAK	16 H or 1 A + 32/48 H	The source TAK used to verify the MAC, encrypted under LMK 16-17.
Destination TAK	16 H or 1 A + 32/48 H	The destination TAK used to verify the MAC, encrypted under LMK 16-17.
MAC	8 H	The MAC to be verified.
EITHER		
For Binary Communications Modes:		
Data length	3 H	'001' … '320' indicating the length of the data field (in hex).
Data	n B	Data to be MAC'd. 1 to 800 bytes.
OR		
For Normal Async Modes:		
Data length	3 H	'002' … '320' indicating the length of the data field (in hex).
Data	n H	Data to be MAC'd. 2 to 800 hexadecimal characters representing 1 to 400 bytes.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'MP'.
Error Code	2 A	'00' : No error '01' : MAC verification failure '10' : Source TAK parity error '11' : Destination TAK parity error '68' : Command disabled or a standard error code.
MAC	8 H	The computed 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 PIN from BDK to ZPK Encryption (DUKPT)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: Translate a PIN from encryption under the unique DUKPT key to encryption under an interchange key (ZPK) for transmission to another node.

Notes: This command implements the original DUKPT method of deriving a single-length PIN encryption key from the (double length) BDK. This command is provided for legacy applications: new applications should use the equivalent 3DES DUKPT command (G0).

The command performs the same function as CA and CC, except the Host supplies the HSM with the information necessary to compute the current key.

The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'CI'.
BDK		The Base Derivation Key, used to decrypt the PIN block.
	32 H or 1 A + 32 H	For a Variant LMK, the 'BDK' must be encrypted under LMK pair 28-29.
	or 1 A + n A	For a Keyblock LMK, the 'BDK' must comply with the following: Key Usage: 'B0'; Algorithm: 'T'; Mode of Use: 'N'
ZPK		The Zone PIN Key, used to re-encrypt the PIN block.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'ZPK' must be encrypted under LMK pair 06-07.
	or 1 A + n A	For a Keyblock LMK, the 'ZPK' must comply with the following: Key Usage: 'P0', '72'; Algorithm: 'D', 'T'; Mode of Use: 'B', 'E', 'N'
KSN Descriptor	3 H	The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information.
Key Serial Number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information.
Source Encrypted Block	16 H	The encrypted PIN block received from the POS PIN terminal.
Destination PIN Block Format Code	2 N	One of the following codes: '01' : ANSI format '04' : Plus format.
Account Number	12 N or 18 H	For a Destination PIN Block Format Code ≠ '04', this field has

Field	Length & Type	Details
		length 12 N, and specifies the 12 right most digits of the account number, excluding the check digit. For a Destination PIN Block Format Code = '04', this field has length 18 H, and specifies the entire 18 digit account number, excluding the check digit, padded with 'F' on the left.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'CJ'.
Error Code	2 A	'00' : No error '10' : BDK parity error '11' : Interchange key parity error '27' : BDK not double length '68' : Command disabled '69' : PIN Block format has been disabled or a standard error code.
PIN Length	2 N	Length of the translated PIN.
Encrypted PIN	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.

Verify a PIN Using the IBM Method (DUKPT)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: Verify a PIN using the IBM method.

Notes: This command implements the original DUKPT method of deriving a single-length PIN encryption key from the (double length) BDK. This command is provided for legacy applications: new applications should use the equivalent 3DES DUKPT command (G0).

The command performs the same function as DA and EA, plus it computes the PIN pad key. The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

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 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 TDES 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.)

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'CK'.
BDK		The Base Derivation Key, used to decrypt the PIN block.
	32 H or 1 A + 32 H	For a Variant LMK, the 'BDK' must be encrypted under LMK pair 28-29.
	or 1 A + n A	For a Keyblock LMK, the 'BDK' must comply with the following: **Key Usage**: 'B0'; **Algorithm**: 'T'; **Mode of Use**: 'N'
PVK		The PIN Verification Key, used to verify the customer PIN.
	16 H or 1 A + 32/48 H	For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.
	or 1 A + n A	For a Keyblock LMK, the 'PVK' must comply with the following: **Key Usage**: 'V1'; **Algorithm**: 'D', 'T'; **Mode of Use**: 'C', 'V', 'N'
KSN descriptor	3 H	The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information.
Key serial number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information.
Source encrypted block	16 H	Encrypted PIN block received from the POS PIN terminal.
Check Length	2 N	The minimum PIN length.
Account Number	12 N	The 12 right-most digits of the primary account number (PAN), excluding the check digit.
Decimalization Table	16 N or 16 H or 1 A + 3 H or 1 A + 32 H	16 N when using Plaintext decimalization tables. 16 H when using Encrypted decimalization tables and a Variant LMK or 3-DES Keyblock 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 Keyblock LMK.
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 account number; 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'.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'CL'.
Error Code	2 A	'00' : No error '01' : Verification failure '02' : Warning PVK not single length (See the notes at the start of this section.0 '10' : BDK parity error '11' : PVK parity error '27' : BDK not double length '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 PIN Using the VISA PVV Method (DUKPT)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: Verify a PIN using the VISA PVV method.

Notes: This command implements the original DUKPT method of deriving a single-length PIN encryption key from the (double length) BDK. This command is provided for legacy applications: new applications should use the equivalent 3-DES DUKPT command (GQ).

The command performs the same function as DC and EC.

The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'CM'.
BDK		The Base Derivation Key, used to decrypt the PIN block.
	32 H or 1 A + 32 H	For a Variant LMK, the 'BDK' must be encrypted under LMK pair 28-29.
	or 1 A + n A	For a Keyblock LMK, the 'BDK' must comply with the following: **Key Usage**: 'B0'; **Algorithm**: 'T'; **Mode of Use**: 'N'
PVK		The PIN Verification Key, used to verify the customer PIN.
	32 H or 1 A + 32/48 H	For a Variant LMK, the 'PVK' must be encrypted under LMK pair 14-15 variant 0.
	or 1 A + n A	For a Keyblock LMK, the 'PVK' must comply with the following: **Key Usage**: 'V2'; **Algorithm**: 'T'; **Mode of Use**: 'C', 'V', 'N'
KSN descriptor	3 H	The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information.
Key serial number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information.
Source encrypted block	16 H	The encrypted PIN block received from the POS PIN terminal.
Account Number	12 N	The 12 right-most digits of the PAN, excluding the check digit.
PVKI	1 N	The PIN verification key indicator.
PVV	4 N	The PIN verification value from the card or data base.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'CN'.
Error Code	2 A	'00' : No error '01' : Verification failure '10' : BDK parity error '11' : PVK parity error '27' : BDK or PVK not double length '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 PIN Using the Diebold Method (DUKPT)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: Verify a PIN using the Diebold method.

Notes: This command implements the original DUKPT method of deriving a single-length PIN encryption key from the (double length) BDK. This command is provided for legacy applications: new applications should use the equivalent 3-DES DUKPT command (GS).

The command performs the same function as CG and EG. The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

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 'CO'.
BDK		The Base Derivation Key, used to decrypt the PIN block.
	32 H or 1 A + 32 H	For a Variant LMK, the 'BDK' must be encrypted under LMK pair 28-29.
	or 1 A + n A	For a Keyblock LMK, the 'BDK' must comply with the following: **Key Usage**: 'BO'; **Algorithm**: 'T'; **Mode of Use**: '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). See the Host Programmer Manual for further information.
Key serial number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information.
Source encrypted block	16 H	The encrypted PIN block received from the POS PIN terminal.
Account Number	12 N	The 12 right-most digits of the PAN, excluding the check digit.

Field	Length & Type	Details
PIN validation	16 H	User-defined data consisting of hexadecimal characters, and the letter N, which indicates where the HSM is to insert the last five digits of the account number specified in the Host request message. (The digits must be left-justified).
Offset	4 N	The Diebold offset value.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'CP'.
Error Code	2 A	'00' : No error '01' : Verification failure '10' : BDK parity error '27' : BDK not double length '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 PIN Using the Encrypted PIN Method (DUKPT)

Variant LMK ☑	Keyblock LMK ☑
License: **HSM9-LIC025**	
Authorization: **Not required**	

Function: Verify a PIN using the Encrypted PIN method.

Notes: This command implements the original DUKPT method of deriving a single-length PIN encryption key from the (double length) BDK. This command is provided for legacy applications: new applications should use the equivalent 3-DES DUKPT command (GU).

The command performs the same function as BC and BE. The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'CQ'.
BDK		The Base Derivation Key, used to decrypt the PIN block.
	32 H or 1 A + 32 H	For a Variant LMK, the 'BDK' must be encrypted under LMK pair 28-29.
	or 1 A + n A	For a Keyblock LMK, the 'BDK' must comply with the following: Key Usage: 'B0'; Algorithm: 'T'; Mode of Use: 'N'
KSN descriptor	3 H	The descriptor for the KSN (in the next field). See the Host Programmer Manual for further information.
Key serial number	12 - 20 H	The KSN supplied by the PIN pad. See the Host Programmer Manual for further information.
Source encrypted block	16 H	The encrypted PIN block received from the POS PIN terminal.
Account Number	12 N	The 12 right-most digits of the PAN, excluding the check digit.
PIN	L N or L H or 1 A + 32 H	The PIN from the host database, encrypted under the LMK. When using a 3-DES Variant or Keyblock LMK, the length of the encrypted PIN is L digits, where L is defined by the security setting "PIN Length". When using an AES Keyblock LMK, this field must consist of a 'J' followed by 32 hex digits.
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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 'CR'.
Error Code	2 A	'00' : No error '01' : Verification failure '10' : BDK parity error '27' : BDK not double length '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.

>> Chapter 3 – PIN Block Formats

General

For PIN verification and PIN translation, the HSM requires the PIN to be input as an encrypted 16-character PIN block. The plaintext data within the PIN block comprises the PIN and some form of padding to ensure that this data is 16 characters. The padding mechanism is known as the PIN block format. 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 and KY commands.

Detailed information on PIN Block formats can be found in Chapter 6 of the payShield 9000 General Information Manual.

>> Chapter 4 – Error Codes

General

The standard error codes returned by the payShield 9000 HSM 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 9000 HSM's host commands are backward compatible with those of the HSM8000, 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
31	Insufficient solicitation entries for batch
32	LIC007 (AES) not installed
33	LMK key change storage is corrupted
39	Fraud detection
40	Invalid checksum

Code	Description
41	Internal hardware/software error: bad RAM, invalid error codes, etc.
42	DES failure
43	RSA Key Generation Failure
47	Algorithm not licensed
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	Public key 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
91	Longitudinal Redundancy Check (LRC) character does not match the value computed over the input data (when the HSM has received a transparent async packet)
92	The Count value (for the Command/Data field) is not between limits, or is not correct (when the HSM has received a transparent async packet)
A1	Incompatible LMK schemes
A2	Incompatible LMK identifiers
A3	Incompatible keyblock LMK identifiers
A4	Key block authentication failure
A5	Incompatible key length
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 keyblock error
B3	Invalid number of optional blocks
B4	Optional block data error
B5	Incompatible components
B6	Incompatible key status optional blocks

Code	Description
B7	Invalid change field
B8	Invalid old value
B9	Invalid new value
BA	No key status block in the keyblock
BB	Invalid wrapping key
BC	Repeated optional block
BD	Incompatible key types
BE	Invalid keyblock header ID

>> Appendix A – EBCDIC to ASCII Table

EBCDIC Hex	Cha	ASCII Hex	EBCDIC Hex	Cha	ASCII Hex	EBCDIC Hex	Cha	ASCII Hex	EBCDIC Hex	Cha	ASCII Hex
00	NUL	00	40	SP	20	80		80	C0	{	7B
01	SOH	01	41		B9	81	a	61	C1	A	41
02	STX	02	42		C1	82	b	62	C2	B	42
03	ETX	03	43		C2	83	c	63	C3	C	43
04		97	44		C3	84	d	64	C4	D	44
05	HT	09	45		C4	85	e	65	C5	E	45
06		87	46		C5	86	f	66	C6	F	46
07	DEL	7F	47		C6	87	g	67	C7	G	47
08		92	48		C7	88	h	68	C8	H	48
09		86	49		C8	89	i	69	C9	I	49
0A		D0	4A		C9	8A		8A	CA		CA
0B	VT	0B	4B	.	2E	8B		8B	CB		CB
0C	FF	0C	4C	<	3C	8C		8C	CC		CC
0D	CR	0D	4D	(	28	8D		8D	CD		CD
0E	SO	0E	4E	+	2B	8E		8E	CE		CE
0F	SI	0F	4F		F1	8F		8F	CF		CF
10	DLE	10	50	&	26	90		90	D0	}	7D
11	DC1	11	51		D1	91	j	6A	D1	J	4A
12	DC2	12	52		D2	92	k	6B	D2	K	4B
13	DC3	13	53		D3	93	l	6C	D3	L	4C
14		A4	54		D4	94	m	6D	D4	M	4D
15		A5	55		D5	95	n	6E	D5	N	4E
16	BS	08	56		D6	96	o	6F	D6	O	4F
17		A1	57		D7	97	p	70	D7	P	50
18	CAN	18	58		D8	98	q	71	D8	Q	51
19	EM	19	59		D9	99	r	72	D9	R	52
1A		A7	5A	!	21	9A		9A	DA		DA
1B		88	5B	$	24	9B		9B	DB		DB
1C		1C	5C	*	2A	9C		9C	DC		DC
1D		1D	5D	)	29	9D		9D	DD		DD
1E		1E	5E	;	3B	9E		9E	DE		DE
1F		1F	5F	^	5E	9F		9F	DF		DF
20		AD	60	-	2D	A0		A0	E0	\	5C
21		E0	61	/	2F	A1	~	7E	E1		E1
22	FS	5D	62		E3	A2	s	73	E2	S	53
23		E2	63		E4	A3	t	74	E3	T	54
24		C0	64		E5	A4	u	75	E4	U	55
25	LF	0A	65		E6	A5	v	76	E5	V	56
26	ETB	17	66		E7	A6	w	77	E6	W	57
27	ESC	1B	67		E8	A7	x	78	E7	X	58
28		81	68		E9	A8	y	79	E8	Y	59
29		82	69		F0	A9	z	7A	E9	Z	5A
2A		83	6A	|	7C	AA		AA	EA		EA
2B		84	6B	,	2C	AB		AB	EB		EB
2C		85	6C	%	25	AC		AC	EC		EC
2D	ENQ	05	6D	_	5F	AD	[	5B	ED		ED
2E	ACK	06	6E	>	3E	AE		AE	EE		EE
2F	BEL	07	6F	?	3F	AF		AF	EF		EF
30		89	70		A8	B0		B0	F0	0	30
31		91	71		A9	B1		B1	F1	1	31
32	SYN	16	72		F2	B2		B2	F2	2	32
33		93	73		F3	B3		B3	F3	3	33
34		94	74		F4	B4		B4	F4	4	34
35		95	75		F5	B5		B5	F5	5	35
36		96	76		F6	B6		B6	F6	6	36
37	EOT	04	77		F7	B7		B7	F7	7	37
38		98	78		F8	B8		B8	F8	8	38
39		99	79	‘	60	B9		F9	F9	9	39
3A		A2	7A	:	3A	BA		BA	FA		FA
3B		A3	7B	#	23	BB		BB	FB		FB
3C	DC4	14	7C	@	40	BC		BC	FC		FC
3D	NAK	15	7D	\	5C	BD		BD	FD		FD
3E		A6	7E	=	3D	BE		BE	FE		FE
3F	SUB	1A	7F	"	22	BF		BF	FF		FF

>> Appendix B – Internal Auditing

General

The audit log is stored within the payShield 9000 HSM in an audit trail buffer that will hold up to 2000 (50,000 from v1.4a) audit records. The audit records stored inside the HSM can be viewed by use of the AUDITLOG console command. Viewing the audit records at the console does *not* alter their archived or retrieved status.

When the audit records are output to either host or printer, they are protected with a MAC. The random MAC key used to generate the MAC is output at the same time. The MAC key will be different for every record that is output. When an audit record is output in this way, the internal copy has its corresponding archived or retrieved status updated immediately following the output.

The internal copy of the audit record remains in the HSM's audit log until it is deleted using an appropriate host or console command (or overwritten due to the number of records reaching the maximum permitted). An audit record must be archived or retrieved (or both) before it can be deleted by the host.

When the HSM's LMK is changed, records previously extracted using the host commands will require their MAC keys translating from the old LMK to the new LMK.

Audit Record Format

This section describes the format of the Audit Record, which can be retrieved from the HSM using the Q2 host command. The same information is included in the output from the AUDITPRINT Console command, described in the Console Reference Manual.

Field #	Name	Length	Description
1	Audit Counter	4 bytes	Binary counter (0..4294967295), indicating the position of this record within the audit log.
2	Date/Time Stamp	6 bytes	The following six fields are BCD encoded: Hour (00..23) Minute (00..59) Second (00.59) Day (01..31) Month (01..12) Year (00..99) (years since 2000).
3	Command Code / Action Code	2 bytes	For Command Code Types 00, 01 and 10, this field contains the relevant Command Code. For Command Code Type 11, this contains an Action Code.
4	Command Code Type *	2 bits	00 – Host Command 01 – Console Command 10 – Fraud Event 11 – User Action
5	Archived Status Bit	1 bit	1 = archived, 0 = not archived.
6	Retrieved Status Bit	1 bit	1 = retrieved, 0 = not retrieved.
7	Unused	12 bits	Set to binary 0.
8	Response Error Code	2 bytes	2 digit Response Code from host command's response message.
9	Audit Record MAC	8 bytes	MAC generated over fields 1..8 using the following Random MAC Key.
10	Random MAC Key	16 bytes	Key used to generate the audit record MAC. Encrypted under the LMK.

* In the output from AUDITPRINT Console command, the Command Code Type is changed to an alphabetic indicator as follows:

- Host Command: "H" (in place of "00" in the Q2 Host command)
- Console Command: "C" (in place of "01" in the Q2 Host command)
- Fraud Event: "F" (in place of "10" in the Q2 Host command)
- User Action: "A" (in place of "11" in the Q2 Host command)

Command Code Types

Command Code Type 00 – Host Command

Audited host commands have their command code in the record's Command Code field and, the corresponding response error code in the Response Error Code field.

Command Code Type 01 – Console Command

Audited console commands have their command code* in the record's Command Code field and 00 in the Response Error Code field.

*Note: The payShield HSM has some console commands that do not have exactly two characters in length. In addition, there are some actions which are not strictly Console activities but are designated as Console commands in the Audit record. For storage within the audit record, these longer commands should be mapped to the following two character strings:

Console Command	Audit Record Command Code
User actions performed using HSM Manager, inc. log retrieval, log clearing, logins, disconnections, state changes, setting audit options, and automatic audit log entry arising from a key or component entry action made using HSM Manager.	'00'
AUDITLOG	'01'
AUDITOPTIONS	'02'
CLEARAUDIT	'03'
CLEARERR	'04'
EJECT	'05'
ERRLOG	'06'
GETCMDS	'07'
GETTIME	'08'
SETTIME	'09'
A	'0A'
B	'0B'
C	'0C'
D	'0D'
F	'0E'
K	'0F'
N	'10'
R	'11'
T	'12'
V	'13'
Z	'14'

Console Command	Audit Record Command Code
$	'15'
CONFIGCMDS	'16'
CONFIGPB	'17'
PING	'18'
TRACERT	'19'
NETSTAT	'1A'
AUDITPRINT	'1B'
SYSLOG	'1C'
UTILCFG	'1D'
UTILENABLE	'1E'
UTISTATS	'1F'
HEALTHENABLE	'20'
HEALTHSTATS	'21'
SNMP	'22'
SNMPADD	'23'
SNMPDEL	'24'
RESET	'25'
ROUTE	'26'
TRAP	'27'
TRAPADD	'28'
TRAPDEL	'29'
CONFIGACL	'2A'

Note: some of the above Console commands are not currently in use, and are for possible future enhancements to the payShield 9000.

Command Code Type 10 – Fraud Event

The command code type 'Fraud Event' represents the fraud detection functions built into the payShield 9000.

When a fraud event is detected, the command code of the command that caused the fraud event to be detected is recorded in the audit record's Command Code field. The Response Error Code field is then set as follows:

Fraud Event	Audit Record Response Code
Limit for number of PIN verifications per minute exceeded	01
Limit for number of PIN verifications per hour exceeded	02
Limit for total number of failed PIN verifications exceeded	03

Command Code Type 11 – User Action

The command code type 'User Action' represents the actions under user control that do not involve a console or host command, for example, changing to/from online, offline and secure mode, into/out of authorized state, and power cycling the HSM.

Note: User actions cannot be enabled or disabled individually.

The following table indicates the contents of the Command Code field for each possible User Action:

Audited User Action	Audit Record Command Code
Automatic audit log entry arising from Authorization Cancelled (i.e. single authorized state)	'A0' (zero)
Automatic audit log entry arising from Authorization ON (i.e. single authorized state)	'A1'
Automatic audit log entry arising from Authorization Activity ON (i.e. multiple authorized states)	'AA'
Automatic audit log entry arising from Authorization Activity Cancelled (i.e. multiple authorized states)	'AC'
Automatic audit log entry arising from Authorization Timeout	'AT'
Audit log cleared	'CL'
Automatic audit log entry arising from Diagniostic Event (Self test)	'DE'
Automatic audit log entry arising from Key/component Entry at the Console or using a smartcard to authenticate a user at the Console or HSM Manager.	'KE'
LMK erased	'LE'
License file load failure	'LF'
LMK loaded	'LL'
License file successfully loaded	'LS'
Old LMK erased	'OE'
Change to Offline	'OF'
Old LMK loaded	'OL'
Change to Online	'ON'
Cycle power supply	'PW'
Change to Secure	'SE'
Utilization Reset	'UT'

The Response Code for all User Action records is 00.

>> Appendix C – Fraud Detection

This information can now be found in Chapter 7 of the payShield 9000 General Information Manual.

>> Appendix D – Key Usage Table

The Keyblock Key Usage Table can now be found in Chapter 5 of the payShield 9000 General Information Manual.

>> Appendix E – Mode of Use Table

The Keyblock Mode of Use Table can now be found in Chapter 5 of the payShield 9000 General Information Manual.

>> Appendix F – Key Usage Conversion Table

The conversions used when exporting from Thales Keyblock format to TR-31 format are now included in the Keyblock Key Usage Table in Chapter 5 of the payShield 9000 General Information Manual..

>> Appendix G – Example Host Commands and Sample Code

Notation

In the "Format" column in the following examples the following abbreviations are used:

- n – represents a variable number of characters or bytes.
- A – represents Alphanumeric (ASCII or EBCDIC) characters.
- H – represents hexadecimal digits ("0..9" and "A..F")
- B – represents Bytes of binary data
- C – represents Control characters

In the following examples of input/output data, <…> indicates binary data represented as Hexadecimal characters to allow the data to be shown as printable characters in this document. In reality the data would be sent/received as bytes of binary data. The "<" and ">" are not part of the sent/received data.

Sample Code

The unsupported sample code provided below lets software developers send individual commands to a payShield 9000 and receive responses back.

The code below runs the host command *HEADNC* (i.e. a 4-character header followed by the command code *NC*). The text *HEADNC* can be replaced by any desired host command. The example command text provided in this Appendix can be cut & pasted into the code below. Note that:

- Responses may be different from the examples in this document depending on security settings and the LMK being used. Most of the example commands use the Test LMKs delivered with the payShield 9000.
- This code is designed for use with Python v2.7. It may not run correctly if used with other versions of Python. The Python runtime environment can be downloaded free of charge from www.python.org .
- Copy the code within the text box below and save it as a file with a *.py* extension (for example *codeSample1.py*)
- After installing Python, the code can then be run by executing the following from the command line:
    - *python codeSample1.py*

Code Sample 1

This code is very simple, and is suggested to be used for initial testing to get connections established with the HSM. The main limitation of this code is that it supports only Alphanumeric data in commands and responses, and cannot be used to send/receive binary data.

```
#!/usr/bin/python

import socket
from struct import *

# Change HSM IP and Port below to match deployment
TCP_IP = '192.168.0.60'
TCP_PORT = 1500
BUFFER_SIZE=1024

# paste command example within inverted commas below:
#e.g.:
COMMAND = 'HEADNC'

# 1st two bytes must be command length
SIZE=pack('>h',len(COMMAND))

# join everything together
MESSAGE = SIZE + COMMAND

# Create socket and connect
hsmSocket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
hsmSocket.connect((TCP_IP, TCP_PORT))

# send MESSAGE
hsmSocket.send(MESSAGE)

# receive
data = hsmSocket.recv(BUFFER_SIZE)

# close socket
hsmSocket.close()

print "sent data (ASCII)     : ", MESSAGE
print "sent data (HEX)       : ", MESSAGE.encode('hex')
print "received data (ASCII): ", data
print "received data (HEX)   : ", data.encode('hex')
```

Code Sample 2

This code supports the input and output of binary data, with the binary data being represented as hexadecimal characters and enclosed in angle brackets. For example, to enter the binary data *1001011001011110* the command input would include *<965E>* .

```
#!/usr/bin/python

import socket, binascii, string
from struct import *

# Change HSM IP and Port below to match deployment
TCP_IP = "192.168.0.60"
TCP_PORT = 1500

# paste command example within inverted commas below:
#e.g.:
COMMAND = 'HEADNC'

def testPrintable(str):
    return all(c in string.printable for c in str)

def buildCommand(command):
  #convert hex supplied data into binary
  hCommand = ''
  i = 0
  while True:
    if (command[i:i+1] == '<'):
      i = i + 1
      while True:
        hCommand = hCommand + binascii.a2b_hex(command[i:i+2])
        i = i + 2
        if (command[i:i+1] == '>'):
          i = i + 1
          break
    else:
      hCommand = hCommand + command[i]
      i = i + 1

    if (i == len(command)):
      break

  return hCommand

def main():
  global TCP_IP
  global TCP_PORT
  global COMMAND

  # Create socket and connect
  connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
  connection.connect((TCP_IP, TCP_PORT))

  BUFFER_SIZE = 1024
```

Continued on next page …

... continued from previous page.

```
    # Convert hex to binary
    COMMAND = buildCommand(COMMAND)

    # calculate the size and format it correctly
    SIZE=pack('>h',len(COMMAND))

    # join everything together
    MESSAGE = SIZE + COMMAND

    # send MESSAGE
    connection.send(MESSAGE)

    # receive data
    data = connection.recv(BUFFER_SIZE)

    # don't print ascii if msg or resp contain non printable chars
    if (testPrintable(MESSAGE[2:])):
      print "sent data (ASCII)     :", MESSAGE[2:]
    print "sent data (HEX)       :", MESSAGE.encode('hex')

    if (testPrintable(data[2:])):
      print "received data (ASCII):", data[2:]
    print "received data (HEX)   :", data.encode('hex')

    connection.close()

  if __name__ == "__main__":
    main()
```

A0 Command - Generate a TPK

The A0 command is used to generate DES or TDES keys. (The EI command is used to generate RSA key pairs – see later.) The key will be encrypted under the appropriate LMK variant or in an LMK-encrypted keyblock with appropriate parameters. Optionally the key can also be encrypted under a TMK or ZMK for export to other systems.

In the example below, we are generating a double-length TDES TPK, which is also to be exported under a double-length TDES ZMK using X9.17 methods. (*Note: for this to be allowed, the security settings must allow export using X9.17 and to allow export in non-trusted format.*)

The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
HDR1 A01002U;1U3E8C28EBF7D3799DC7147E3441F8E452X
```

Fld	Format	Value	Description
1	4 A	HDR1	Message header (as defined by user).
2	2 A	A0	Command Code. (Note: the second character is a numeric zero.)
3	1 H	1	Mode. 0 = Generate key and encrypt under a TMK
4	3 H	002	Key Type. 002 = TPK
5	1 A	U	Key Scheme - for encrypting the output key under the LMK. U = Double-length TDES key scheme
6	1 A	;	Delimiter
7	1 N	1	TMK/ZMK Flag 1 = Key is to be exported under a TMK.
8	1 A + 32 H	U3E8C28EBF7D3799DC7147E3441F8E452	The TMK (encrypted under LMK pair 14-15 variant 0 or 36-37 variant 8, depending on whether PCI HSM compliance has been enforced) that the exported TPK is to be encrypted under.
9	1 A	X	Key Scheme for exporting the TPK encrypted under the TMK. X = Encryption of a double length key using X9.17 methods

Response

HDR1A100UF4395AE377FA12297721AB182E96C552XE2C6964890CEF33393BAFAD61D26D11ADD60A7

Fld	Format	Value	Description
1	4 A	HDR1	Message header (as defined by user).
2	2 A	A1	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	1 A+ 32 H	UF4395AE377FA12297721AB182E96C552	The generated TPK, encrypted under LMK pair 14-15 variant 0 or 36-37 variant 7, depending on whether PCI HSM compliance has been enforced. U = Double-length TDES key scheme
5	1 A+ 32 H	XE2C6964890CEF33393BAFAD61D26D11A	The generated TPK encrypted under the TMK
6	6 H	DD60A7	Key Check Value

A0 Command - Generate an IKEY/IPEK

In this example for A0, we are deriving a double-length TDES DUKPT Initial Key (a.k.a. Initial PIN Encryption Key) from a double-length TDES BDK (Type 2). The key does not need to be exported.

The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

HDR2A0A302U02U000595797DB29310FDF463ABB8396F451016E3658200007

Fld	Format	Value	Description
1	4 A	HDR2	Message header (as defined by user).
2	2 A	A0	Command Code. (Note: the second character is a numeric zero.)
3	1 H	A	Mode. A = Derive key (from a BDK)
4	3 H	302	Key Type. 302 = IKEY/IPEK, encrypted under Variant LMK pair 14-15.
5	1 A	U	Key Scheme - for encrypting the output key under the LMK. U = Double-length TDES key scheme
6	1 A	0	Derive Key Mode 0 = Derive IKEY/IPEK from BDK
7	1 H	2	DUKPT Master Key Type. 2 = Type 2 BDK
8	1 A + 32 H	U000595797DB29310FDF463ABB8396F45	The Type 2 BDK encrypted under LMK pair 28-29 variant 6
9	15 H	1016E3658200007	KSN (Key Serial Number), consisting of a Key Set Identifier and Device ID for deriving the Initial Key. (NOTE: there is no Transaction Counter, as there would be with a KSN sent in transaction data from a terminal.)

Response

HDR2A100U4D374057BB0CB56246B0417CE2319C8175CA90

Fld	Format	Value	Description
1	4 A	HDR2	Message header (as defined by user).
2	2 A	A1	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	1 A + 32 H	U4D374057BB0CB56246B0417CE2319C81	The generated IKEY/IPEK, encrypted under Variant LMK pair 14-15, variant 3. U = Double-length TDES key scheme
5	6 H	75CA90	Key Check Value (KCV).

CA Command - Translate a PIN from TPK to ZPK Encryption

The CA command is used to translate a PIN Block received from an ATM or POS terminal (and encrypted under a TPK) into PIN Block encrypted under a ZPK for onward transmission into the payments network. Different formats can be used for the received and translated PIN Blocks, but note that some standards (e.g. PCI HSM) limit which PIN Block format translations are permitted.

The CA command is used as the benchmark for specifying the payShield 9000. For example, the Model X payShield 9000, rated at 1,500 tps, can process 1,500 CA transactions (commands) per second.

In the example here, both the TPK and ZPK are double-length TDES keys, and Thales Format 01 (= ISO/ANSI Format 0) is used for both PIN Blocks.

The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
HDR7CAU1750CDFB0757D3B3994430636DBB281BUA787EF2F6595A8158EECE42B11
70228912BFB87728013AD7610101234567812345
```

Fld	Format	Value	Description
1	4 A	HDR7	Message header (as defined by user).
2	2 A	CA	Command Code.
3	1 A + 32 H	U1750CDFB0757D3B3994430636DBB281B	The TPK (encrypted under LMK pair 14-15 variant 0 or 36-37 variant 7, depending on whether PCI HSM compliance has been enforced) under which the PIN block is currently encrypted. U = Double-length TDES key scheme
4	1 A + 32 H	UA787EF2F6595A8158EECE42B11702289	The ZPK (encrypted under LMK pair 06-07 variant 0) under which the PIN block is to be encrypted. U = Double-length TDES key scheme
5	2 N	12	Maximum PIN Length -must be between 04 and 12.
6	16 H	BFB87728013AD761	Source PIN Block, encrypted under the TPK.
7	2 N	01	Source PIN Block format code. 01 = ISO 9564-1 & ANSI X9.8 format 0.
8	2 N	01	Output PIN Block format code. 01 = ISO 9564-1 & ANSI X9.8 format 0.
9	12 N	234567812345	Account Number. For output PIN Block format code = 01, the 12 right-most digits of the PAN excluding the check digit.

Response

HDR7CB000447125015E32C3FA301

Fld	Format	Value	Description
1	4 A	HDR7	Message header (as defined by user).
2	2 A	CB	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	2 N	04	Length of the returned PIN.
5	16 H	47125015E32C3FA3	Output PIN Block
5	2 N	01	Output PIN Block format code - as provided in the command. 01 = ISO 9564-1 & ANSI X9.8 format 0.

CA Command - Translate a PIN from TPK to ZPK Encryption (using keys and PIN Block held in user storage)

In this example, rather than the encrypted TPK, ZPK, and PIN Block being included in the command data, the command includes indexes to these items stored within the HSM's user storage area.

The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
HDR7CAUK000UK00212K0040101234567812345
```

Fld	Format	Value	Description
1	4 A	HDR7	Message header (as defined by user).
2	2 A	CA	Command Code.
3	2 A + 3 H	UK000	Index to the TPK (encrypted under LMK pair 14-15 variant 0 or 36-37 variant 7, depending on whether PCI HSM compliance has been enforced) held in user storage. First character is used to define the key scheme (e.g. "U" = Double-length TDES key scheme) or is not present for single-length DES. The second character of "K" indicates that a key reference is being used. The final 3 hex characters, "000", are the index to where the key is stored in user storage. If the key is stored in multiple indices (e.g. the block size has been set to "Single" but a double-length key has been stored) then this index points to the first of the blocks where the key is stored.
4	2 A + 3 H	UK002	Index to the ZPK (encrypted under LMK pair 06-07 variant 0) under which the PIN block is to be encrypted, held in user storage. "U" = Double-length TDES key scheme. The second character of "K" indicates that a key reference is being used. The final 3 hex characters, "002", are the index to where the key is stored in user storage. If the key is stored in multiple indices (e.g. the block size has been set to "Single" but a double-length key has been stored) then this index points to the first of the blocks where the key is stored.
5	2 N	12	Maximum PIN Length -must be between 04 and 12.
6	16 H	K004	Index to the Source PIN Block encrypted under the TPK, held in user storage. "K" indicates that a key reference is being used. The final 3 hex characters, "004", are the index to where the PIN Block is stored in user storage.
7	2 N	01	Source PIN Block format code. 01 = ISO 9564-1 & ANSI X9.8 format 0.
8	2 N	01	Output PIN Block format code. 01 = ISO 9564-1 & ANSI X9.8 format 0.
9	12 N	234567812345	Account Number. For output PIN Block format code = 01, the 12 right-most digits of the PAN excluding the check digit.

Response

The response will be the same as in the preceding example.

CA Command - Translate a PIN from TPK to ZPK Encryption (Keyblock LMK)

In this example of the use of the CA command, we are using a keyblock LMK rather than a variant LMK. Both the TPK and the ZPK are included in the command in the format of a Thales Keyblock, which contains metadata about the key as well as the encrypted key and a MAC.

The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
HDR8CAS0005671DN00N00026C2A641FEA15E950310D601D7E274B4C74032139S00
05672DN00N00022BA44D32EE85E5BCEF74AA3C376D8C18EF702A70123C8FFAD1C7
4C12AB0102123456789012
```

Fld	Format	Value	Description
1	4 A	HDR8	Message header (as defined by user).
2	2 A	CA	Command Code.
3	1 A + 56 H	S0005671DN00N00026C2A641FEA15E950310D601D7E274B4C74032139	The TPK (encrypted under a Keyblock LMK) under which the PIN block is currently encrypted. S = Keyblock key scheme 0 = Version 0056 = total length of keyblock 71 = key usage (TPK) D = Algorithm (DES) N = Mode of Use (No special restrictions) 00 = Key Version Number N = Exportability (No Export permitted) 00 =number of optional header blocks 02 = LMK Identifier 6C2…B4C = Encrypted TPK 74032139 = MAC
4	1 A + 56 H	S0005672DN00N00022BA44D32EE85E5BCEF74AA3C376D8C18EF702A70	The ZPK (encrypted under a Keyblock LMK) under which the PIN block is to be encrypted. S = Keyblock key scheme 0 = Version 0056 = total length of keyblock 72 = key usage (ZPK) D = Algorithm (DES) N = Mode of Use (No special restrictions) 00 = Key Version Number N = Exportability (No Export permitted) 00 =number of optional header blocks 02 = LMK Identifier 2BA…C18 = Encrypted ZPK EF702A70 = MAC
5	2 N	12	Maximum PIN Length - must be between 04 and 12.
6	16 H	3C8FFAD1C74C12AB	Source PIN Block, encrypted under the TPK.
7	2 N	01	Source PIN Block format code. 01 = ISO 9564-1 & ANSI X9.8 format 0.
8	2 N	02	Output PIN Block format code. 02 = Docutel ATM format.
9	12 N	123456789012	Account Number.

Response

HDR7CB0004B9392CE3ABBA5BE702

Fld	Format	Value	Description
1	4 A	HDR7	Message header (as defined by user).
2	2 A	CB	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	2 N	04	Length of the returned PIN.
5	16 H	B9392CE3ABBA5BE7	Output PIN Block
5	2 N	02	Output PIN Block format code - as provided in the command. 02 = Docutel ATM format..

DE Command - Generate an IBM PIN Offset

The DE command allows for customer-selected PINs where the "natural" PIN has been generated using the IBM 3624 method (e.g. by using the EE host command), by calculating the offset between the natural and selected PINs.

The command is required because the card issuer does not know the natural PIN – they have access only to the natural PIN encrypted under the LMK. Note that the LMK-encrypted PIN uses an algorithm which involves the account number, and therefore the LMK-encrypted PIN for two different cardholders will be different even if they have the same cleartext PIN.

In this example we are using a single-DES PVK. The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
HDRCDE9A7EC8F365E1C0B01582604423046815398DD0BDFA69B41010C112233N44
556
```

Fld	Format	Value	Description
1	4 A	HDRC	Message header (as defined by user).
2	2 A	DE	Command Code.
3	16 H	9A7EC8F365E1C0B0	PVK that is used to generate the offset. The PVK is encrypted under LMK pair 14-15 variant 0.
4	10 N	1582604423	LMK-encrypted PIN. The length of this field is determined by the "PIN Length" security setting + 1.
5	2 N	04	Minimum PIN Length
6	12 N	423046815398	The 12 right-most digits of the PAN, excluding the check digit.
7	16 H	DD0BDFA69B41010C	Encrypted Decimalisation Table.
8	12 A	112233N44556	User-defined data. The "N" indicates where the last 5 digits of the PAN should be inserted.

Response

```
HDRCDF000835FFFFFFFF
```

Fld	Format	Value	Description
1	4 A	HDRC	Message header (as defined by user).
2	2 A	DF	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	12 H	0835FFFFFFFF	The resulting Offset, F-padded to the left.

DE Command - Generate an IBM PIN Offset (using a Decimalisation Tabel held in User Storage)

The DE command allows for customer-selected PINs where the "natural" PIN has been generated using the IBM 3624 method (e.g. by using the EE host command), by calculating the offset between the natural and selected PINs.

The command is required because the card issuer does not know the natural PIN – they have access only to the natural PIN encrypted under the LMK. Note that the LMK-encrypted PIN uses an algorithm which involves the account number, and therefore the LMK-encrypted PIN for two different cardholders will be different even if they have the same cleartext PIN.

In this example we are using a single-DES PVK. The Decimalisation Table is held in the User Storaget area. The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
HDRCDE9A7EC8F365E1C0B0158260442304681539 8DD0BDFA69B41010C112233N44
556
```

Fld	Length	Value	Description
1	4 A	HDRC	Message header (as defined by user).
2	2 A	DE	Command Code.
3	16 H	9A7EC8F365E1C0B0	PVK that is used to generate the offset. The PVK is encrypted under LMK pair 14-15 variant 0.
4	10 N	1582604423	LMK-encrypted PIN. The length of this field is determined by the "PIN Length" security setting + 1.
5	2 N	04	Minimum PIN Length
6	12 N	423046815398	The 12 right-most digits of the PAN, excluding the check digit.
7	16 H	K123	Reference to the Encrypted Decimalisation Table, held in user storage at index 123. (Note: first character is the Index Flag and always has a value of 'K', irrespective of the value of the Index Flag used when the data was read into user storage using the LA command.)
8	12 A	112233N44556	User-defined data. The "N" indicates where the last 5 digits of the PAN should be inserted.

Response

```
HDRCDF000835FFFFFFFF
```

Fld	Length	Value	Description
1	4 A	HDRC	Message header (as defined by user).
2	2 A	DF	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	12 H	0835FFFFFFFF	The resulting Offset, F-padded to the left.

DG Command - Generate a Visa PVV of an LMK-encrypted PIN

The DG command is used to calculate the PVV from the PIN – e.g. after the cardholder has selected a new PIN. The PIN is provided in the command as an LMK-encrypted PIN, which uses an algorithm involving the account number, and therefore the LMK-encrypted PIN for two different cardholders will be different even if they have the same cleartext PIN. The command can optionally check the PIN against a list of weak or excluded PINs.

In the example below, the PVK pair are each single-length DES keys. Two excluded PINs are provided in the command, and LMK with ID=02 is to be used.

The user has specified a header (with the length set to 4 characters in the host port settings) and a trailer.

Command

```
HDRDDG445ACC722DB0B8854A1DAAD18F1B59A6158264230468153983*020412341
111%03<19>TRLRD
```

Fld	Format	Value	Description
1	4 A	HDRD	Message header (as defined by user).
2	2 A	DG	Command Code.
3	32 H	445ACC722DB0B885 4A1DAAD18F1B59A6	PVK Key Pair, each encrypted under LMK Pair 14-15 variant 0.
4	5 N	15826	LMK-encrypted PIN. The length of this field is determined by the "PIN Length" security setting + 1.
5	12 N	423046815398	The 12 right-most digits of the PAN, excluding the check digit.
6	1 N	3	PVKI. Valid range is "0" to "6".
7	1 A	*	Delimiter, indicating that an excluded PIN table follows.
8	2 N	02	Number of entries in the excluded PIN table.
9	2 N	04	Length of each encrypted PIN (must be in range 04-12).
10	8 N	12341111	Excluded PIN table – i.e. PINs "1234" and "1111" are not allowed.
11	1 A	%	Delimiter to indicate that an LMK ID follows
12	2N	03	LMK 03 must be used for this command.
13	1 C	<19>	Delimiter to indicate that a trailer follows.
14	4 A	TRLRD	Trailer, as defined by user.

Response

```
HDRDDH005809<19>TRLD
```

Fld	Format	Value	Description
1	4 A	HDRD	Message header (as defined by user).
2	2 A	DH	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	4 N	5809	The output PVV
5	1 C	<19>	Delimiter to indicate that a trailer follows.
6	4 A	TRLRD	Trailer, as provided in command.

EE Command – Derive a PIN using the IBM Method

The EE command derives a "natural" PIN based on the account number, using the IBM 3642 method.

A single-length DES PVK is being used to derive the PIN.

The user has specified a header (with the length set to 4 characters in the host port settings) and a trailer.

Command

```
HDRDEE9A7EC8F365E1C0B02468FFFFFFFF04423046815398DD0BDFA69B41010C11
2233N44556<19>TRLRD
```

Fld	Format	Value	Description
1	4 A	HDRD	Message header (as defined by user).
2	2 A	EE	Command Code.
3	16 H	9A7EC8F365E1C0B0	PVK Key Pair used to derive the PIN, each encrypted under LMK Pair 14-15 variant 0.
4	12 H	2468FFFFFFFF	Offset, padded to the right with hexadecimal digit F.
5	2 N	04	Minimum PIN length
6	12 N	423046815398	Account number – 12 rightmost digits excluding the check digit.
7	16 H	DD0BDFA69B41010C	Decimalization table.
8	12 A	112233N44556	User defined PIN Validation Data. The "N" character indicates where the last 5 digits of the account number should be inserted.
9	1 C	<19>	Delimiter to indicate that a trailer follows.
10	4 A	TRLRD	Trailer, as provided in command.

Response

```
HDRDEF0088949<19>TRLRD
```

Fld	Format	Value	Description
1	4 A	HDRD	Message header (as defined by user).
2	2 A	EF	Response Code.
3	5 N	88949	The derived PIN encrypted under the LMK. The length of this field is determined by the "PIN Length" security setting + 1.
4	1 C	<19>	Delimiter to indicate that a trailer follows.
5	4 A	TRLRD	Trailer, as provided in command.

EI Command - Generate RSA Key Pair

The EI command is used to generate RSA key pairs. (AO command is used to generate DES and TDES keys – see the examples earlier in this section).

In this example we are generating a key pair for use in key management with modulus length of 1,024 bits. The user has specified a header (with the length set to 4 characters in the host port settings) and a trailer.

Command

```
HDR9 EI1102401<19>4RH486ET4U8J4R5874T8
```

Fld	Format	Value	Description
1	4 A	HDR9	Message header (as defined by user).
2	2 A	EI	Command Code.
3	1 N	1	Key type indicator. 0 = key management only.
4	4 N	1024	Modulus length in bits.
5	2 N	01	Encoding rules for the public key. 01 = DER encoding for ASN.1 Public Key (INTEGER uses unsigned representation).
6	1 C	<19>	Delimiter, indicating that there is a trailer for the message.
7	20 A	4RH486ET4U8J4R5874T8	Message trailer, defined by user. (Max length is 32 chars.)

Response

```
HDR9EJ00<308188028180ADAF406F3901EC0F2583BB1945C49D7B3924A4AFC7833
FFC4C03BF13134DA8E3F28DE306E40D83B7975AC45D128D24EFF0057505F1FEC90
A7EA4CBB483A884168E85E60939A72F74945D3D3889BD41B564736E8FC90D26B1E
97FBFF03A7B584E2AFEAE39D19F00798782FCA09BEF18A3F3027900DF5A1E0ED50
384AED1C52FAF0203010001>0344<AC5DC5A50CA3D9293629994FF8452E767B790
90C9F6B86C60149473B5EAFDF109828250DF286542120A4EFB678694B244A8C18F
5889109F6EBB226200559212730C13609274A5816A6074DC7AAE39B707EB5B3F2A
A7D2EAAA10A6D3A6EFC784A7749F0800E784F0E6E03921317426D4DA8522E50E50
63DA1F2AEC33018E7A6BC07AA2914D42E351BB88A2FAF3D581D6D16D800D6FFAF5
1FCABF1F95A9429AF94E564C549B0FFF261C8310EE165DCBA3E7CEF83421D3FAEB
40FD7A1BBDD620EEA44B4233D15A7F9FBBB8BAB8D2016601A43110F7EF5CACAC28
2E82D5D580171EEB0515422B71CC2F746C427D48B9F3FAF0D2B8F7186F0E5D63A9
946E97F08BB97443FD700D641169FD975792EF7FA79E78CDFB85973EE14F7F1234
478F947ACB472B51130FD2C4959B7835D49CF2FA014F17CC913CD8A4D2D92ABF6A
3BE6FBE0E12026077C2FDFCDA1D825402E0399AC47527F7E881BA68F1><19>4RH4
86ET4U8J4R5874T8
```

Fld	Format	Value	Description
1	4 A	HDR9	Message header (as defined by user).
2	2 A	EJ	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	392 bits	<3081…0001>	Public key, encoded as required by field 5 of the command.
5	4 N	0344	Length of Private key, in bytes.

Fld	Format	Value	Description
6	120 B	<AC5D…68F1>	Private key, encrypted under the LMK.
7	1 C	<19>	Delimiter, indicating that there is a trailer for the message.
8	20 A	4RH486ET4U8J4R5874T8	Message trailer as provided in the command.

EO Command - Import a Public Key

This command allows a public RSA key to be imported by generating a MAC on it (variant LMK) or creating a keyblock (keyblock LMK). This might be used to protect a CA public key.

If the payShield 9000 has optional license LIC019 installed and generated the RSA key as Type 4 keys, this command can be used to decrypt and import random binary data in place of the public key.

In the following example, we are importing a public key. The user has specified a header (with the length set to 4 characters in the host port settings) and a trailer.

Command

```
HDRAEO01<30470240AE213EBDFE272616058114CA5D6E8DDD2F976EF0C6D6F6ADE
0204E916CE0B5C704A1A9F1F631F578D7B87D1981951BB99A572400AC43BB3AF8C
2A4068A0052250203010001><41555448454E2D44415441><19>GF6W54G65WR456
GAER54GE6R45G6E4AR
```

Fld	Format	Value	Description
1	4 A	HDRA	Message header (as defined by user).
2	2 A	EO	Command Code. (NOTE: the 2nd character is an alphabetic "O" for Oscar.)
3	2 N	01	Encoding rules for the public key. 01 = DER encoding for ASN.1 Public Key (INTEGER uses unsigned representation).
4	584 bits	<3047…0001>	Public key, encoded as required by field 3.
5	88 bits	<4155…5441>	Additional data for the MAC calculation.
6	1 C	<19>	Delimiter, indicating that there is a trailer for the message.
7	32 A	GF6W54G65WR456GAER54GE 6R45G6E4AR	Message trailer, defined by user. (Max length is 32 chars.)

Response

```
HDRAEP00<9C350891><30470240AE213EBDFE272616058114CA5D6E8DDD2F976EF
0C6D6F6ADE0204E916CE0B5C704A1A9F1F631F578D7B87D1981951BB99A572400A
C43BB3AF8C2A4068A0052250203010001><19>GF6W54G65WR456GAER54GE6R45G6
E4AR
```

Fld	Format	Value	Description
1	4A	HDR9	Message header (as defined by user).
2	2A	EP	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	4 Bytes	<9C350891>	MAC on the public key and additional data, calculated using LMK key pair 36-37.
5	584 bits	<3047…0001>	The imported Public Key, encoded as per field 3 of the command.
6	1 C	<19>	Delimiter, indicating that there is a trailer for the message.
7	32 A	GF6W54G65WR456GAER54GE 6R45G6E4AR	Message trailer, as provided in the command.

EW Command - Generate a signature (with variant LMK-encrypted RSA key provided in the command)

The EW command generates a signature over a message using an RSA private key encrypted under a variant LMK. In this example, the variant LMK-encrypted RSA private key is included in the command.

Command

```
0320EW0201010013<6162636465676869606162636 4>;990264<6783CD3B9B468B
622190C50C91D7559CB1654D2BBEB41F449CB202A910B5AB7B1716A2B13012403D
D1333E264BE0ED677B0ADF8F5B849C3E9312887E095F3A97E6AA9A7B33E23AE2E7
41801ADA0589173C22BC6355368B737BA6C78781D0308EDF4E7A7AD833FF7061BE
6B988C9399A13FDDDF66EAAEEC3744016ACEA6FCF49F2BF69D45784F561324B0D4
DC9EF65373E4566DEFC2B67F328780E38FEEA74519F63BCE9712C82A8763DEEBFD
FF24CA2CA98A7C1DC799A897C3AD0C25355A9F0CD9D7262C84D2D1C5C4556E3488
7B6975AEC66E2A244EBAE3C582CFD91A8747A735BCE60B905F6053691440C9BB2E
658C27D77B2752674026A1676EB9EC5FC6B158A4916C92864040>
```

Fld	Format	Value	Description
1	4 A	0320	Message header (as defined by user).
2	2 A	EW	Command Code.
3	2 N	02	Hash identifier. (02 = MD5)
4	2 N	01	Signature identifier. (01 = RSA)
5	2 N	01	Pad mode identifier (01 = PKCS#1 v1.5)
6	4 N	0013	Data Length
7	13 B	<6162636465676869606162636364>	Message to be signed
8	1 A	;	Delimiter
9	2 N	99	Private key flag. (99 = key identified below.)
10	4 N	0264	Private key length
11	264 B	<6783CD3B9B468B622190C50C91D7559CB1654D2BBEB … 77B2752674026A1676EB9EC5FC6B158A4916C92864040>	Private RSA key used to generate the signature

Response

```
0320EX000097<008226CE8A1FD195DF87975DF65A810182700EABC7C73DBC75204
40C2C48230BCB8749B843A0B22FC2C16163288A182710B4BFFFBC870ABA67BBDD7
4F3DABB3A1FB1DB8BD69DE7D384C69167530DD706302509291AC60239CEC0EA577
4A372762A>
```

Fld	Format	Value	Description
1	4 A	0320	Message header (as defined by user).
2	2 A	EX	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	4 N	0097	Length of signature
5	97 B	<008226CE8A1FD195DF87975DF65A810182700EABC7C … 30DD706302509291AC60239CEC0EA5774A372762A>	Calculated signature

EW Command - Generate a signature (with variant LMK-encrypted RSA key held in user storage)

The EW command generates a signature over a message using an RSA private key encrypted under a variant LMK. In this example, the variant LMK-encrypted RSA private key is held in user storage at index 000, with the block size set to V(ariable) in security settings. *(NOTE: the ability to reference RSA keys in user storage is not available in payShield 9000 v2.2a or earlier.)*

Command

```
0310EW0101010009<616263646567686960>;990004K000
```

Fld	Format	Value	Description
1	4 A	0310	Message header (as defined by user).
2	2 A	EW	Command Code.
3	2 N	01	Hash identifier. (01 = SHA-1)
4	2 N	01	Signature identifier. (01 = RSA)
5	2 N	01	Pad mode identifier (01 = PKCS#1 v1.5)
6	4 N	0009	Data Length
7	9 B	<616263646567686960>	Message to be signed
8	1 A	;	Delimiter
9	2 N	99	Private key flag. (99 = key identified below.)
10	4 N	0004	Private key length
11	1 A + 3 H	K000	Index to RSA private key in user storage ("K" = the index flag; "000" is index of key in user storage).

Response

```
0310EX000064<418AFB0364BCD82C2240EAABFDBBA0F9C0DD84319005D8686BD77
ADF8ACA59C8513B86D76444B757E30B081B2D05F2A888354EEEEE134A6370FA528
F34C82163>
```

Fld	Format	Value	Description
1	4 A	0310	Message header (as defined by user).
2	2 A	EX	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	4 N	0064	Length of signature
5	64 B	<418AFB0364BCD82C2240E AABFDBBA0F9C0DD8431900 … B2D05F2A888354EEEEE134 A6370FA528F34C82163>	Calculated signature

EW Command - Generate a signature (with keyblock LMK-encrypted RSA key held in user storage)

The EW command generates a signature over a message using an RSA private key encrypted under a keyblock LMK. In this example, the keyblock LMK-encrypted RSA private key is held in user storage at index 022, with the block size set to V(ariable) in security settings. *(NOTE: the ability to reference RSA keys in user storage is not available in payShield 9000 v2.2a or earlier.)*

Command

```
0310EW0101010003<616263>;99FFFFSK022%02
```

Fld	Format	Value	Description
1	4 A	0310	Message header (as defined by user).
2	2 A	EW	Command Code.
3	2 N	01	Hash identifier. (01 = SHA-1)
4	2 N	01	Signature identifier. (01 = RSA)
5	2 N	01	Pad mode identifier (01 = PKCS#1 v1.5)
6	4 N	0003	Data Length
7	3 B	<616263>	Message to be signed
8	1 A	;	Delimiter
9	2 N	99	Private key flag. (99 = key identified below.)
10	4 N	FFFF	Private key length. (Always set to "FFFF" for keyblock LMKs.)
11	1 A + 3 H	SK022	Index to RSA private key in user storage ("S" identifies keyblock LMK scheme; "K" = the index flag; "022" is index of key in user storage. (Note: the index flag always has a value of 'K', irrespective of the value of the Index Flag used when the data was read into user storage using the LA command.)).
12	1A	%	Delimiter
13	2N	02	LMK identifier.

Response

```
0310EX000128<02658202FF77FE249356E9A4B2B43771A87A1B59518B64955A6AA
4C56DA268FF65521BA4C9A594D136354DA2F83040988AD3115224A29CF5CE2F8CF
084EA1E4ED7C3BC5C59C023F0CB59B53F5ECE58A133E2682B2BC1600749641EAC5
BDE729FAB66715DF7566C5CAD80E443DC5519A11690FB5B5BBC0BF984283286928
46856>
```

Fld	Format	Value	Description
1	4 A	0310	Message header (as defined by user).
2	2 A	EX	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	4 N	0128	Length of signature
5	128 B	<02658202FF77FE249356E 9A4B2B43771A87A1B59518 … 15DF7566C5CAD80E443DC5 519A11690FB5B5BBC0BF98 428328692846856>	Calculated signature

EY Command - Validate a signature (with variant LMK-encrypted RSA key provided in the command)

The EY command validates, using the RSA public key, a signature previously generated over a message using an RSA private key. In this example, the variant LMK-encrypted RSA private key is included in the command.

Command

```
0350EY0301010040<6F3291898D0488CB52478A84628596617CE7F92BB22724771
072F0885F823C5210AEDA2CAE0A6848>;0003<616263>;<60973C58><302F0228B
4FA9DC06844F408116C0B8EF7D1046593F73FB44F432E3732891C4E75F5C0EA07D
968D2FFB5E6250203010001><41555448454E2D44415441>
```

Fld	Format	Value	Description
1	4 A	0350	Message header (as defined by user).
2	2 A	EY	Command Code.
3	2 N	03	Hash identifier. (03 = ISO 10118-2)
4	2 N	01	Signature identifier. (01 = RSA)
5	2 N	01	Pad mode identifier (01 = PKCS#1 v1.5)
6	4 N	0040	Signature Length
7	40 B	<6F3291898D0488CB52478A84628596617CE7F92BB22724771072F0885F823C5210AEDA2CAE0A6848>	Signature to be validated
8	1 A	;	Delimiter
9	4 N	0003	Length of data in message for which the signature is to be validated.
10	3B	<616263>	Message whose signature is to be validated.
11	1 A	;	Delimiter
12	4 B	<60973C58>	MAC on the Public Key and Authentication Data
13	49 B	<302F0228B4FA9DC06844F408116C0B8EF7D1046593F73FB44F432E3732891C4E75F5C0EA07D968D2FFB5E6250203010001>	RSA Public Key
14	11 B	<41555448454E2D44415441>	Optional Authentication Data.

Response

```
0350EZ00
```

Fld	Format	Value	Description
1	4 A	0350	Message header (as defined by user).
2	2 A	EZ	Response Code.
3	2 A	00	Error Code. 00 = No error. Other codes would indicate the reason why the signature was not validated.

GO Command - Translate a PIN block from BDK to ZPK Encryption

The GO command performs a function analogous to the CA command described earlier, but is used for DUKPT terminals. It translates a PIN Block received from a DUKPT terminal into a PIN Block (encrypted under a ZPK) that can be passed into the payments network. The key used to encrypt the PIN is not provided to the payShield 9000: instead, it derives it from the BDK provided to it (which is identified to the host system in the KSN sent from the terminal) and the KSN itself. The command can also translate between different PIN Block formats.

In this example, the received PIN Block will be decrypted using a double-length TDES BDK and the transmitted PIN Block is encrypted using a double-length TDES ZPK. Both received and transmitted PIN Blocks use Thales format 01 (= ISO/ANSI Format 0).

The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
HDR4G0~U000595797DB29310FDF463ABB8396F45U16FAD09093F342EC35AE6049B
4F80834609FFFF01016E3658200007080C2A27DF4D6A4F0101345678912345
```

Fld	Format	Value	Description
1	4 A	HDR4	Message header (as defined by user).
2	2 A	G0	Command Code. (NOTE: the 2nd character is a zero.)
3	1 A	~	BDK Flag. ~ indicates that the supplied BDK is a Type 2 BDK.
4	1 A + 32 H	U000595797DB29310FDF463ABB8396F45	The Type 2 BDK (encrypted under LMK pair 28-29 variant 6) required to decrypt the PIN Block. U = Double-length TDES key scheme
5	1 A + 32 H	U16FAD09093F342EC35AE6049B4F80834	The ZPK (encrypted under LMK pair 06 07) to be used to re-encrypt the PIN Block. U = Double-length TDES key scheme
6	3 H	609	KSN Descriptor. 6 = BDK identifier length (in Hex chars.) 0 = Sub-key identifier length (in Hex chars.) 9 = Device identifier length (in Hex chars.)
7	20 H	FFFF01016E3658200007	KSN (Key Serial Number) FFFF02 = BDK identifier 016E36582 = Device identifier 00003 = Transaction Counter
8	16 H	080C2A27DF4D6A4F	Source PIN Block, encrypted using DUKPT
9	2 N	01	Source PIN Block format code. 01 = ISO 9564-1 & ANSI X9.8 format 0.
10	2 N	01	Output PIN Block format code. 01 = ISO 9564-1 & ANSI X9.8 format 0.
11	12 N	345678912345	Account Number. For output PIN Block format code = 01, the 12 right-most digits of the PAN excluding the check digit.

Response

HDR4G10004BE09A161870F9E8F01

Fld	Format	Value	Description
1	4 A	HDR4	Message header (as defined by user).
2	2 A	G1	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	2 N	04	PIN Length
5	16 H	BE09A161870F9E8F	Output PIN Block, encrypted under the ZPK.
6	2 N	01	Output PIN Block format code - as in the command, field 10. 01 = ANSI X9.8 Format 0.

GM Command – Hash a block of data

The GM command calculates a hash over a block of data of up to 32,000 Bytes.

The user has specified a header (with the length set to 4 characters in the host port settings), and a trailer.

Command

```
4000GM0100032<000000000000000000000000000000000000000000000000000000
000000000000><19> = 2EF96
```

Fld	Format	Value	Description
1	4 A	4000	Message header (as defined by user).
2	2 A	GM	Command Code.
3	2 N	01	Hash algorithm to be used. 01 =SHA-1.
4	5 N	00032	Length of message over which hash is to be calculated.
5	32 B	<00000000000000000000 00000000000000000000 00000000000000000000>	Message to be hashed.
6	1 C	<19>	Delimiter, indicating that there is a trailer for the message.
7	8 A	= 2EF96	Message trailer, defined by user. (Max length is 32 chars.)

Response

```
4000GN00<DE8A847BFF8C34>=<69B853A215E6EE775EF2EF9619> = 2EF96
```

Fld	Format	Value	Description
1	4 A	4000	Message header (as defined in the command).
2	2 A	GN	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	20 B	<DE8A847BFF8C34>=<69B8 53A215E6EE775EF2EF96>	Calculated hash. The length depends on the algorithm used.
5	1 C	<19>	Delimiter, indicating that there is a trailer for the message.
6	8 A	= 2EF96	Message trailer, as defined in the command.

JC Command - Translate a PIN Block from TPK to LMK Encryption.

This command takes a PIN block from a terminal encrypted using a TPK and returns an LMK-encrypted PIN. The LMK-encrypted PIN can be stored, or used as input to a number of commands which accept LMK-encrypted PINs (e.g. PIN mailers, or generate a PVV from an LMK-encrypted PIN).

The LMK-encryption of a PIN uses an algorithm involving the account number, such that the result will be different for two cardholders who have the same PIN.

In the example below, the TPK is single-length DES. The user has specified a header (with the length set to 4 characters in the host port settings) and a trailer.

Command

`HDR5JCC8784A7C991251031166E5FDD7BCFCEA01787296260268<19>=41781`

Fld	Format	Value	Description
1	4 A	`HDR5`	Message header (as defined by user).
2	2 A	`JC`	Command Code.
3	16 H	`C8784A7C99125103`	The TPK (encrypted under LMK pair 14-15 variant 0 or LMK pair 36-37, depending on PCI HSM compliance settings) under which the PIN block is currently encrypted.
4	16 H	`1166E5FDD7BCFCEA`	The source PIN Block, encrypted under the TPK.
5	2 N	`01`	Source PIN Block format code `01` = ISO 9564-1 & ANSI X9.8 format 0
6	12 N	`787296260268`	Account Number. For PIN Block format code = `01`, the 12 right-most digits of the PAN excluding the check digit.
7	1 C	`<19>`	End Message delimiter, to indicate that what follows is a message trailer.
8	6 A	`=41781`	Message trailer, as provided by the user.

Response

`HDR5JD0041781<19>=41781`

Fld	Format	Value	Description
1	4 A	`HDR5`	Message header (as defined by user).
2	2 A	`JD`	Response Code.
3	2 A	`00`	Error Code. `00` = No error.
4	5 N	`41781`	Output PIN encrypted under LMK pair 02-03. Notes: ➢ The length of the PIN is defined by the payShield 9000 security settings. ➢ The LMK encrypted PIN uses an algorithm involving the account number.
5	1 C	`<19>`	End Message delimiter, to indicate that what follows is a message trailer.
6	6 A	`=41781`	Message trailer, as provided in the command.

JE Command - Translate a PIN Block from ZPK to LMK Encryption.

The JE command performs a very similar function to the JC command described above, but in the case of JE the received PIN Block is coming from the payments network and is encrypted using a ZPK.

In the example below, the ZPK is a double-length TDES key. The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
HDR5JEU16FAD09093F342EC35AE6049B4F80834BE09A161870F9E8F01345678912
345
```

Fld	Format	Value	Description
1	4 A	HDR5	Message header (as defined by user).
2	2 A	JE	Command Code.
3	1 A + 32 H	U16FAD09093F342EC35AE6 049B4F80834	The ZPK (encrypted under LMK pair 06-07) under which the PIN block is currently encrypted.
4	16 H	BE09A161870F9E8F	The source PIN Block, encrypted under the ZPK.
5	2 N	01	Source PIN Block format code 01 = ISO 9564-1 & ANSI X9.8 format 0
6	12 N	345678912345	Account Number. For PIN Block format code = 01, the 12 right-most digits of the PAN excluding the check digit.

Response

```
HDR5JF0081011
```

Fld	Format	Value	Description
1	4A	HDR5	Message header (as defined by user).
2	2A	JF	Response Code.
3	2A	00	Error Code. 00 = No error.
4	5N	81011	Output PIN encrypted under LMK pair 02-03. Notes: ➢ The length of the PIN is defined by the payShield 9000 security settings. ➢ The LMK encrypted PIN uses an algorithm involving the account number.

JE Command – Translate a PIN from ZPK to LMK encryption (using a ZPK and PIN Block held in user storage)

In this example, both the LMK-encrypted PIN and the LMK-encrypted ZPK are held in user storage and are identified in the command using their user storage indexes. The ZPK is a double-length TDES key.

The LMK is of the variant TDES type.

Command

0260JEUK012K20001123456789012

Fld	Format	Value	Description
1	4 A	0269	Message header (as defined by user).
2	2 A	JE	Command Code.
3	2 A + 3 H	UK012	Reference to the ZPK in user storage. The 'U' identifies the key scheme as double-length TDES using a variant LMK. 'K' is the index flag. '012' is the index for the ZPK in user storage.
4	1 A + 3 H	K200	Reference to the PIN Block held in user storage. 'K' is the index flag, and '200' is the index in user storage where the PIN Block is stored.
5	2 N	01	PIN Block format code
6	12 N	123456789012	The 12 right-most digits of the PAN, excluding the check digit.

Response

0260JF0082050

Fld	Format	Value	Description
1	4 A	0260	Message header (as defined by user).
2	2 A	JF	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	5 N	82050	PIN encrypted under the LMK

JG Command - Translate a PIN from LMK to ZPK Encryption.

The JG command is the converse of the JE command described above. It takes an LMK-encrypted PIN and translates it into a PIN Block encrypted under a ZPK for transmission into the payments network.

In the example below, the ZPK is a single-length DES key. The user has specified a header (with the length set to 4 characters in the host port settings) and a trailer.

Command

HDR5 JG95FE090036A200C1017872962602684178 1<19>=FC96

Fld	Format	Value	Description
1	4 A	HDR5	Message header (as defined by user).
2	2 A	JG	Command Code.
3	16 H	95FE090036A200C1	The ZPK that the PIN Block is to be encrypted under. The ZPK is single-length DES and is encrypted under LMK pair 06-07 variant 0.
4	2 N	01	The PIN Block format code for the ZPK-encrypted PIN. 01 = ISO 9564-1 & ANSI X9.8 format 0
5	12 N	78729626026841781	Account Number. For PIN Block format code = 01, the 12 right-most digits of the PAN excluding the check digit.
6	5 N	41781	The LMK-encrypted PIN, encrypted under LMK pair 02-03. Notes: ➢ The length of the PIN is defined by the payShield 9000 security settings. ➢ The LMK encrypted PIN uses an algorithm involving the account number.
7	1 C	<19>	End Message delimiter, to indicate that what follows is a message trailer.
8	5 A	=FC96	Message trailer, as provided by the user.

Response

HDR5JH00B6720B1B0DBFFC96<19>=FC96

Fld	Format	Value	Description
1	4 A	HDR5	Message header (as defined by user).
2	2 A	JH	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	16 H	B6720B1B0DBFFC96	PIN Block, encrypted under the ZPK.
5	1 C	<19>	End Message delimiter, to indicate that what follows is a message trailer.
6	5 A	=FC96	Message trailer, as provided in the command.

JG Command – Translate a PIN from LMK to ZPK encryption (using a ZPK held in user storage)

In this example, the LMK-encrypted ZPK is held in user storage and is identified in the command using its user storage indexes. The ZPK is a double-length TDES key. (Because the user storage length was set to Single, the key was loaded using the LA command into 2 contiguous blocks.)

The LMK is of the variant TDES type.

Command

0260 JGUK0120112345678901282050

Fld	Format	Value	Description
1	4 A	0269	Message header (as defined by user).
2	2 A	JG	Command Code.
3	2 A + 3 H	UK012	Reference to the ZPK in user storage. The 'U' identifies the key scheme as double-length TDES using a variant LMK. 'K' is the index flag. '012' is the index for the ZPK in user storage.
4	2 N	01	PIN Block format code
5	12 N	123456789012	The 12 right-most digits of the PAN, excluding the check digit.
6	5 N	82050	PIN encrypted under the LMK

Response

0260JH0028D2BF543AC94665

Fld	Format	Value	Description
1	4 A	0260	Message header (as defined by user).
2	2 A	JF	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	16 H	28D2BF543AC94665	PIN Block encrypted under the ZPK

LA Command - Load Data to User Storage (double-length TDES key encrypted under a variant LMK).

The LA command is used to load multiple blocks of data into the payShield 9000's internal user storage area. This process is described in this Application Note.

The data can be in blocks of 16, 32, or 48 hexadecimal digits (8, 16, or 24 Bytes) or (after v2.2a) of variable length – as specified in the security settings. Each block is identified by an index of 0-4,095 (0-FFF in hexadecimal).

In this example the data block size has been set to "Single" in the CS console command (or HSM Manager Edit/General Settings dialogue box). We are storing two 8-byte blocks to indexes 0FE and 0FF representing a double-length TDES ZMK key. The user has specified a header (with the length set to 4 characters in the host port settings) and a trailer.

Command

```
HDRALAK0000292385025801691228682054947200919<19>=01
```

Fld	Format	Value	Description
1	4 A	HDRA	Message header (as defined by user).
2	2 A	LA	Command Code.
3	1 A	K	Index Flag
4	3 H	0FE	Index for location where first data block in the command is to be stored.
5	2 H	02	Number of data blocks included in the command
6	16 H	9238502580169122	Data Block 1. (The data block size has been set to "Single" in the *CS* console command or HSM Manager *Edit/General Settings* dialogue box.)
7	16 H	8682054947200919	Data Block 2. (The data block size has been set to "Single" in the *CS* console command or HSM Manager *Edit/General Settings* dialogue box.)
8	1 C	<19>	End Message delimiter, to indicate that what follows is a message trailer.
9	4 A	=01	Message trailer, as provided by the user.

Response

```
HDRALB00<19>=01
```

Fld	Format	Value	Description
1	4 A	HDRA	Message header (as defined by user).
2	2 A	LB	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	1 C	<19>	End Message delimiter, to indicate that what follows is a message trailer.
5	4 A	=01	Message trailer, as provided in the command.

LA Command - Load Data to User Storage (RSA private key encrypted under a TDES variant LMK).

In this example the data block size has been set to "Variable" in the CS console command (or HSM Manager Edit/General Settings dialogue box): this setting is not available in payShield 9000 v2.2a or earlier. We are storing a variant LMK-encrypted RSA private key consisting of 176 bytes of binary data.

Command

```
0000LABK0000176<813C82DB56E9AEA2A4AFC0B068259553DF18C32AFCA60F4983
3F52CFC0E6FC70287794AEE01F43F96B91B0492229367B6C9DDC2715CD668F9488
0D0AC0C4E5A0B22C8DAF12E2DA2F9BF8F475959D64FFCF80F03F86DAF297B92A2F
1E0CE1CF629564EADB3B5689A0FAE636B9B6E27E652186A45BC49CB13307281F5B
3A63FBA315047071CDDBE15247E278120C467481CF99F4EE09626E85613B1994B8
230FED7F4C04B8BC9205A6CFB285B1DBA22D24>
```

Fld	Format	Value	Description
1	4 A	0000	Message header (as defined by user).
2	2 A	LA	Command Code.
3	1A	B	Index Flag (B = Binary).
4	3 H	000	Index for location where the data block is to be stored. Because this in the range 000-07F, up to 1,000 bytes can be stored.
5	4N	0176	Total length of data, in bytes.
6	176B	<813C82DB56E9AEA2A4AFC0B068259553DF18C32AFCA … 994B8230FED7F4C04B8BC9205A6CFB285B1DBA22D24>	RSA Private key encrypted under the variant LMK.

Response

```
0000LB00
```

Fld	Format	Value	Description
1	4 A	0000	Message header (as defined by user).
2	2 A	LB	Response Code.
3	2 A	00	Error Code. 00 = No error.

LA Command - Load Data to User Storage (RSA private key encrypted under a TDES keyblock LMK).

In this example the data block size has been set to "Variable" in the CS console command (or HSM Manager Edit/General Settings dialogue box): this setting is not available in payShield 9000 v2.2a or earlier. We are storing an RSA private key consisting of 336 bytes of binary data held with a 376-byte keyblock.

Command


```
0000LABK02203760037603RN00N02020005TPB0B4vzoOWb<F343F5C367CB557BC2
17195EBFD4821E91E70D05CADF74C2E9F90F4E4184B9D8827F03CB337A0873787F
00D27FED0D1CF71AF4391DE2E4101E47D602BB5D5C3E91E54BBE034F19A4AF3562
766AC607940FE58F66EEFDE42D1D904C1510B1BB6323DA350517EFA647215A4224
874F24C6A1A4A7E4FEA6DB93640AABA4B7A3F2E7923C21526A4C2B69FF254F4C6D
F633103475404CF90A8FC2C6ADF4187FBFC1414D79575275353751B4E1777CE093
347A128AB30A959BE8827433E522147C8129E66BC59BD4466E08B9BCBE136E6FDB
00EB6F12B81957AA37544800D85CAFE630894302E92F84ADD2C9A22F302A6CD772
A47EBF9BEBF82C4718321100D73A66991277309CD3D37D6377180336BF9F1FE813
03A6C33EBD1B29A9A4530DDD54D8592D288397BBA7F06AFA80AE6E28FA0788463B
328D9E6FEC8CFFCD8BAE2CE2E904F09E3AD2CFCE4B045CEC4D2C23061455>99653
B1A
```


Fld	Format	Value	Description
1	4 A	0000	Message header (as defined by user).
2	2 A	LA	Command Code.
3	1A	B	Index Flag (B = Binary).
5	3 H	022	Index for location where the data block is to be stored. Because this in the range 000-07F, up to 1,000 bytes can be stored.
5	4N	0376	Total length of data, in bytes.
6.1	1N	0	(Keyblock Header) Version ID
6.2	4N	0376	(Keyblock Header) Total length of key block
6.3	2H	03	(Keyblock Header) Key Usage (03 = RSA Private Key)
6.4	1A	R	(Keyblock Header) Algorithm (R = RSA)
6.5	1A	N	(Keyblock Header) Mode of Use (N = No special restrictions)
6.6	2N	00	(Keyblock Header) Key Version No.
6.7	1A	N	(Keyblock Header) Exportability (N = No exportability)
6.8	2N	02	(Keyblock Header) Number of optional header blocks
6.9	2N	02	(Keyblock Header) LMK ID.
6.10	2A	00	(Optional Keyblock Header 1) Block Type (00 = Key Status)
6.11	2H	05	(Optional Keyblock Header 1) Block Length
6.12	1A	L	(Optional Keyblock Header 1) Key Status (L = Live)
6.13	2A	PB	(Optional Keyblock Header 2) Block Type (PB = Padding Block)

Fld	Format	Value	Description
6.14	2H	0B	(Optional Keyblock Header 2) Block Length
6.15	7A	4vzoOWb	(Optional Keyblock Header 2) Padding text
6.16	376B	<F343F5C367CB557BC2171 95EBFD4821E91E70D05CAD … 904F09E3AD2CFCE4B045CE C4D2C23061455>	(Keyblock data) RSA Private key encrypted under the keyblock LMK
6.17	8A	99653B1A	Keyblock MAC

In this example, Field 6, the data field in the LA command, has been subdivided to explain the keyblock structure.

Response

0000LB00

Fld	Format	Value	Description
1	4 A	0000	Message header (as defined by user).
2	2 A	LB	Response Code.
3	2 A	00	Error Code. 00 = No error.

LE Command - Read Data from User Storage (single/double/triple block size setting).

With the LE command, data previously written to the payShield 9000's internal user storage using the LA command can be retrieved.

In this example the data block size has been set to "Single" in the CS console command (or HSM Manager Edit/General Settings dialogue box). We are retrieving two 8-byte blocks from indexes 0FE and 0FF representing a double-length TDES ZMK key. The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
HDRBLEK0FE02<19>=09199238502580169122
```

Fld	Format	Value	Description
1	4 A	HDRB	Message header (as defined by user).
2	2 A	LE	Command Code.
3	1 A	K	Index Flag
4	3 H	0FE	Index for location where first data block is stored.
5	2 H	02	Number of data blocks to be retrieved
6	1 C	<19>	End Message delimiter, to indicate that what follows is a message trailer.
7	21 A	=09199238502580169122	Message trailer, as provided by the user.

Response

```
HDRBLF00868205494720091992385025801691 22<19>=0919 9238502580169122
```

Fld	Format	Value	Description
1	4 A	HDRB	Message header (as defined by user).
2	2 A	LF	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	16 H	8682054947200919	Data Block 1. (The data block size has been set to "Single" in the *CS* console command or HSM Manager *Edit/General Settings* dialogue box.)
5	16 H	9238502580169122	Data Block 2. (The data block size has been set to "Single" in the *CS* console command or HSM Manager *Edit/General Settings* dialogue box.)
6	1 C	<19>	End Message delimiter, to indicate that what follows is a message trailer.
7	21 A	=09199238502580169122	Message trailer, as provided in the command.

LE Command - Read Data from User Storage (variable block size setting).

In this example the data block size has been set to "Variable" in the CS console command (or HSM Manager Edit/General Settings dialogue box) – this capability is not available in payShield 9000 version 2.2a or earlier. When this option is selected, a single data block is retrieved.

We are retrieving an RSA Private key encrypted using a keyblock LMK. The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
0000LEK0FE02<19>=09199238502580169122
```

Fld	Format	Value	Description
1	4 A	0000	Message header (as defined by user).
2	2 A	LE	Command Code.
3	1 A	K	Index Flag (Note: this field always has a value of 'K', irrespective of the value of the Index Flag used when the data was read into user storage using the LA command.)
4	3 H	022	Index for location where first data block is stored.

Response

```
0000LF00B03760037603RN00N02020005TPB0B4vzoOWb<F343F5C367CB557BC217
195EBFD4821E91E70D05CADF74C2E9F90F4E4184B9D8827F03CB337A0873787F00
D27FED0D1CF71AF4391DE2E4101E47D602BB5D5C3E91E54BBE034F19A4AF356276
6AC607940FE58F66EEFDE42D1D904C1510B1BB6323DA350517EFA647215A422487
4F24C6A1A4A7E4FEA6DB93640AABA4B7A3F2E7923C21526A4C2B69FF254F4C6DF6
33103475404CF90A8FC2C6ADF4187FBFC1414D79575275353751B4E1777CE09334
7A128AB30A959BE8827433E522147C8129E66BC59BD4466E08B9BCBE136E6FDB00
EB6F12B81957AA37544800D85CAFE630894302E92F84ADD2C9A22F302A6CD772A4
7EBF9BEBF82C4718321100D73A66991277309CD3D37D6377180336BF9F1FE81303
A6C33EBD1B29A9A4530DDD54D8592D288397BBA7F06AFA80AE6E28FA0788463B32
8D9E6FEC8CFFCD8BAE2CE2E904F09E3AD2CFCE4B045CEC4D2C23061455>99653B1
A
```

Fld	Format	Value	Description
1	4 A	0000	Message header (as defined by user).
2	2 A	LF	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	1A	B	Data type (B = Binary).
5	4N	0376	Total length of data, in bytes.
6	376B	0037603RN00N02020005TPB0B4vzoOWb<F343F5C367CB557BC217195EBFD4821E9 … FCE4B045CEC4D2C23061455>99653B1A	Keyblock, including RSA Private key encrypted under LMK

MO Command – encrypt a block of data (using a keyblock LMK-included in the command).

The MO command is used for encryption of general messages. The encryption key may be provided as one of the command's parameters, as in this example. It is a triple-length TDES key encrypted using a keyblock LMK. The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
0000M00000FFFS1009621AB00N00021E96DD97D8B0F388B525E93F522952F7A394
F29D6E8C20D8F2775DF5654BDCAFCA96DD6F427AA8630040<8D56A1282943E0974
23A6FA8A951BD127D94F16088FEE8DD1BFC506B22CCE4F022BDB3F63A2E6C531F2
9EFB59130274827CDCE094BD84295B68EE4227B610738>
```

Fld	Format	Value	Description
1	4 A	0000	Message header (as defined by user).
2	2 A	M0	Command Code.
3	2 N	00	Mode flag. (00 = ECB)
4	1 N	0	Input format (0 = Binary)
5	1 N	0	Output format (0 = Binary)
6	3 H	FFF	Key type. (Always set to FFF when using a keyblock LMK.)
7	1 A + 48 H	S1009621AB00N00021E96DD97D8B0F388B525E93F522952F7A394F29D6E8C20D8F2775DF5654BDCAFCA96DD6F427AA863	Key to be used to encrypt the message. The 'S' at the start of the field is the key scheme and identifies that the key is encrypted using a keyblock LMK.
8	4 H	0040	Length of message to be encrypted (i.e. 64 in decimal)
9	64 B	<8D56A1282943E097423A6FA8A951BD127D94F16088F … 59130274827CDCE094BD84295B68EE4227B610738>	Message to be encrypted.

Response

```
0000M1000040<82DA2F20A0121F58EA006E47AB6321BD09A592AC3C11032069E34
C1011261F4128BD73CF3BDBE5C91515FF65928FB812380F58B722DA1149A464E77
679CD60F0>
```

Fld	Format	Value	Description
1	4 A	0000	Message header (as defined by user).
2	2 A	M1	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	4 H	0040	Length of encrypted message (i.e. 64 in decimal)
5		<82DA2F20A0121F58EA006E47AB6321BD09A592AC3C1 … 5928FB812380F58B722DA1149A464E77679CD60F0>	Encrypted message

MO Command – encrypt a block of data (using a keyblock LMK-encrypted key held in user storage).

The MO command is used for encryption of general messages. The encryption key may be provided as one of the command's parameters or, as in this example, the command may contain a reference to the key held in the user storage area.

In this example the user storage data block size has been set to "Variable" in the CS console command (or HSM Manager Edit/General Settings dialogue box) – this capability is not available in payShield 9000 version 2.2a or earlier. When this option is selected, a single data block is retrieved.

We are retrieving from user storage a TDES encryption key encrypted using a keyblock LMK. The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
0000M00000FFFSK0110040<8D56A1282943E097423A6FA8A951BD127D94F16088F
EE8DD1BFC506B22CCE4F022BDB3F63A2E6C531F29EFB59130274827CDCE094BD84
295B68EE4227B610738>
```

Fld	Format	Value	Description
1	4 A	0000	Message header (as defined by user).
2	2 A	M0	Command Code.
3	2 N	00	Mode flag. (00 = ECB)
4	1 N	0	Input format (0 = Binary)
5	1 N	0	Output format (0 = Binary)
6	3 H	FFF	Key type. (Always set to FFF when using a keyblock LMK.)
7	2 A + 3 H	SK011	Index to key in user storage. ('S' identifies key scheme as keyblock LMK; 'K' is the index flag; '011' is the index to the key in user storage. (Note: the index flag always has a value of 'K', irrespective of the value of the Index Flag used when the data was read into user storage using the LA command.))
8	4 H	0040	Length of message to be encrypted (i.e. 64 in decimal)
9	64 B	<8D56A1282943E097423A6FA8A951BD127D94F16088F … 59130274827CDCE094BD84295B68EE4227B610738>	Message to be encrypted.

Response

0000M1000040<82DA2F20A0121F58EA006E47AB6321BD09A592AC3C11032069E34C1011261F4128BD73CF3BDBE5C91515FF65928FB812380F58B722DA1149A464E77679CD60F0>

Fld	Format	Value	Description
1	4 A	0000	Message header (as defined by user).
2	2 A	M1	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	4 H	0040	Length of encrypted message (i.e. 64 in decimal)
5		<82DA2F20A0121F58EA006E47AB6321BD09A592AC3C1 … 5928FB812380F58B722DA1149A464E77679CD60F0>	Encrypted message

M2 Command - Decrypt Data

The M2 command is used to decrypt data which has been encrypted using a DES or TDES key.

In the example below, the data has been encrypted by a DUKPT terminal. The BDK (identified in the KSN returned by the terminal) is a double-length TDES BDK. The data encryption key is derived by the payShield 9000 using the BDK supplied by the host system and the KSN provided by the terminal.

The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
HDR3M20102609U1B42F9A78E0670174839434890D0D58F609FFFF02016E3658200
0030000000000000000020<95E55D4EC345B87E7878C9CCFA0099287DB8908D21
FEA8E0CB9A2BAF20C2FB94>
```

Fld	Format	Value	Description
1	4 A	HDR3	Message header (as defined by user).
2	2 A	M2	Command Code.
3	2 N	01	Mode Flag. 01 = CBC
4	1 N	0	Input Format Flag. 0 = Binary
5	1 N	2	Output Format Flag. 2 = Text
6	3 H	609	Key Type. 609 = Type 2 BDK, encrypted under Variant LMK pair 28-29, variant 6.
7	1 A + 32 H	U1B42F9A78E06701748394 34890D0D58F	Key that data is encrypted under. U = Double-length TDES key scheme The remainder of the field is the Type 2 BDK encryption key encrypted under the LMK.
8	3 H	609	KSN Descriptor. 6 = BDK identifier length (in Hex chars.) 0 = Sub-key identifier length (in Hex chars.) 9 = Device identifier length (in Hex chars.)
9	20 H	FFFF02016E3658200003	KSN (Key Serial Number) FFFF02 = BDK identifier 016E36582 = Device identifier 00003 = Transaction Counter
10	16 H	0000000000000000	IV (Initial Value)
11	4 H	0020	Message Length, i.e. length (in hexadecimal) of message to be decrypted, in bytes.
12	32 Bytes	<95E55D4EC345B87E7878C 9CCFA0099287DB8908D21F EA8E0CB9A2BAF20C2FB94>	Message to be decrypted.

Response

```
HDR3M300CB9A2BAF20C2FB9400200123456789123456<F04C6352435B49FDD4E16
1769857233D>
```

Fld	Format	Value	Description
1	4 A	HDR3	Message header (as defined by user).
2	2 A	M3	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	16 H	CB9A2BAF20C2FB94	Output Initial Value (IV)
5	4 H	0020	Message Length, i.e. length (in hexadecimal) of decrypted message, in bytes.
6	32 Bytes	0123456789123456<F04C6 352435B49FDD4E16176985 7233D>	Decrypted message.

M4 Command – Translate a Data Block

The M4 command is used to take a data block encrypted under a source key and output the data block encrypted under a destination key.

In this example, the user has specified that no headers or trailers will be used.

Command

M400000000A06FA0EF7DAF5B67300A0053474C2A7782190018<36B26099B626AA3C8450764D58B885E30A60400564EC400A>

Fld	Format	Value	Description
1	2 A	M4	Command Code.
2	2 N	00	Source Mode Flag. 00 = ECB (does not require an IV)
3	2 N	00	Destination Mode Flag. 00 = ECB (does not require an IV)
4	1 N	0	Input Format Flag. 0 = Binary
5	1 N	0	Output Format Flag. 0 = Binary
6	3 H	00A	Source Key Type 00A = ZEK
7	16 H	06FA0EF7DAF5B673	Source key (single-length DES)
8	3 H	00A	Destination Key Type 00A = ZEK
9	16 H	0053474C2A778219	Destination key (single-length DES)
10	4 H	0018	Message length (i.e. 24 in decimal)
11	24 B	<36B26099B626AA3C8450764D58B885E30A60400564EC400A>	The source key-encrypted message that is to be encrypted under the destination key.

Response

M5000018<656C3E1F122823EA8F3EC458D49AC9502AA7DF8BE6CB388B>

Fld	Format	Value	Description
1	2 A	M5	Response Code.
2	2 A	00	Error Code. 00 = No error.
3	4 N	0018	Message length (i.e. 24 in decimal)
4	24 B	<656C3E1F122823EA8F3EC458D49AC9502AA7DF8BE6CB388B>	The message encrypted under the destination key

M6 Command – Generate a MAC

The M6 command calculates a MAC on a block of data, which may be one of a sequence of data blocks.

In this example, the user has specified that a header but no trailer will be used.

Command

```
0000M60101000832F6643A4D6E277C003029AA7319C23CF0BBA09FDA87A56066FB
83A113731EF085BB
```

Fld	Format	Value	Description
1	4 A	0000	Header (as provided by the user).
2	2 A	M6	Command Code.
3	1 N	0	Mode Flag. 0 = This is the one and only block of data that the MAC is to be calculated over.
4	1 N	1	Input Format Flag. 1 = Hex-encoded Binary
5	1 N	0	MAC size. 0 = 8 hex digits.
6	1 N	1	MAC algorithm. 1 = ISO 9797 MAC algorithm 1 (= ANSI X9.9 when used with a single-length key) (DES only)
7	1 N	0	Padding method. 0 = No padding.
8	3 H	008	Key type. 008 = ZAK
9	16 H	32F6643A4D6E277C	Key to be used in calculating the MAC. (This is a single-length DES key.)
10	4 H	0030	Message length (i.e. 38 in decimal).
11	48 H	29AA7319C23CF0BBA09FDA87A56066FB83A113731EF085BB	Message that the MAC is to be calculated over.

Response

```
0000M70022C7A93A
```

Fld	Format	Value	Description
1	4 A	0000	Message header (as defined by user).
2	2 A	M7	Response Code.
3	2 A	00	Error Code. 00 = No error.
4	8 H	22C7A93A	The calculated MAC.

M8 Command – Verify a MAC

The M8 command verifies a MAC that has previously been calculated on a block of data, which may be one of a sequence of data blocks – for example by using the M6 command.

In this example, the user has specified that a header but no trailer will be used.

Command

```
0000M80101000812A9D314EA1CBA11003096220688795FD5E01372311E6DBBF4BA
B24573A7D492BD19029FBEBF
```

Fld	Format	Value	Description
1	4 A	0000	Header (as provided by the user).
2	2 A	M8	Command Code.
3	1 N	0	Mode Flag. 0 = This is the one and only block of data that the MAC is to be calculated over.
4	1 N	1	Input Format Flag. 1 = Hex-encoded Binary
5	1 N	0	MAC size. 0 = 8 hex digits.
6	1 N	1	MAC algorithm. 1 = ISO 9797 MAC algorithm 1 (= ANSI X9.9 when used with a single-length key) (DES only)
7	1 N	0	Padding method. 0 = No padding.
8	3 H	008	Key type. 008 = ZAK
9	16 H	12A9D314EA1CBA11	Key to be used in calculating the MAC. (This is a single-length DES key.)
10	4 H	0030	Message length (i.e. 48 in decimal).
11	48 H	96220688795FD5E01372311E6DBBF4BAB24573A7D492BD19	Message that the MAC is to be calculated over.
12	8 H	029FBEBF	The MAC to be verified

Response

```
0000M900
```

Fld	Format	Value	Description
1	4 A	0000	Message header (as defined by user).
2	2 A	M9	Response Code.
3	2 A	00	Error Code. 00 = No error. Other codes would give the reason for a failure of the MAC verification.

MY Command – Verify and Translate a MAC (first data block)

The MY command is used to verify a MAC previously generated (e.g. using the M6 host command). If the verification is successful, the command generates a new MAC on the same message but using a different TAK (Terminal Authentication Key) or ZAK (Zone Authentication Key).

The data block is the first of a multi-block series.

The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
0000MY11010003B2B6DC382E5729BB010003BC0738B386A539500010725B79AD1A
ACC2A0
```

Fld	Format	Value	Description
1	4 A	0000	Message header (as defined by user).
2	2 A	MY	Command Code.
3	1 N	1	Mode Flag. 1 = First block of a multi-block message.
4	1 N	1	Input Format Flag. 1 = Hex-encoded Binary
5	1 N	0	Source MAC size. 0 = 8 Hex digits
6	1 N	1	Source MAC algorithm. 1 = ISO 9797 MAC algorithm 1 (= ANSI X9.9 when used with a single-length key) (DES only)
7	1 N	0	Source Padding Method. 0 = No padding.
8	3 H	003	Source Key Type. 003 = TAK (Terminal Authentication Key).
9	16 H	B2B6DC382E5729BB	Source Key. (This is a single-length DES key.)
10	1 N	0	Destination MAC size. 0 = 8 Hex digits
11	1 N	1	Destination MAC algorithm. 1 = ISO 9797 MAC algorithm 1 (= ANSI X9.9 when used with a single-length key) (DES only)
12	1 N	0	Destination Padding Method. 0 = No padding.
13	3 H	003	Destination Key Type. 003 = TAK (Terminal Authentication Key).
14	16 H	BC0738B386A53950	Destination Key. (This is a single-length DES key.)
15	4 H	0010	The length of the following message field (i.e. 16 decimal).
16	16 H	725B79AD1AACC2A0	The message over which the MAC is to be verified and re-calculated.

Response

0000MZ00A80D11486AF05185F58B6D4FDD7135A6

Fld	Format	Value	Description
1	4 A	0000	Message header (as defined by user).
2	2 A	MZ	Response Code.
3	2 A	00	Error Code. 00 = No error. Other codes would give reason for verification failure.
4	16 H	A80D11486AF05185	Source Initial Value (IV) – for input to the next data block.
5	16 H	F58B6D4FDD7135A6	Output Initial Value (IV) – for input to the next data block.

MY Command – Verify and Translate a MAC (middle data block)

The MY command is used to verify a MAC previously generated (e.g. using the M6 host command). If the verification is successful, the command generates a new MAC on the same message but using a different TAK (Terminal Authentication Key) or ZAK (Zone Authentication Key).

The data block is the second of a multi-block series.

The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
0001MY21010003B2B6DC382E5729BB010003BC0738B386A53950A80D11486AF051
85F58B6D4FDD7135A600102124056E1FA1BC46
```

Fld	Format	Value	Description
1	4 A	0001	Message header (as defined by user).
2	2 A	MY	Command Code.
3	1 N	2	Mode Flag. 2 = Middle block of a multi-block message.
4	1 N	1	Input Format Flag. 1 = Hex-encoded Binary
5	1 N	0	Source MAC size. 0 = 8 Hex digits
6	1 N	1	Source MAC algorithm. 1 = ISO 9797 MAC algorithm 1 (= ANSI X9.9 when used with a single-length key) (DES only)
7	1 N	0	Source Padding Method. 0 = No padding.
8	3 H	003	Source Key Type. 003 = TAK (Terminal Authentication Key).
9	16 H	B2B6DC382E5729BB	Source Key. (This is a single-length DES key.)
10	1 N	0	Destination MAC size. 0 = 8 Hex digits
11	1 N	1	Destination MAC algorithm. 1 = ISO 9797 MAC algorithm 1 (= ANSI X9.9 when used with a single-length key) (DES only)
12	1 N	0	Destination Padding Method. 0 = No padding.
13	3 H	003	Destination Key Type. 003 = TAK (Terminal Authentication Key).
14	16 H	BC0738B386A53950	Destination Key. (This is a single-length DES key.)
15	16 H	A80D11486AF05185	Source IV (provided in output from preceding data block).
16	16 H	F58B6D4FDD7135A6	Destination IV (provided in output from preceding data block).
17	4 H	0010	The length of the following message field (i.e. 16 decimal).
18	16 H	2124056E1FA1BC46	The message over which the MAC is to be verified and re-calculated.

Response

0001MZ00D89E397EB1841EEBFA4664E582BF6356

Fld	Format	Value	Description
1	4 A	0001	Message header (as defined by user).
2	2 A	MZ	Response Code.
3	2 A	00	Error Code. 00 = No error. Other codes would give reason for verification failure.
4	16 H	D89E397EB1841EEB	Source Initial Value (IV.
5	16 H	FA4664E582BF6356	Output Initial Value (IV) – for input to the next data block.

MY Command – Verify and Translate a MAC (last data block)

The MY command is used to verify a MAC previously generated (e.g. using the M6 host command). If the verification is successful, the command generates a new MAC on the same message but using a different TAK (Terminal Authentication Key) or ZAK (Zone Authentication Key).

The data block is the third and last of a multi-block series.

The user has specified a header (with the length set to 4 characters in the host port settings), but no trailer.

Command

```
0002MY31010003B2B6DC382E5729BB010003BC0738B386A53950D89E397EB1841E
EBFA4664E582BF63560010308AF466AB612CB8EFEE8D5E
```

Fld	Format	Value	Description
1	4 A	0002	Message header (as defined by user).
2	2 A	MY	Command Code.
3	1 N	3	Mode Flag. 3 = Last block of a multi-block message.
4	1 N	1	Input Format Flag. 1 = Hex-encoded Binary
5	1 N	0	Source MAC size. 0 = 8 Hex digits
6	1 N	1	Source MAC algorithm. 1 = ISO 9797 MAC algorithm 1 (= ANSI X9.9 when used with a single-length key) (DES only)
7	1 N	0	Source Padding Method. 0 = No padding.
8	3 H	003	Source Key Type. 003 = TAK (Terminal Authentication Key).
9	16 H	B2B6DC382E5729BB	Source Key. (This is a single-length DES key.)
10	1 N	0	Destination MAC size. 0 = 8 Hex digits
11	1 N	1	Destination MAC algorithm. 1 = ISO 9797 MAC algorithm 1 (= ANSI X9.9 when used with a single-length key) (DES only)
12	1 N	0	Destination Padding Method. 0 = No padding.
13	3 H	003	Destination Key Type. 003 = TAK (Terminal Authentication Key).
14	16 H	BC0738B386A53950	Destination Key. (This is a single-length DES key.)
15	16 H	D89E397EB1841EEB	Source IV (provided in output from preceding data block).
16	16 H	FA4664E582BF6356	Destination IV (provided in output from preceding data block).
17	4 H	0010	The length of the following message field (i.e. 16 decimal).
18	16 H	308AF466AB612CB8	The message over which the MAC is to be verified and re-calculated.
19	8 H	EFEE8D5E	The source MAC to be verified.

Response

0002MZ0086296C9A

Fld	Format	Value	Description
1	4 A	0002	Message header (as defined by user).
2	2 A	MZ	Response Code.
3	2 A	00	Error Code. 00 = No error. Other codes would give reason for verification failure.
4	8 H	86296C9A	Destination MAC, generated using the destination key.

NG Command - Decrypt PIN from LMK-encryption to clear

The command is used when printing PIN mailers. It converts an LMK-encrypted PIN to cleartext. LMK encryption of the PIN uses an algorithm which involves the account number.

When the cleartext PIN is returned, the account number is returned in the form of a random reference number, such that PIN and account number do not appear together in the clear.

The command is available only:

- If enabled by the security setting "Select clear PINs?" (CS Console command) or "Enable clear PINs?" (HSM Manager Initial Settings).
- If the command is authorized.

Command

`HDR6NG34567891234581011`

Fld	Format	Value	Description
1	4 A	`HDR6`	Message header (as defined by user).
2	2 A	`NG`	Command Code.
3	12 N	`345678912345`	Account Number.
4	5 N	`81011`	PIN encrypted under LMK pair 02-03. Notes: ➢ The length of the encrypted PIN is defined by the payShield 9000 security settings. ➢ The LMK encrypted PIN uses an algorithm involving the account number.

Response

`HDR6NH001234F511599955529`

Fld	Format	Value	Description
1	4 A	`HDR6`	Message header (as defined by user).
2	2 A	`NH`	Response Code.
3	2 A	`00`	Error Code. 00 = No error.
4	5 H	`1234F`	The clear PIN, left-justified and padded with F.
5	12 N	`511599955529`	The reference number derived by encrypting the account number under the LMK. This allows the PIN to be associated with an account number without both being available in the clear.

PM Command - Verify Dynamic CVV/CVC (MasterCard)

The PM command allows a Dynamic CVV/CVC to be verified when processing a transaction. In this example, we are verifying a CVC3 in the magstripe track data of a MasterCard PayPass card.

Command

```
HDREPM12U42F5FBDFE936A8CCFC0F0CDBA7D80C03A5241060000000069;00019<5
241060000000069D1305202000000000000003F>000000083900032XX942
```

Fld	Format	Value	Description
1	4 A	HDRE	Message header (as defined by user).
2	2 A	PM	Command Code.
3	1 N	1	Scheme ID. 1 = MasterCard PayPass
4	1 N	2	Version 2 = For MasterCard PayPass, PSN is provided in input and IVCVC3 calculated from provided mag. Stripe data.
5	1 A + 32 H	U42F5FBDFE936A8CCFC0F0CDBA7D80C03	Master Key for Dynamic CVV (MK-DCVV), encrypted under LMK pair 28-29 variant 7, where Scheme ID = 1. U = Double-length TDES key scheme
6	1 A	A	Key derivation method. A = EMV4.1 Book 2 Option A method.
7	16 N	5241060000000069	PAN. (Maximum length allowed for Scheme ID = 1 is 19 digits.)
8	1 A	;	Delimiter to indicate end of PAN.
9	2 N	00	PAN Sequence Number (PSN). 00 = not available.
10	3 N	019	Length of Track Data field. (REMINDER: we are using Scheme ID = 1, Version = 2 in this example.)
11	19 Bytes	<5241060000000069D1305202000000000000003F>	Static Track (1 or 2) Data
12	10 N	0000000839	Unpredictable number. Random number provided to the card by the terminal during a PayPass transaction. (NOTE: the Unpredictable number could also use a format of 8D, e.g. 00000347.)
13	5 N	00032	Decimal value of Application Transaction Counter.
14	5 A	XX942	The CVC3 to be validated. The "X" characters are like wildcard characters such that, for example, a CVC3 of "XX942" will match a calculated CVC3 of "87942".

Response

```
HDREPN00
```

Fld	Format	Value	Description
1	4 A	HDRE	Message header (as defined by user).
2	2 A	PN	Response Code.
3	2 A	00	Error Code. 00 = No error - i.e. verification successful.

PM Command - Verify Dynamic CVV/CVC (Visa)

In this example, we are verifying a dCVV in the magstripe track data of a Visa contactless card.

Command

```
HDREPM00UDD4BB1AF0B96841182E94DD953FF4146A13123456784808;060612300
5530598
```

Fld	Format	Value	Description
1	4 A	HDRE	Message header (as defined by user).
2	2 A	PM	Command Code.
3	1 N	0	Scheme ID. 0 = Visa
4	1 N	0	Version Always 0 for Visa.
5	1 A + 32 H	UDD4BB1AF0B96841182E94 DD953FF4146	Master Key for Dynamic CVV (MK-DCVV), encrypted under LMK pair 28-29 variant 7, where Scheme ID = 1. U = Double-length TDES key scheme
6	1 A	A	Key derivation method. A = EMV4.1 Book 2 Option A method.
7	14 N	13123456784808	PAN. (Maximum length allowed for Scheme ID = 0 is 16 digits.)
8	1 A	;	Delimiter to indicate end of PAN.
9	4N	0606	Card Expiry Date
10	3N	123	Service Code, from card's Track 2 data.
11	6N	005530	Application Transaction Counter (ATC) – padded to the left with 0's.
12	3N	598	dCVV to be validated

Response

```
HDREPN00
```

Fld	Format	Value	Description
1	4 A	HDRE	Message header (as defined by user).
2	2 A	PN	Response Code.
3	2 A	00	Error Code. 00 = No error - i.e. verification successful.

Americas

THALES e-SECURITY
900 South Pine Island Road
Suite 710
Plantation
Florida
33324. USA

T: +1 888 744 4976
or +1 954 888 6200

F: +1 954 888 6211

E: sales@thalesesec.com

Asia Pacific

THALES e-SECURITY
Unit 4101, 41/F
248 Queen's Road East
Wanchai
Hong Kong,
PRC

T: +852 2815 8633

F: +852 2815 8141

E: asia.sales@thales-esecurity.com

Europe, Middle East, Africa

THALES e-SECURITY
Meadow View House
Long Crendon
Aylesbury
Buckinghamshire
HP18 9EQ. UK

T: +44 (0)1844 201800

F: +44 (0)1844 208550

E: emea.sales@thales-esecurity.com

© Copyright 1987 - 2014 THALES UK LTD

This document is issued by Thales UK Limited (hereinafter referred to as Thales) in confidence and is not to be reproduced in whole or in part without the prior written approval of Thales. The information contained herein is the property of Thales and is to be used only for the purpose for which it is submitted and is not to be released in whole or in part without the prior written permission of Thales.

THALES