cpl.thalesgroup.com

payShield 9000 v3.5

Host Command Reference Manual Addendum for License LIC003 (Australian AS2805 Commands)

1270A547-038

14 October 2021

Contents

End User License Agreement

Use of this product is subject to the Thales Cloud Protection & Licensing *End User License Agreement* found at:

https://cpl.thalesgroup.com/legal

Revision Status

Document No.	Manual Set	Software Version	Release Date
1270A547-038	Issue 38	payShield 9000 v3.5	October 2120

References

The following documents are referenced in this document:

1	RG7000 Host Security Module, Operation and Installation Manual, Document Number 1270A513 Issue 7.
2	RG7000 Host Security Module, Programmer's Manual, Document Number 1270A514 Issue 7.
3	payShield 9000 Security Operations Manual
4	payShield 9000 Installation Manual
5	payShield 9000 Console Reference Manual
6	payShield 9000 Host Programmer's Manual
7	payShield 9000 Host Command Reference Manual
8	AS2805 Electronic Funds Transfer – various parts: Specifically AS2805 4.1 Electronic Funds Transfer – Requirements for Interfaces; Message Authentication Mechanism using a block cipher. AS2805 5.2 Electronic Funds Transfer – Requirements for Interfaces; Modes of operation for an *n*-bit block cipher algorithm AS2805.5.4, Electronic Funds Transfer – Requirements for Interfaces; DEA3 and related techniques. AS2805.6.2, Electronic Funds Transfer – Requirements for Interfaces; Key Management – Transaction Keys, 2002. AS2805.6.3, Electronic Funds Transfer – Requirements for Interfaces; Key Management – Session Keys – Node-to-Node, 2000 AS2805.6.4, Electronic Funds Transfer – Requirements for Interfaces; Key Management – Session Keys – Terminal-to-Acquirer, 2000 AS2805.6.5.1, Electronic Funds Transfer – Requirements for Interfaces; TCU initialisation Principles
9	HSM Support for the Australian Transaction Key Scheme to AS2805 Part 6.2, Document Number 40-1018-02, written by Racal-Guardata Financial Systems Ltd, 08 June 1989

The term PRODUCT is used throughout this document to refer to the device or system that this document describes.

Abbreviations

Abbreviation	Meaning
KEK	Double length Key Encryption Key
TDES	Triple DES
ANSI	American National Standard Institute
CBC	Cipher Block Chaining
DES	Data Encryption Standard
ECB	Electronic Code Book
IV	Initialization Vector
LMK	Local Master Key
MAC	Message Authentication Code
MK	MAC Key
PIN	Personal Identification Number
PVK	PIN Verification Key
TMK	Terminal Master Key
TPK	Terminal PIN Key
PKr	Public Key of recipient
PKs	Public Key of sender
SKr	Secret Key of recipient
SKs	Secret Key of sender
ZAK	Zone Authentication Key
ZEK	Zone Encryption Key
ZMK	Zone Master Key
ZPK	Zone PIN Key
KHSK	Host RSA Secret Key

Host Command Conventions

The following conventions will be used when describing various host commands.

Code	Convention
L	Encrypted PIN length. This is either H or N format (see below) depending on how it is specified in each command. Set during configuration.
m	Message header length. Set during configuration. Value 1 to 255 see Ref. 1 page 3-10. Message header is always format A – Alphanumeric characters.
n	Variable length field.
A	Alphanumeric characters. ASCII values between X’20 and X’7F inclusive and EBCDIC values between X’40 and X’7F inclusive.
H	Hexadecimal characters sent Hex-Encoded. For example, the data X’1A9F would be sent as the 4 bytes, X’31413946(ASCII), or X’F1C1F9C6(EBCDIC).
N	Numeric field sent Hex-Encoded. For example, the data 975 (decimal) would be sent as the 3 bytes, X’393735(ASCII), or X’F9F7F5(EBCDIC).
B	Raw binary data, in bytes. For example, the data X’1FA7 would be sent as the 2 bytes X’1FA7.
C	Control characters. ASCII values between X’00 and X’1F inclusive and EBCDIC values between X’00 and X’3F inclusive.

Additionally, the headers and control characters associated with the transport layer protocol will not be shown. For example, control characters STX and ETX which bracket every Host command on the async host interface will not be shown.

Further explanation of these codes can be found in reference [2] and [6].

Chapter 1 - Introduction

Overview

This document specifies the functions to be provided by a payShield 9000 host security module (HSM) to support the Australian AS2805 Standards. This document also provides the functionality to support the Australian Payments Clearing Association (APCA) Security Control Module specifications.

PIN Block 46 in Appendix K, is applicable to standard HSM PIN translate and verify function calls. The standard HSM function calls used are CA, CC, DA, DC, EA and EC.

A comparison guide between the APCA specifications and the Thales equivalent functions is provided in Appendix S. This is not a definitive guide but seeks to provide an equivalent where there is no direct comparison.

The functionality described in this manual is enabled by applying optional license HSM9-LIC003 to the payShield 9000.

PCI HSM Certification and Compliance

From version 1.1b, a number of payShield 9000 software versions have been certified to the PCI HSM security standard. Prior to PCI HSM certification being mandated by the card schemes, only some versions of base payShield 9000 software will be certified. Once the mandates are in place, all versions of base software will be PCI HSM certified.

See Chapter 10 of the General Information Manual on PCI HSM Compliance for information about PCI HSM compliance. This includes a table that indicating which versions of payShield 9000 software are PCI HSM certified: this information is also accessible in the Release Notes.

Table of Commands

Code	Console / Host	Name	Chapter	Interchange / Terminal
		Console Commands		
EA	Console	Convert (KEK)ZMK into a KEKr or KEKs	2	Inter
		DES Host Commands		
OI	Host	Generate a Set of Zone Keys	3	Inter
OK	Host	Translate a Set of Zone Keys to Encryption under the Local Master Key	3	Inter
PO	Host	Translate a PIN Block to Encryption under a Zone PIN Key	3	Inter
PQ	Host	Generate a Message Authentication Code AS2805 – 1985	3	Inter
C2	Host	Generate a Message Authentication Code (large messages)	3	Inter
PS	Host	Validate a Message Authentication	3	Inter

Code	Console / Host	Name	Chapter	Interchange / Terminal
		Code AS2805 –1985		
C4	Host	Verify a Message Authentication Code (large messages)	3	Inter
PU	Host	Encrypt Data	3	Inter
PW	Host	Decrypt Data	3	Inter
E0	Host	Generate a KEKs Validation Request	3	Inter
E2	Host	Generate a KEKr Validation Response	3	Inter
F6	Host	KEKGEN	3	Inter
F8	Host	KEKREC	3	Inter
C0	Host	Generate Initial Terminal Master Keys	3	Term
OU	Host	Update Terminal Master Key 1	3	Term
OW	Host	Update Terminal Master Keys	3	Term
PI	Host	Generate a Set of Terminal Keys	3	Term
PK	Host	Generate a PIN Pad Acquirer Security Number	3	Term
C8	Host	Generate an Acquirer Master Key Encrypting Key	3	Term
D4	Host	Translate a PIN Block to Encryption under a PIN Encryption Key	3	Term
D6	Host	Translate an Acquirer Master Key Encrypting Key	3	Term
E4	Host	Verify a PIN Pad Proof of End Point	3	Term
F0	Host	Verify a Terminal PIN using the IBM Method	3	Term
F2	Host	Verify a Terminal PIN using the VISA Method	3	Term
F4	Host	Calculate KMACI	3	Term
C6	Host	Generate a Random Number	3	Term
D0	Host	Generate a PIN Pad Authentication Code	3	Term
D8	Host	Encrypt a CPAT Authentication Value	3	Term
D2	Host	Verify a PIN pad Authentication code	3	Term
E6	Host	Generate a PIN Pad Proof of Endpoint	3	Term
E8	Host	Generate a KCA and KMACH	3	Term
QI	Host	Translate a PPASN from old to new LMK	3	Term
PY	Host	Verify and Generate an IBM PIN Offset	3	Term
P0	Host	Verify and Generate a VISA PVV	3	Term
P2	Host	Generate a VISA PVV	3	Term
P4	Host	Generate a Proof of Host value	3	Term
		AS2805.6.2 functionality		

Code	Console / Host	Name	Chapter	Interchange / Terminal
RE	Host	Verify a Transaction Request, without PIN	6	Term
RG	Host	Verify a Transaction Request, with PIN, when CD Field Available	6	Term
RI	Host	Verify a Transaction Request, with PIN, when CD Field not Available	6	Term
RK	Host	Generate Transaction Response, with Auth Para Generated by Acquirer	6	Term
RM	Host	Generate Transaction Response with Auth Para Generated by Card Issuer	6	Term
RO	Host	Translate a PIN from PEK to ZPK Encryption	6	Term
RQ	Host	Verify a Transaction Completion Confirmation Request	6	Term
RS	Host	Generate a Transaction Completion Response	6	Term
QQ	Host	Verify a PIN at Card Issuer using IBM Method	6	Term
QS	Host	Verify a PIN at Card Issuer using the Diebold Method	6	Term
QU	Host	Verify a PIN at Card Issuer using Visa Method	6	Term
QW	Host	Verify a PIN at Card Issuer using the Comparison Method	6	Term
RU	Host	Generate Auth Para at the Card Issuer	6	Term
RW	Host	Generate an Initial Terminal Key	6	Term
QM	Host	Data Encryption Using a Derived Privacy Key	6	Term
QO	Host	Data Decryption Using a Derived Privacy Key	6	Term
		RSA Host Commands		
H0	Host	Decrypt a PIN Pad Public Key	6	Term
H2	Host	Generate a RSA Public Key Verification Code	6	Inter
H4	Host	Generate a KEKs for use in Node to Node interchange using RSA	6	Inter
H6	Host	Receive a KEKr for use in Node to Node interchange using RSA	6	Inter
H8	Host	Encrypt a Cross Acquirer Key Encrypting Key under an Initial Transport Key	6	Term
I0	Host	Encrypt a Terminal Key under the Local Master Key	6	Term

Other firmware changes

LMK pair validation and usage

Generic commands are used to generate keys and to export and import them. An export command is one that translates a key from LMK encryption to encryption under a ZMK, for sending to another party. Import is the reverse, for receiving keys and translation for local storage. A table of 'permitted actions' controls both console and host generic commands. These generic commands will be used to generate, import and export keys. Some of these keys use their own specific LMK pairs and variants. To permit these actions, changes have been made to the Key Type Table – see Chapter 4 of the General Information Manual.

Errors are created when an action breaks the rules imposed by the table. The error given in this case:

29 : Key function not permitted

The commands to which the table applies are:

Command	Console	Host
Generate a key	KG	A0
Generate & print a component		A2
Form a key from encrypted components		A4
Import a key	KI	A6
Export a key	KE	A8
Generate & print a key as split components		NE
Generate key component	GC	
Generate key component & write to smart card	GS	
Encrypt a clear component	EC	
Form a key from components	FK	

NOTES for the Key Table at Chapter 1 of the Host Command Reference Manual:

KR & KS keys are only available under variants of KEK (ZMK)

G = Generate. E = Export. I = Import.

N = Not allowed. A = allowed in Authorized state. U = allowed Unconditionally, i.e. without Authorized state.

The A6 & A8 commands should take the permissions from the table and not have an overriding requirement for Authorized state.

Three new key encryption schemes are specified in Appendix M they are only applicable for import and export. These schemes use CBC method to encrypt the keys and apply an appropriate transport variant documented in Appendix D.

Chapter 2 – Console Commands

EA – Convert (KEK)ZMK into a KEKr or KEKs

Function: To move a (KEK)ZMK from encryption under LMK Pair 4 – 5 to encryption under LMK Pair 4 – 5 variant 3 or 4.

Notes: **The payShield 9000 must be in Authorized State.**

This command supports Variant LMKs only.

Input: KEK (ZMK) encrypted under LMK pair 4 – 5: 32 Hex or 1 Alpha + 32 Hex or 1 Alpha + 48 Hex.

Key Check Value: 6 Hex

KEK type (R/ S) : KEKr or KEKs

Key scheme: Key scheme for encrypting key under LMK.

Output: KEKr or KEKs.

Errors: NOT AUTHORISED – Self explanatory.

KEY PARITY ERROR – The KEK (ZMK) does not have odd parity.

KEY CHECK VALUE FAILURE – The Key Check Value does not match the key.

MASTER KEY PARITY ERROR – The contents of LMK storage have been corrupted or erased. Do not continue – inform the Security Department.

Example:

```
Online-AUTH> EA <Return>
Enter ZMK: U AAAA AAAA AAAA AAAA BBBB BBBB BBBB BBBB <Return>
Enter Key check value: XXXXXX <Return>
Enter KEK type (R/S): R <Return>
Key Scheme: U <Return>
KEKr : U CCCC CCCC CCCC CCCC DDDD DDDD DDDD DDDD
Online-AUTH>
```

Chapter 3 – Host Commands

OI/OJ Generate a Set of Zone Keys

Command:

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

Notes:

Each of the zone keys will be adjusted for odd parity on each byte. A check value for each key will be generated (as defined in Appendix C). The definition of each of the KEKs / ZMK variants is given in Appendix D.

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

This command supports Variant LMKs only.

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

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

OK/OL Translate a Set of Zone Keys to Encryption under the Local Master Key

Command:

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

Note:

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

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

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

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

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

This command supports Variant LMKs only.

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

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

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

C0/C1 Generate Initial Terminal Master Keys (AS2805 – 2001)

Command:

To generate two random initial Terminal Master Keys (TMK_1 and TMK_2) and encrypt them under a Acquirer Initialization Key (KIA) and the appropriate LMK pair.

Notes:

The plaintext keys will be adjusted for odd parity on each byte before they are encrypted under the LMK. A check value for each key is generated (see Appendix C).

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

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

This command supports Variant LMKs only.

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

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

OU/OV Update Terminal Master Key 1

Command:

To generate a new Terminal Master Key (TMK_1) and encrypt it under Variant 1 of LMK pair 14-15.

Notes:

The plaintext key will be adjusted for odd parity on each byte before it is encrypted under the LMK. A check value for the key is generated (see Appendix C). The method of updating the Terminal Master Key is defined in Appendix I.

The PIN Pad Acquirer Security Number (PPASN) is not checked for parity.

This command supports Variant LMKs only.

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

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

OW/OX Update Terminal Master Keys

Command:

To generate two new Terminal Master Keys (TMK_1 and TMK_2) and encrypt them under the appropriate LMK pairs.

Notes:

The plaintext keys will be adjusted for odd parity on each byte before they are encrypted under the LMK. A check value for each key is generated (see Appendix C). The method of updating the Terminal Master Keys is defined in Appendix I.

The PIN Pad Acquirer Security Number (PPASN) is not checked for parity.

This command supports Variant LMKs only.

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

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

PI/PJ Generate a Set of Terminal Keys

Command:

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

Notes:

A flag will indicate whether TMK_1 , TMK_2 or KMA will be used.
Each of the terminal keys will be adjusted for odd parity on each byte.
A check value for each key will be generated (as defined in Appendix C).
The definition of each of the TMK and KMA variants is given in Appendix D.
This command supports Variant LMKs only.

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

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

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

PK/PL Generate a PIN Pad Acquirer Security Number

Command:

To generate a PIN Pad Acquirer Security Number (PPASN) and return it encrypted under an Acquirer Key (KIA) and Variant 8 of LMK pair 14-15.

Note:

The PPASN is not a key and so will not be adjusted for odd parity.

If KIA is double length (1 A + 32 H) then output eKIAV88(PPASN) as per AS2805.6.4 section 7.2.4

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'PK'
Acquirer Key	16 H or 1 A + 32 H	KIA, encrypted under either Variant 1 or Variant 6 of LMK pair 14-15.
PIN Pad Serial Number	16 H	Optional PIN Pad Serial Number
Delimiter	1 A	Optional: If present the following field must be present. Value ';'
Acquirer Key flag	1 N	Optional field, present if delimiter is present. 1 = KIA under Variant 1 of LMK pair 14-15 2 = KIA under Variant 6 of LMK pair 14-15
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'PL'
Error Code	2 N	00 - No errors 10 - KIA parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 – Invalid user storage index
PPASN (LMK)	16 H	PPASN, encrypted under Variant 8 of LMK pair 14-15
PPASN (KIA)	16 H	PPASN, encrypted under the KIA. Variant 88 applied when 1 A + 32 H key used in input.
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

PO/PP Translate a PIN Block to Encryption under a Zone PIN Key

Command:

To translate a PIN block from encryption under a PIN Encryption Key (KPE) to encryption under a Zone PIN Key (ZPK).

Notes:

The KPE is derived from a Terminal PIN Key (TPK) and two other values, the Systems Trace Audit Number (STAN) and the transaction amount. The method of derivation of the KPE varies between single and double length TPK. These are defined in Appendix J.

The PIN block formats supported by the HSM are either given in Ref.2, Chapter 3. or a "zero" PIN block. The HSM will identify the "zero" PIN block type and translate it accordingly.

"Zero" PIN block defined in Appendix K.

This command supports Variant LMKs only.

Field	**Length and Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'PO'
Zone PIN Key	16 H or 1 A + 32 H or 1 A + 48 H	ZPK, encrypted under LMK pair 06-07
Terminal PIN Key	16 H or 1 A + 32 H	TPK, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
STAN	6 N	Systems Trace Audit Number
Transaction Amount	12 N	Transaction amount
Incoming PIN Block Format Code	2 N	A valid PIN block format code
Outgoing PIN Block Format Code	2 N	A valid PIN block format code
Incoming PIN Block	16 H	PIN block, encrypted under KPE
Account Number	12 N	Account number, used in PIN Block Format 01 or 04
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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'PP'
Error Code	2 N	00 - No errors 10 - TPK parity error 11 - ZPK parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 20 - PIN block error 21 - Invalid user storage index 23 - Invalid PIN block format code 24 - PIN length error 88 - Warning: AS2805.3 “zero” PIN block received
Outgoing PIN Block	16 H	PIN block, encrypted under the ZPK
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

PQ/PR Generate a Message Authentication Code AS2805.4 - 1985

Command:

To generate a Message Authentication Code (MAC) using either a Zone Authentication Key (ZAK) or a Terminal Authentication Key (TAK).

Notes:

The method of generating the MAC is defined in AS2805.4 (1985).

The HSM input and output buffers can support 2K bytes of data. It is recommended that the Authentication Data field in the command message is no greater than 1800 bytes.

If the Host communication link is configured for standard asynchronous communications then the Authentication Data will be in expanded hexadecimal format, with two hexadecimal characters representing each 8 bits of data. Thus 400 bytes of data would be represented by 800 hexadecimal characters.

If the Host communication link is configured for non asynchronous communications then the Authentication Data will be in binary format, with each byte representing 8 bits of data.

The Authentication Data field must be an exact multiple of 16 hexadecimal haracters if standard asynchronous communications are used or an exact multiple of 8 bytes if the non asynchronous mode is used.

This command supports Variant LMKs only.

Field	**Length and Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'PQ'
Key Flag	1 N	Flag to indicate which authentication key is used 0 = ZAK, encrypted under LMK pair 26-27 1 = TAK, encrypted under LMK pair 16-17
Authentication Key	16 H	ZAK or TAK, encrypted under relevant LMK pair
Length	3 H	Number of characters or bytes (non-asynchronous communications) of data to be authenticated. Note: For Asynchronous data, if the data is in expanded-hex format, the value given will be half the length of the data.
Authentication Data	n H or n B	Data to be authenticated (asynchronous communications) Data to be authenticated (non asynchronous communications)
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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	**Length and Type**	**Details**
	RESPONSE MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'PR'
Error Code	2 N	00 - No errors 10 - ZAK or TAK parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index 80 - Invalid data length
MAC	8 H	MAC, calculated on the data, using the given key
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

C2/C3 Generate a Message Authentication Code (large messages)

Command:

To generate a MAB for a large message using either a TAK or a ZAK. This command supports ANSI X9.9, X9.19, AS2805.4.1 (2001) standards.

Note:

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) 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.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'C2'
Message Block Number	1 N	Message block processing number 0 - Only Block 1 - First Block 2 - A Middle Block 3 - Last Block
Key Type	1 N	Key type 0 – TAK (Terminal Authentication Key) 1 – ZAK (Zone Authentication Key) 2 – TAKs (Send Terminal Authentication Key) 3 – ZAKs (Send Zone Authentication Key)
MAC generation Mode	1 N	Mode = 0 – X9.9 1 – X9.19 2 – AS2805.4.1 (2001) MAB output 3 – AS2805.4.1 (2001) MAC output
Message Type	1 N	Message Type 0 – Message data is binary 1 – Message data is expanded Hex
Key	16 H or 1 A + 32 H or 1 A + 48 H	Key, encrypted under appropriate LMK pair TAK under LMK pair 16 – 17 ZAK under LMK pair 26 – 27 TAKs under LMK pair 16 – 17 variant 1 ZAKs under LMK pair 26 – 27 variant 1
IV	16 H	Initialization value, present only when message block number is 2 or 3. Encrypted under LMK pair 16-17 variant 3.
Message Length	4 H	Length of Message to be MACED (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.

Field	Length and 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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MEESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'C3'
Error Code	2 N	00 - No errors 03 - Invalid Message Type Code 04 - Invalid Key Type Code 05 - Invalid Message Block Number 06 - Invalid MAC generation Mode 07 - Invalid key length 10 - KEY parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index 80 - Incorrect input data length
MAB / MAC	8 H or 16 H	Used as IV for next block when message block number is 1 or 2. Encrypted under LMK pair 16-17 variant 3. Used as message authenticator when message block is 0 or 3 If MAC generation mode = 3 output is MAC (8H)
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

PS/PT Validate a Message Authentication Code AS2805.4 -1985

Command:

To validate a Message Authentication Code (MAC) using either a Zone Authentication Key (ZAK) or a Terminal Authentication Key (TAK).

Notes:

The method of generating the MAC is defined in AS2805.4 (1985).

The input and output buffers can support 2K bytes of data. It is recommended that the Authentication Data field in the command message is no greater than 1800 bytes.

If the Host communication link is configured for standard asynchronous communications then the Authentication Data will be in expanded hexadecimal format, with two hexadecimal characters representing each 8 bits of data. Thus 400 bytes of data would be represented by 800 hexadecimal characters.

If the Host communication link is configured for non asynchronous communications then the Authentication Data will be in binary format, with each byte representing 8 bits of data.

The Authentication Data field must be an exact multiple of 16 hexadecimal characters if standard asynchronous communications are used or an exact multiple of 8 bytes if the non asynchronous mode is used.

This command supports Variant LMKs only.

Field	Length and Type	Details
		COMMAND MESSAGE
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'PS'
Key Flag	1 N	Flag to indicate which authentication key is used 0 = ZAK, encrypted under LMK pair 26-27 1 = TAK, encrypted under LMK pair 16-17
Authentication Key	16 H	ZAK or TAK, encrypted under relevant LMK pair
MAC	8 H	MAC, for validation
Length	3 H	Number of characters or bytes (non-asynchronous communications) of data to be authenticated. Note: For Asynchronous data, if the data is in expanded-hex format, the value given will be half the length of the data.
Authentication Data	n H or n B	Data to be authenticated (asynchronous communications) Data to be authenticated (non asynchronous communications)
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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'PT'
Error Code	2 N	00 - No errors 01 - MAC validation failure 10 - ZAK or TAK parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index 80 - Invalid data length
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

C4/C5 Verify a Message Authentication Code (large messages)

Command:

To verify a MAC for a large message using either a TAK or a ZAK. This command supports ANSI X9.9, X9.19, AS2805.4.1 (2001) standards

Note:

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) command.

The data for which the MAC is to be verified 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.

This command supports Variant LMKs only.

Field	Length and Type	Details
	COMMAND MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'C4'
Message Block Number	1 N	Message block processing number 0 - Only Block 1 - First Block 2 - A Middle Block 3 - Last Block
Key Type	1 N	Key type 0 – TAK (Terminal Authentication Key) 1 – ZAK (Zone Authentication Key) 2 – TAKr (Receive Terminal Authentication Key) 3 – ZAKr (Receive Zone Authentication Key)
MAC verification Mode	1 N	Mode = 0 – X9.9 1 – X9.19 2 – AS2805.4.1 (2001)
Message Type	1 N	Message Type 0 – Message data is binary 1 – Message data is expanded Hex
Key	16 H or 1 A + 32 H or 1 A + 48 H	Key, encrypted under appropriate LMK pair TAK under LMK pair 16 – 17 ZAK under LMK pair 26 – 27 TAKr under LMK pair 16 – 17 variant 2 ZAKr under LMK pair 26 – 27 variant 2
IV	16 H	Initialization value, present only when message block number is 2 or 3. Encrypted under LMK pair 16-17 variant 3.
MAC	8 H	MAC for verification, present only when message block number is either 0 or 3
Message Length	4 H	Length of Message to be MACED (length of following field if message type binary, Half the length of the

Field	Length and Type	Details
		following field if expanded Hex)
Message Block	n B or n 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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'C5'
Error Code	2 N	00 - No errors 01 – MAC verification failure 03 – Invalid Message Type Code 04 – Invalid Key Type Code 05 - Invalid Message Block Number 06 – Invalid MAC Verification Mode 07 - Invalid key length 10 - KEY parity error 12 No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index 80 - Incorrect input data length
MAB	16 H	MAB encrypted under LMK pair 16-17 variant 3. Only output if message block number is 1 or 2. Used as IV for next block.
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

PU/PV Encrypt Data

Command:

To encrypt a block of data, using either a Zone Encryption Key (ZEK) or a Terminal Encryption Key (TEK).

Note:

The modes of encryption supported by this command are Electronic Codebook (ECB), Cipher Block Chaining (CBC), 8-bit Cipher Feedback (CFB-8), and OFB (8 Bit or 8 Byte) - see AS2805.5.2 (Ref.8.2).

The input and output buffers can support 2K bytes of data. It is recommended that the Plaintext Data field in the command message is no greater than 1800 bytes.

If the Host communication link is configured for standard asynchronous communications then the input Plaintext Data and the output Encrypted Data will be in expanded hexadecimal format, with two hexadecimal characters representing each 8 bits of data. Thus 400 bytes of data would be represented by 800 hexadecimal characters.

If the Host communication link is configured for transparent asynchronous communications then the input Plaintext Data and the output Encrypted Data will be in binary format, with each byte representing 8 bits of data.

The Plaintext Data field must be an exact multiple of 16 hexadecimal fields if standard asynchronous communications are used or an exact multiple of 8 bytes if the transparent asynchronous mode is used. The Encrypted Data field will be the same size as the Plaintext Data field.

This command supports Variant LMKs only.

Field	**Length and Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'PU'
Key Flag	1 N	Flag to indicate which encryption key is used 0 = ZEK, encrypted under LMK pair 30-31 1 = TEK, encrypted under LMK pair 32-33 2 = ZEKs, encrypted under LMK pair 30-31 variant 1 3 = TEKs, encrypted under LMK pair 32-33 variant 1
Encryption Key	16 H or 1 A + 32 H or 1 A + 48 H	ZEK or TEK, encrypted under relevant LMK pair
Encryption Mode	1 N	Flag to indicate the mode of encryption 0 = ECB mode of encryption 1 = CBC mode of encryption 2 = CFB-8 mode of encryption 3 = OFB mode of encryption
Initialization Value	16 H	Initialization value, used with the CBC, CFB-8 or OFB modes of encryption
Plaintext Value (j)	1 N	Only used with OFB mode, value of either 1 for 1 byte (8bits) feedback or 8 for 8 byte (64bits) feedback
Length	3 H	Length (in bytes) of data to be encrypted
Plaintext Data	n H or n B	Data to be encrypted (asynchronous mode) Data to be encrypted (transparent asynchronous mode)

Field	Length and 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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'PV'
Error Code	2 N	00 - No errors 10 - ZEK or TEK parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index 80 - Invalid data length
Encrypted Data	n H or n B	Encrypted data (asynchronous mode) Encrypted data (transparent asynchronous mode)
OCV	16 H	Output Chaining Value, only used when OFB mode is used
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

PW/PX Decrypt Data

Command:

To decrypt a block of data, using either a Zone Encryption Key (ZEK) or a Terminal Encryption Key (TEK).

Note:

The modes of encryption supported by this command are Electronic Codebook (ECB), Cipher Block Chaining (CBC) or 8-bit Cipher Feedback (CFB-8) - see AS2805.5.2 (Ref.8.2).

The HSM input and output buffers can support 2K bytes of data. It is recommended that the Encrypted Data field in the command message is no greater than 1800 bytes.

If the Host communication link is configured for standard asynchronous communications then the input Encrypted Data and the output Plaintext Data will be in expanded hexadecimal format, with two hexadecimal characters representing each 8 bits of data. Thus 400 bytes of data would be represented by 800 hexadecimal characters.

If the Host communication link is configured for transparent asynchronous communications then the input Encrypted Data and the output Plaintext Data will be in binary format, with each byte representing 8 bits of data.

The Encrypted Data field must be an exact multiple of 16 hexadecimal fields if standard asynchronous communications are used or an exact multiple of 8 bytes if the transparent asynchronous mode is used. The Plaintext Data field will be the same size as the Encrypted Data field.

This command supports Variant LMKs only.

Field	Length and Type	Details
	COMMAND MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'PW'
Key Flag	1 N	Flag to indicate which encryption key is used 0 = ZEK, encrypted under LMK pair 30-31 1 = TEK, encrypted under LMK pair 32-33 2 = ZEKr, encrypted under LMK pair 30-31 Variant 2 3 = TEKr, encrypted under LMK pair 32-33 Variant 2
Encryption Key	16 H or 1 A + 32 H or 1 A + 48 H	ZEK or TEK, encrypted under relevant LMK pair
Encryption Mode	1 N	Flag to indicate the mode of encryption 0 = ECB mode of encryption 1 = CBC mode of encryption 2 = CFB-8 mode of encryption 3 = OFB mode of encryption
Initialization Value	16 H	Initialization value, used with the CBC, CFB-8 or OFB modes of encryption
Plaintext Value (j)	1 N	Only used with OFB mode, value of either 1 for 1 byte (8bits) feedback or 8 for 8 byte (64bits) feedback
Length	3 H	Length (in bytes) of data to be decrypted
Encrypted Data	n H or	Data to be decrypted (asynchronous mode) Data to be decrypted (transparent asynchronous mode)

Field	Length and Type	Details
	n B	
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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'PX'
Error Code	2 N	00 - No errors 10 - ZEK or TEK parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index 80 - Invalid data length
Plaintext Data	n H or n B	Plaintext data (asynchronous mode) Plaintext data (transparent asynchronous mode)
OCV	16 H	Output Chaining Value, only used when OFB mode is used
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

C8/C9 Generate an Acquirer Master Key Encrypting Key

Command:

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

Note:

The KIA is generated from a Cross Acquirer Key Encrypting Key (KCA) and an Acquiring Institution Identification Code (AIIC) using the one-way function defined in Appendix A.

The key scheme flags are ignored in processing.

This command supports Variant LMKs only.

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

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

D4/D5 Translate a PIN Block to Encryption under a PIN Encryption Key

Command:

To translate a PIN Block from encryption under a Terminal PIN Key (KTP) to encryption under a PIN Encryption Key (KPE).

Note:

The input PIN block will be either a standard AS2805 (ANSI X9.8) PIN block or a zero PIN block. The HSM will identify the PIN block type and translate it accordingly.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'D4'
Terminal PIN Key	16 H or 1 A + 32 H or 1 A + 48 H	TPK, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
PIN Encryption Key	16 H or 1 A + 32 H or 1 A + 48 H	KPE, encrypted under LMK pair 06-07
PIN Block	16 H	PIN block, encrypted under TPK
Account Number	12 N	Rightmost 12 digits of the Primary Account Number (PAN), excluding the check digit.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'D5'
Error Code	2 N	00 - No errors 10 - KTP parity error 11 - KPE parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 20 - PIN block error 21 - Invalid user storage index 24 - PIN length error 88 - Warning: AS2805.3 “zero” PIN block received
PIN Block	16 H	PIN block, encrypted under the KPE
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

D6/D7 Translate an Acquirer Master Key Encrypting Key

Command:

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

Note:

The TMK 1 is received encrypted under a Privacy Key (KP) which in turn is received encrypted under a Communications Key (KC). The KC will be received encrypted under LMK pair 04-05.

The key scheme flags are ignored in processing.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'D6'
KC	16 H or 1 A + 32 H or 1 A + 48 H	KC, encrypted under LMK pair 04-05
KP	16 H or 1 A + 32 H or 1 A + 48 H	KP, encrypted under KC
TMK 1	16 H or 1 A + 32 H or 1 A + 48 H	TMK 1, encrypted under KP
Delimiter	1 A	Optional: If present the following three fields must be present. Value ';'
Key Scheme ZMK	1 A	Optional. Key Scheme for encrypting keys under ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H (Appendix C)
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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

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

E0/E1 Generate a KEKs Validation Request

Command:

To generate a random key (KRs) and encrypt it with a variant of a double length Key Encrypting Key (KEKs). In addition, KRs is inverted (to form KRr) and the result encrypted with another variant of the KEKs.

Note:

The definition of the KEKs variants is given in Appendix D.

If no key scheme flags are supplied, the HSM generates a single length KRs & KRr, and the single length KEKs variants are used. If key scheme flags are used the HSM generates the appropriate length KRs & KRr as per the scheme and appropriate KEKs variants for the length of KR are used.

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

This command supports Variant LMKs only.

Field	**Length and Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'E0'
KEKs / Zone Master Key	32 H or 1 A + 32 H or 1 A + 48 H	KEKs, encrypted under LMK pair 04-05 variant 4 or ZMK, encrypted under LMK pair 04-05
Delimiter	1 A	Optional: If present the following three fields must be present. Value ';'
Key Scheme KEKs / ZMK	1 A	Optional. Key Scheme for encrypting keys under KEKs / ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H (Appendix C)
Delimiter	1 A	Optional: If present the following field must be present. Value ';'
Flag	1 N	Optional flag to indicate if KEKs or ZMK is used. 1 = KEKs; 2 = ZMK ONLY AVAILABLE IF PRECEDING KEY SCHEME IS USED
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'E1'
Error Code	2 N	00 - No errors 10 - KEKs parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index 26 - Invalid Key Scheme 27 - Incompatible key length 28 - Invalid key type
KRs	16 H or 1 A + 32 H or 1 A + 48 H	KRs, encrypted with variant 7 of KEKs or variant 7 of ZMK (see Appendix D)
KRr	16 H or 1 A + 32 H or 1 A + 48 H	KRr (i.e. inverted KRs), encrypted with variant 8 of KEKs or variant 8 of ZMK (see Appendix D)
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

E2/E3 Generate a KEKr Validation Response

Command:

To receive a random key (KRs) encrypted under a variant of a double length Key Encrypting Key (KEKr), compute from KRs another value, denoted KRr and encrypt it under another variant of the KEKr

Note:

The definition of the KEKr variants is given in Appendix D.

If no key scheme flags are supplied, the HSM will use the single length KEKr variant for the input KRs and output KRr, regardless of length of the KRs. If key scheme flags are supplied the HSM uses the appropriate variant of KEKr, depending on length for the input KRs and output KRr.

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

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'E2'
KEKr / Zone Master Key	32 H or 1 A + 32 H or 1 A + 48 H	KEKr, encrypted under LMK pair 04-05 variant 3 or ZMK, encrypted under LMK pair 04-05
KRs	16 H or 1 A + 32 H or 1 A + 48 H	KRs, encrypted with variant 7 of KEKr or variant 7 of ZMK (see Appendix D)
Delimiter	1 A	Optional: If present the following three fields must be present. Value ';'
Key Scheme KEKr	1 A	Optional. Key Scheme for encrypting keys under KEKr
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H (Appendix C)
Delimiter	1 A	Optional: If present the following field must be present. Value ';'
Flag	1 N	Optional flag to indicate if KEKr or ZMK is used. 1 = KEKr; 2 = ZMK ONLY AVAILABLE IF PRECEDING KEY SCHEME IS USED
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	**Length and Type**	**Details**
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'E3'
Error Code	2 N	00 - No errors 10 – KEKr parity error 12 - No keys loaded in user storage 13 LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index 26 - Invalid Key Scheme 27 - Incompatible key length 28 - Invalid key type
KRr	16 H or 1 A + 32 H or 1 A + 48 H	KRr (i.e. inverted KRs, encrypted with variant 8 of KEKr or variant 8 of ZMK(see Appendix D)
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

E4/E5 Verify a PIN Pad Proof of End Point

Command:

To verify a PIN Pad Proof of End point (POEP).

Note:

The proof of end point (POEP) is generated by the PIN pad by encrypting the PPASN (PIN Pad Acquirer Secret Number) with one of the Terminal Master Keys (known as KEK1 or KEK2 in AS2805 Part 6.4) or a Terminal Encryption Key. Only the left 32 bits is used for the POEP. This command will validate a proof of endpoint provided by the PIN Pad.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'E4'

Flag	1 N	Flag to indicate which TMK is used
		Flag = 1 if TMK1 is used
		Flag = 2 if TMK2 is used
		Flag = 3 if TEKr is used

Terminal Master Key or Terminal Encryption Key	32 H or 1 A + 32 H or 1 A + 48 H	TMK, encrypted under a Variant of LMK pair 14-15 (Variant 1 if Flag = 1; Variant 2 if Flag = 2). TEKr, encrypted under LMK pair 32-33 variant 2
PPASN	16 H	PIN Pad Acquirer Secret Number encrypted under Variant 8 of LMK pair 14-15
POEP	8 H	Proof of end point to be validated
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'E5'
Error Code	2 N	00 - No errors 01 – POEP does not Verify 10 - TMK parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index 88 - Warning: AS2805.3 "zero" PIN block received
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

F0/F1 Verify a Terminal PIN using the IBM Method (AS2805 6.4).

Command:

To verify a PIN from a terminal using the IBM 3624 method.

Note:

The PIN block shall be as specified in AS2805.3. The KPE shall be calculated as specified in AS2805.6.4 (Refer Appendix J)

The decimalization table can be stored in user storage and referenced in the same way as keys. The decimalization table of 16 digits must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, Error Code 25 is returned.

This command supports Variant LMKs only.

Field	**Length and Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'F0'
TPK	16 H or 1 A + 32 H	The TPK under which the PIN block is encrypted; encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
PVK	16 H or 1 A + 32 H or 1 A + 48 H	PVK encrypted under LMK pair 14-15 variant 0
STAN	6 N	Systems Trace Audit Number
Transaction Amount	12 N	Transaction Amount
PIN block	16 H	The PIN block encrypted under the KPE
PIN block format code	2 N	One of the valid format codes.
Check length	2 N	The minimum PIN length.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
Decimalization table	16 N or 1 A + 3 H	The table for converting hexadecimal values to decimal 'K' + 3 H to reference a decimalization table held in the HSM's User Storage Area.
PIN validation data	12A	User-defined data consisting of hexadecimal characters and the character N, which indicates to the HSM where to insert the last 5 digits of the account number.
Offset	12H	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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	**Length and Type**	**Details**
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'F1'
Error Code	2 N	00 - No errors 01 - Warning: Verification failure 02 - Warning: PVK not single length 06 - Invalid offset length 10 - TPK parity error 11 - PVK parity error 12 - No keys or table loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 20 - PIN block error 21 - Invalid user storage index 23 - Invalid PIN block format code 24 - PIN is fewer than 4 or more than 12 digits 25 - Decimalization table error 88 - Warning: AS2805.3 “zero” PIN block received
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

F2/F3 Verify a Terminal PIN using the VISA Method (AS2805 6.4).

Command:

To verify a PIN from a terminal using the VISA method.

Note:

The PIN block shall be as specified in AS2805.3. The KPE shall be calculated as specified in AS2805.6.4 (Refer Appendix J)

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'F2'
TPK	16 H or 1 A + 32 H	The TPK under which the PIN block is encrypted; encrypted under LMK pair 14-15 variant 0 if the security setting “Enforce key type 002 separation for PCI HSM compliance” has the value “N”, or under LMK pair 36-37 variant 7 if the setting has the value “Y”.
PVK pair	32 H or 1 A + 32 H or 1 A + 48 H	PVK encrypted under LMK pair 14-15 variant 0
STAN	6 N	Systems Trace Audit Number
Transaction Amount	12 N	Transaction Amount
PIN block	16 H	The PIN block encrypted under the KPE
PIN block format code	2 N	One of the valid format codes.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PVKI	1 N	The PVKI (should be between 0 and 6).
PVV	4 N	The PIN Verification Value
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'F3'
Error Code	2 N	00 - No errors. 01 - Verification failure. 10 - TPK parity error. 11 - PVK parity error. 12 - No keys or table loaded in user storage. 13 - LMK error; report to supervisor. 15 - Error in input data. 20 - PIN block does not contain valid values 21 - Invalid user storage index. 23 - Invalid PIN block format code. 24 - PIN is fewer than 4 or more than 12 digits. 88 - Warning: AS2805.3 “zero” PIN block received
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

F4/F5 Calculate KMACI

Command:

To calculate a initial MAC key.

Note:

The key scheme flags are ignored in processing.
This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'F4'
KIA	16 H or 1 A + 32 H or 1 A + 48 H	The KIA encrypted under LMK pair 14-15 Variant 6
Flag	1 N	Flag to denote format of AIIC following: 1 = 11N 2 = 16H 3 = 32H
AIIC	11N or 16H or 32H	The Acquirer Institution Identification Code
Delimiter	1 A	Optional: If present the following three fields must be present. Value ';'
Key Scheme ZMK	1 A	Optional. Key Scheme for encrypting keys under ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H (Appendix C)
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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	**Length and Type**	**Details**
	RESPONSE MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'F5'
Error Code	2 N	00 : No errors. 10 : KIA parity error. 12 : No keys or table loaded in user storage. 13 : LMK error; report to supervisor. 15 : Error in input data. 21 : Invalid user storage index. 26 - Invalid Key Scheme 27 - Incompatible key length 28 - Invalid key type
KMACI	16 H or 1 A + 32 H	The KMACI encrypted under LMK pair 16-17
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

F6/F7 KEKGEN – 6.3

Command:

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

Note:

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

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'F6'
ZMK	16 H or 32 H or 1 A + 32 H or 1 A + 48 H	The ZMK encrypted under LMK pair 4-5
Delimiter	1 A	Optional: If present the following three fields must be present. Value ';'
Key Scheme ZMK	1 A	Optional. Key Scheme for encrypting keys under ZMK
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H (Appendix C)
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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

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

F8/F9 KEKREC – 6.3

Command:

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

Note:

The partner’s KEKs becomes the host KEKr, and conversely the partner’s received KEKr becomes the host KEKs

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

This command supports Variant LMKs only.

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

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

C6/C7 Generate a Random Number

Command:

To generate a random 64 bit number.

Notes:

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'C6'
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'C7'
Error Code	2 N	00 - No errors
Random Number	16 H	Random Number
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

D0/D1 Generate a PIN Pad Authentication Code

Command:

To generate a PIN Pad Authentication Code (PPAC).

Note:

The PPAC is formed by encrypting the PIN Pad Serial Number (PPSN) with the acquirer Master Key Encrypting Key (KMA) and using the leftmost 32 bits of the result as the PPAC.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'D0'
KMA	16 H or 1 A + 32 H or 1 A + 48 H	KMA, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
PPSN	16 N	PIN Pad Serial Number
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'D1'
Error Code	2 N	00 - No errors 10 - KMA parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index
PPAC	8 H	PIN Pad Authentication Code
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

D8/D9 Encrypt a CPAT Authentication Value

Command:

To encrypt a CPAT Authentication Value (CAV).

Note:

The CAV is encrypted with a privacy key, denoted KD, which is derived from the current value of the Transaction Key (KT), the Systems Trace Audit Number (STAN) and the Card Acceptor Terminal Identification (CATID) according to the method defined in Appendix B for 16H and Appendix N-E for 32H key lengths.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'D8'
KT	16 H or 1 A + 32 H	KT, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
STAN	6 N	Systems Trace Audit Number
CATID	16 H	Card Acceptor Terminal Identification
CAV	16 H	CPAT Authentication Value
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'D9'
Error Code	2 N	00 - No errors 10 - KT parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index
Encrypted CAV	16 H	CAV, encrypted with KD
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

D2/D3 Verify a PIN Pad Authentication Code

Command:

To verify a PIN Pad Authentication Code (PPAC).

Note:

The PPAC is formed by encrypting the PIN Pad Serial Number (PPSN) with the Acquirer Master Key Encrypting Key (KMA) and using the leftmost 32 bits of the result as the PPAC.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'D2'
KMA	16 H or 1 A + 32 H or 1 A + 48 H	KMA, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
PPSN	16 N	PIN Pad Serial Number
PPAC	8 H	PIN Pad Authentication Code
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'D3'
Error Code	2 N	00 - No errors 01 – PPAC Verification error 10 - KMA parity error 12 - No keys loaded in user storage 13 LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

E6/E7 Generate a PIN Pad Proof of Endpoint (POEP)

Command:

To generate a PIN Pad Proof of End point (POEP).

Note:

The proof of end point (POEP) is generated by the PIN pad by encrypting the PPASN (PIN Pad Acquirer Secret Number) with one of the Terminal Master Keys (known as KEK1 or KEK2 in AS2805 Part 6.4) or a Terminal Encryption Key. Only the left 32 bits is used for the POEP.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'E6'

Flag	1 N	Flag to indicate which TMK is used
		Flag = 1 if TMK1 is used
		Flag = 2 if TMK2 is used
		Flag = 3 if TEKs is used

Terminal Master Key or Terminal Encryption Key	32 H or 1 A + 32 H or 1 A + 48 H	TMK, encrypted under a Variant of LMK pair 14-15 (Variant 1 if Flag = 1; Variant 2 if Flag = 2). TEKs, encrypted under LMK pair 32-33 variant 1
PPASN	16 H	PIN Pad Acquirer Secret Number encrypted under Variant 8 of LMK pair 14-15
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'E7'
Error Code	2 N	00 - No errors 01 - TMK parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index
Generated POEP	8 H	Generated POEP
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

E8/E9 Generate a KCA and KMACH

Command:

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

Note:

The key schemes for KI and LMK must be H & U respectively. If these values are not entered, error code 04 will be returned.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'E8'
Flag	1 N	Flag to indicate which LMK pair input is stored under 0 = LMK 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y". 1 = LMK 14-15 variant 6
KI	16 H or 1 A + 32 H or 1 A + 48 H	Initial Transport Key, encrypted under: If Flag=0: LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y". If Flag=1: LMK 14-15 variant 6
Delimiter	1 A	Optional: If present the following three fields must be present. Value ';'
Key Scheme KI	1 A	Optional. Key Scheme for encrypting keys under KI. Valid values include 'H', 'K' and 'L'.
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H (Appendix C)
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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'E9'
Error Code	2 N	00 - No errors 04 - Invalid key scheme 10 - KI parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor

Field	Length and Type	Details
		15 - Error in input data 21 - Invalid user storage index
KCA (LMK)	16 H or 1 A + 32 H or 1 A + 48 H	Sponsor Cross Acquirer Key encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
KCA (KI)	16 H or 1 A + 32 H or 1 A + 48 H	Sponsor Cross Acquirer Key encrypted under KI with appropriate variant
KMACH (LMK)	16 H or 1 A + 32 H or 1 A + 48 H	Sponsor MAC key encrypted under LMK pair 16-17 variant 1
KMACH (KI)	16 H or 1 A + 32 H or 1 A + 48 H	Sponsor MAC key encrypted under KI with appropriate variant
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

QI/QJ Translate a PPASN from old to new LMK

Command:

To translate a PPASN from encrypted under the old LMK, held in key change storage, to encryption under a new LMK.

Note:

For details of loading the old LMK into Key Change Storage see Ref 3. The PPASN is not a key so will not be checked for parity.

This command supports Variant LMKs only.

Field	**Length and Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'QI'
PPASN	16 H	PIN PAD Acquirer Security Number encrypted under old LMK 14-15 variant 8 held in key change storage
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	**Length and Type**	**Details**
	RESPONSE MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'QJ'
Error Code	2 N	00 - No errors 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index
PPASN	16 H	PIN PAD Acquirer Security Number encrypted under new LMK 14-15 variant 8
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

PY/PZ Verify and Generate an IBM PIN Offset (of a customer selected PIN)

Command:

To Verify an IBM PIN Offset using the AS2805 6.4 key scheme, and if successful, generate the PIN offset of the customer selected PIN using the IBM 3624 method. The current and new PINs are supplied in encrypted PIN Blocks.

Note:

The PIN blocks shall be as specified in AS2805.3. The KPE’s shall be calculated as specified in AS2805.6.4 (Refer Appendix J)

The decimalisation table can be stored in user storage and referenced in the same way as keys. The decimalisation table of 16 digits must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, Error Code 25 is returned.

This command supports Variant LMKs only.

Caution:

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

Decimalization Table: Encrypted/Plaintext [E/P]

When set to ‘E’ (the default setting), the supplied decimalization table must be encrypted (using console command ED), and will consist of 16 hexadecimal digits.

When set to ‘P’, the supplied decimalization table must be plaintext, and will consist of 16 decimal digits

Decimalization Table checks enabled? [Yes/No]

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

When set to ‘No’, the decimalization table is not checked.

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

When set to ‘No’ (the default setting), the length of the generated Offset is determined by the value of the Check Length parameter. This setting makes the command backward compatible with previous versions of HSM software.

When set to ‘Yes’, the length of the generated Offset matches the length of the input PIN.

Enable Weak PIN checking? [Yes/No]

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 ‘Excluded PIN Table’ is not checked. If present, the local ‘Excluded PIN Table’ is checked. If a match is found, then the command fails, returning error code 86.

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 and Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'PY'
TPK	32 H or 1 A + 32 H	The TPK under which the PIN block is encrypted; encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
PVK	32 H or 1 A + 32 H or 1 A + 48 H	PVK encrypted under LMK pair 14-15 variant 0
STAN	6 N	Systems Trace Audit Number
Transaction Amount	12 N	Transaction Amount
Current PIN block	16 H	The PIN block encrypted under the KPE
PIN block format code	2 N	One of the valid format codes.
Check length	2 N	The minimum PIN length.
Account number	12 N or 18 N	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the 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
Old Decimalization table	16 N or 16 H or 1 A + 3 H	16 N if console CS cmd is set for Plaintext decimalisation tables. 16 H if console CS cmd is set for Encrypted decimalisation tables 'K' + 3 H if the decimalization table is held in the HSM's User Storage Area
PIN validation data	12 A or 1 A + 16 H	User-defined data consisting of hexadecimal characters and the character N, which indicates to the HSM where to insert the last 5 digits of the 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 KPE
New Decimalization table	16 N or 16 H or 1 A + 3 H	16 N if console CS cmd is set for Plaintext decimalisation tables. 16 H if console CS cmd is set for Encrypted decimalisation tables 'K' + 3 H if the decimalization table is held in the HSM's User Storage Area
Delimiter	1 A	Value '*' Only present if the following Excluded PIN fields are present
Excluded PIN Count	2 N	'00' .. '99' : The number of excluded PINs listed in the following Excluded PIN Table
Excluded PIN Length	2 N	'04' .. '12' The length of each excluded PIN in the following Excluded PIN Table Only present if Excluded PIN Count > '00'
Excluded PIN Table	n N	A list of PINs to be excluded. The length of this field will be Excluded PIN Count multiplied by the Excluded PIN Length characters Only present if Excluded PIN Count > '00'
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.

Field	Length and 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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'PZ'
Error Code	2 N	00 - No errors 01 - Verification failure 06 - Invalid offset length 10 - TPK parity error 11 - PVK parity error 12 - No keys or table loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 20 - PIN block error 21 - Invalid user storage index 23 - Invalid PIN block format code 24 - PIN is fewer than 4 or more than 12 digits 25 - Decimalization table error 81 - PIN length mismatch 86 - PIN exists in either global or local Excluded PIN Table 88 - AS2805.3 “zero” PIN block received
New Offset	12 H	The new offset value; left justified and padded with ‘F’
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

P0/P1 Verify and Generate a VISA PVV (of a customer selected PIN)

Command:

To Verify a VISA PVV, and if successful, generate the PVV of the customer selected PIN using the VISA method. The Current & New PINs are supplied in an encrypted PIN Block.

Note:

The PIN blocks shall be as specified in AS2805.3. The KPE's shall be calculated as specified in AS2805.6.4 (Refer Appendix J)

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.

This command supports Variant LMKs only.

Caution:

The behaviour 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 and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'P0' (P-zero)
TPK	32 H or 1 A + 32 H	The TPK under which the PIN block is encrypted; encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
PVK pair	32 H or 1 A + 32 H or 1 A + 48 H	PVK encrypted under LMK pair 14-15 variant 0.
STAN	6 N	Systems Trace Audit Number
Transaction Amount	12 N	Transaction Amount
Current PIN block	16 H	The Current PIN block encrypted under the KPE
PIN block format code	2 N	One of the valid format codes.
Account number	12 N or 18 N	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the 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 (value 0 to 9).
Current PVV	4 N	The PIN Verification Value for the current PIN
New PIN Block	16 H	The New PIN block encrypted under the KPE
Delimiter	1 A	Value '*' Only present if the following Excluded PIN fields are present
Excluded PIN Count	2 N	'00' .. '99' : The number of excluded PINs listed in the following Excluded PIN Table
Excluded PIN Length	2 N	'04' .. '12' The length of each excluded PIN in the following Excluded PIN Table Only present if Excluded PIN Count > '00'
Excluded PIN Table	n N	A list of PINs to be excluded. The length of this field will be Excluded PIN Count multiplied by the Excluded PIN Length characters Only present if Excluded PIN Count > '00'
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'P1'
Error Code	2 N	00 - No errors. 01 - PIN Verification failure. 10 - TPK parity error. 11 - PVK parity error. 12 - No keys or table loaded in user storage. 13 - LMK error; report to supervisor. 15 - Error in input data. 20 - PIN block does not contain valid values 21 - Invalid user storage index. 23 - Invalid PIN block format code. 24 - PIN is fewer than 4 or more than 12 digits. 27 - PVK not double length 81 - PIN length mismatch 86 - PIN exists in either global or local Excluded PIN Table 88 - Warning: AS2805.3 "zero" PIN block received
New PVV	4 N	The PVV for the new PIN
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

P2/P3 Generate a VISA PVV (of a customer selected PIN)

Command:

Generate a 4 digit VISA PVV. The PIN (for which a PVV is required) is supplied in an encrypted PIN Block.

Note:

The PIN blocks shall be as specified in AS2805.3. The KPE's shall be calculated as specified in AS2805.6.4 (Refer Appendix J)

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' n order to exclude 'weak' PINs.

This command supports Variant LMKs only.

Caution:

The behaviour 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 and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'P2'
TPK	32 H or 1 A + 32 H	The TPK under which the PIN block is encrypted; encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
PVK pair	32 H or 1 A + 32 H or 1 A + 48 H	PVK encrypted under LMK pair 14-15 variant 0
STAN	6 N	Systems Trace Audit Number
Transaction Amount	12 N	Transaction Amount
PIN block	16 H	The PIN block encrypted under the KPE
PIN block format code	2 N	One of the valid format codes.
Account number	12 N or 18 N	For all PIN Block formats except 04, this is a 12 digit field, consisting of the 12 right-most digits of the 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 (value 0 to 9).
Delimiter	1 A	Value '*' Only present if the following Excluded PIN fields are present
Excluded PIN Count	2 N	'00' .. '99' : The number of excluded PINs listed in the following Excluded PIN Table
Excluded PIN Length	2 N	'04' .. '12' The length of each excluded PIN in the following Excluded PIN Table Only present if Excluded PIN Count > '00'
Excluded PIN Table	n N	A list of PINs to be excluded. The length of this field will be Excluded PIN Count multiplied by the Excluded PIN Length characters Only present if Excluded PIN Count > '00'
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	**Length and Type**	**Details**
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'P3'
Error Code	2 N	00 - No errors. 10 - TPK parity error. 11 - PVK parity error. 12 - No keys or table loaded in user storage. 13 - LMK error; report to supervisor. 15 - Error in input data. 20 - PIN block does not contain valid values 21 - Invalid user storage index. 23 - Invalid PIN block format code. 24 - PIN is fewer than 4 or more than 12 digits. 27 - PVK not double length 81 - PIN length mismatch 86 - PIN exists in either global or local Excluded PIN Table 88 - AS2805.3 “zero” PIN block received
PVV	4 N	The PVV for the PIN
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

P4/P5 Generate a Proof of Host value

Command:

To generate a value for the host to send to the PIN pad to prove the host is the bona fide host for the terminal. As per AS2805 6.4 terminal key management.

Note:

The One Way Function is as specified in AS2805.5.4. (Refer to Appendix N-A). This command supports Variant LMKs only.

Field	**Length and Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'P4'
Terminal Master Key 1	1 A + 32 H or 1 A + 48 H	TMK1, encrypted under Variant 1 of LMK pair 14-15
PPASN (LMK)	16 H	PPASN, encrypted under Variant 8 of LMK pair 14-15
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	**Length and Type**	**Details**
	RESPONSE MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'P5'
Error Code	2 N	00 - No errors. 10 – TMK1 parity error. 12 - No keys or table loaded in user storage. 13 - LMK error; report to supervisor. 15 - Error in input data.
Host Proof	8 H	The value for host proof of endpoint
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

Chapter 4 – RSA Host Commands

Introduction

This section specifies the RSA Host commands provided to support the requirements of the AS2805 standards.

H2/H3 Calculate a RSA Public Key Verification Code

Command:

Calculate a Public Key Verification Code.

Notes:

This command supports Variant LMKs only.
This command requires optional license LIC002 (RSA).

Field	**Length and Type**	**Details**
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'H2'
Public key encoding	2 N	Encoding rules for public key (must allow public key length to be inferred).
Public key	n B	Public key, encoded appropriately
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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	**Length and Type**	**Details**
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'H3' 00 : No errors. 03 : Invalid public key encoding type. 04 : Length error. 06 : Public exponent length error. 08 : Supplied public exponent is even. 15 : Error in input data.
PVC	16 H	The Public Key Verification Code
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

H4/H5 Generate a KEKs for use in Node to Node interchange using RSA

Command:

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

Note:

This command supports Variant LMKs only.

This command requires optional license LIC002 (RSA).

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

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

H6/H7 Receive a KEKr for use in Node to Node interchange using RSA

Command:

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

Note:

This command supports Variant LMKs only.

This command requires optional license LIC002 (RSA).

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

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

H0/H1 Decrypt a PIN Pad Public Key

Command:

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

Note:

All RSA data blocks will conform to the format defined in "APCA2000 SPECIFICATION FOR A SECURITY CONTROL MODULE FUNCTION SET", version 3.3, section 5.4.4.1 DEA 2 Text Block - DFormat 1 (see appendix Z1).

This command supports Variant LMKs only.

This command requires optional license LIC002 (RSA).

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

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

H8/H9 Encrypt a Cross Acquirer Key Encrypting Key under an Initial Transport Key

Command:

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

Note:

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

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

This command supports Variant LMKs only.

This command requires optional license LIC002 (RSA).

Field	**Length and Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'H8'
Public Key encoding	2 N	Encoding rules for the supplied public key (must allow the public key to be inferred)
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37
PIN PAD Public Key	n B	PPPK Public Key of PIN PAD ASN.1 encoded
Authentication Data	n A	Optional. Additional data to be included in the MAC calculation (must not include ;).
Delimiter	1 A	Value ';'
Secret key flag (SKsp)	2 N	The number is the index of the stored secret key, except 99 which means use the key supplied in the command
Secret key length	4 N	Length (in bytes) of the next field (present only if the secret key flag is 99).
Secret Key	n B	SK Secret Key (SKsp) encrypted under LMK pair 34-35. (present only if the secret key flag is 99).
Delimiter	1 A	Value ';' Only present if the secret key flag is 99.
Data Block Format Code Delimiter	1 A	Optional. Required when supplying the Data Block Format Code (in the following field). Note: If using Data Block Format Code = '04', this field is mandatory. Value '#'. If present, the following field must be present.
Data Block Format Code	2 N	The format code of the following Data Block: '01': Format 01 '02': Format 02 '03': Format 03 '04': Format 04 See Appendix V – Plaintext Data Block Formats for details. Must be present if the above delimiter is present.

Field	**Length and Type**	**Details**
Data Length	4 N	Length (in bytes) of the following data block
Data Block	n B	Data block encrypted by the Host Public Key, and the PIN PAD Secret Key
Delimiter	1 A	Optional, If present following field must be present Value ';'
Random Number	16 H	Random number
Delimiter	1 A	Optional: If present the following three fields must be present. Value
Key Scheme KTI	1 A	Optional. Key Scheme for encrypting keys under KTI. Valid values include 'K'.
Key Scheme LMK	1 A	Optional. Key Scheme for encrypting keys under LMK.
Key Check Value type	1 A	Optional. Key check value calculation method. 1 = KCV 6H (Appendix C)
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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

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

I0/I1 Encrypt a Terminal Key under the Local Master Key

Command:

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

Note:

This command supports Variant LMKs only.

This command requires optional license LIC002 (RSA).

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

Field	Length and 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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

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

Chapter 5 – AS2805.6.2 Support – Introduction

This section details all the host commands required to support the AS2805.6.2 – 2002 standard.

Purpose of this Section

The Australian Standard AS2805.6.2 - 2002 (Ref.8) on transaction key management supersedes the earlier (1988) standard (Ref.3). The main difference between the two standards is that the 2002 version of the standard specifies the use of double length keys, whereas the 1988 standard uses single length keys only.

The standard firmware for the Thales payShield 9000 has a number of functions to support the 1988 standard (see Ref.1, Chapter 28, and Ref.4).

This section specifies new functions for the payShield 9000 to support the 2002 standard. In order to maintain backwards compatibility with existing applications, the new commands have been written to permit both single length key (1988 standard) and double length key (2002 standard) processing. Where the 2002 standard processing requirements necessitate additional fields, these have been included as optional fields at the end of each command.

Summary of Transaction Key Scheme

The AS2805.6.2 transaction key management scheme is based on each terminal having a key (the Terminal Key (TK)) that is updated automatically with each transaction. The update is based on the current TK and Message Authentication Code (MAC) Residues of the current transaction. The MAC Residue is calculated using a MAC Key, derived from the current TK and the Primary Account Number (PAN) of the current debit or credit card. Similarly, a PIN Encryption Key is derived from the TK and the card data.

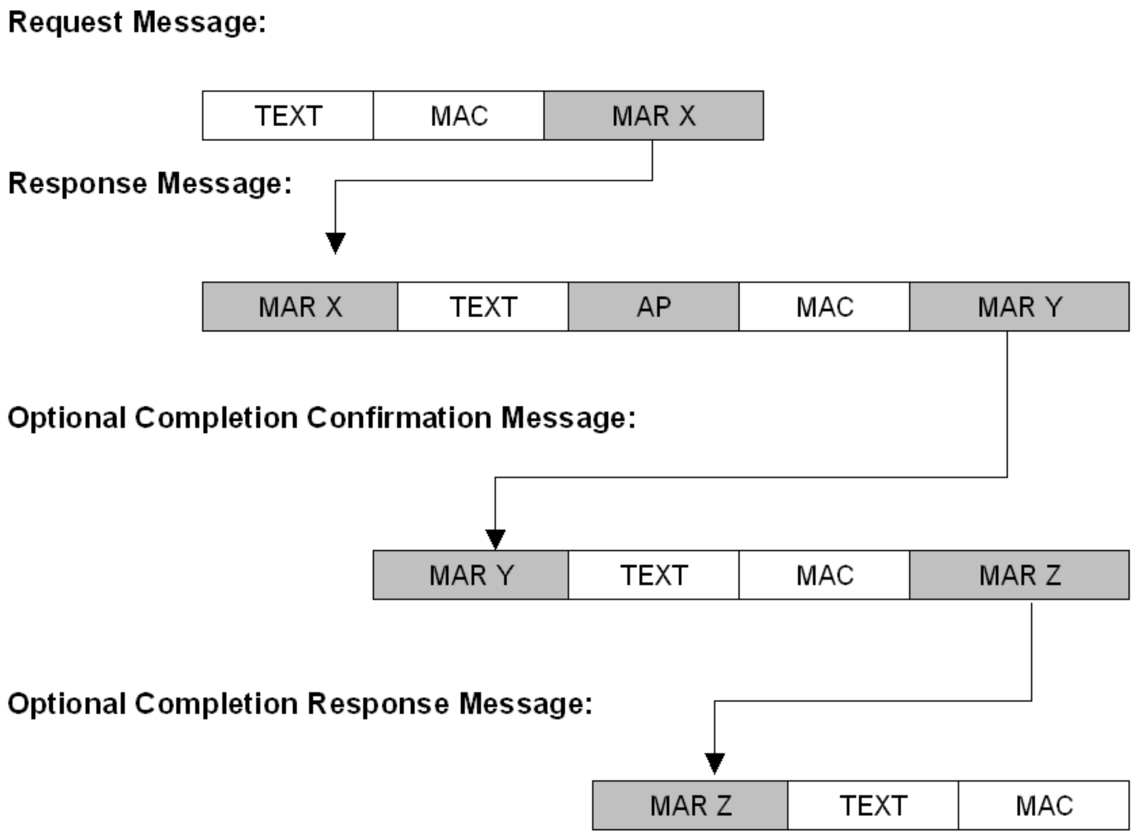
Thus, the current TK at a terminal is a function of the initial TK at that terminal and all previous cards and transaction details at that terminal.

The Acquirer system maintains a database of current TKs for all the terminals it supports, and updates each TK as described above.

Details of all processing primitives used during a transaction are given in the Appendices at the end of this document. Specifically Appendix N, under the following headings:

- One-Way Function (OWF)
- Derivation of Data Values
- MAC Key Derivation
- PIN Encipherment Key Derivation
- Privacy Key Derivation
- Terminal Key Update
- MAC and MAC Residue (MAR) Calculation
- Authentication Parameter (AP)

The following diagram shows a transaction flow, between a terminal and the Acquirer. The transaction is initiated from the terminal. The shaded fields are not transmitted, but where they precede the MAC they form part of the data used to calculate the MAC.



The Authentication Parameter (AP) is calculated from card data, including discretionary data (possibly non-transmitted), certain transaction details and the terminal identifier. In the most secure version of the scheme, where the discretionary data is not transmitted, only the Card Issuer can calculate the AP. Thus, the inclusion of the AP in the MAC calculation for the Response Message is "proof" of the Card Issuer's involvement in the transaction.

If the discretionary card data is transmitted in the Request Message then the AP may be calculated by the Acquirer.

Summary of Commands Specified in this section

The commands specified in this section fall, naturally, into five categories:

Transaction with no PIN and AP Generated by the Acquirer

In this case, the sequence of commands is:

Command	Description	Notes
'RE'	Verify Transaction Request, without PIN	Acquirer function
'RK'	Generate Transaction Response when AP Generated by the Acquirer	Acquirer function
'RQ'	Verify Transaction Completion Confirmation Request	Acquirer function (optional)
'RS'	Generate Transaction Completion Response	Acquirer function (only if previous command ('RQ') is required)

Transaction with no PIN and AP Generated by the Issuer

In this case, the sequence of commands is:

Command	Description	Notes
'RE'	Verify Transaction Request, without PIN	Acquirer function
'RU'	Generate AP at Card Issuer	Issuer function
'RM'	Generate Transaction Response when AP Generated by the Issuer	Acquirer function
'RQ'	Verify Transaction Completion Confirmation Request	Acquirer function (optional)
'RS'	Generate Transaction Completion Response	Acquirer function (only if previous command ('RQ') is required)

PIN Verification at the Acquirer

In this case, the sequence of commands is:

Command	Description	Notes
'RG'	Verify Transaction Request, with PIN, when CD Field Available	Acquirer function
'DA','CG', 'DC','BC'	PIN Verify (standard commands)	Acquirer function
'RK'	Generate Transaction Response when AP Generated by the Acquirer	Acquirer function
'RQ'	Verify Transaction Completion Confirmation Request	Acquirer function (optional)
'RS'	Generate Transaction Completion Response	Acquirer function (only if previous command ('RQ') is required)

PIN Verification at the Issuer

In this case, the sequence of commands is:

Command	Description	Notes
'RI'	Verify Transaction Request, with PIN, when CD Field not Available	Acquirer function
'RO'	Translate PIN from PEK to ZPK Encryption	Acquirer function
'QQ','QS', 'QU','QW'	PIN Verify (various methods)	Issuer function
'RM'	Generate Transaction Response when AP Generated by the Issuer	Acquirer function
'RQ'	Verify Transaction Completion Confirmation Request	Acquirer function (optional)
'RS'	Generate Transaction Completion Response	Acquirer function (only if previous command ('RQ') is required)

Other Commands

The RW command is a “new” command, in that there is no equivalent function specified in Ref.1. The QM & QO commands are required to satisfy the requirement to encipher track 2 data in terminals supporting AS2805.6.2 functionality

Command	Description	Notes
'RW'	Generate Initial Terminal Key	Acquirer function
'QM'	Data Encryption Using a Derived Privacy Key	Acquirer function
'QO'	Data Decryption Using a Derived Privacy Key	Acquirer function

Chapter 6 – AS2805.6.2 Support – Host Commands

RE/RF Verify a Transaction Request, without PIN

Command:

To verify a transaction Request Message, without PIN, and return the MAC Residue (MARX) for subsequent inclusion in the MAC calculation for the Response Message.

Note:

If the host system is unable to support binary communication then this command will use standard (ASCII) asynchronous mode, in which case the message text is in expanded hexadecimal format.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'RE'
TK	16 H or 1 A + 32 H	Single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
AB Field	16 H	AB field, as defined in AS2805.6.2
EITHER (for binary communication) the following two fields		
Message Length	3 H	Length (in bytes) of the next field; max value X'320
Message Text	n B	Message text; the last 64 bits (8 bytes) contain the MAC field, of which the leftmost 4, 6 or 8 bytes contain the MAC (depends on value of optional MAC Length field)
OR (for standard asynchronous (ASCII) communication) the following two fields		
Message Length	3 H	Length (in characters) of the next field; max value X'320
Message Text	n H	Message text; the last 16 characters contain the MAC field, of which the leftmost 8, 12 or 16 characters contain the MAC (depends on value of optional MAC Length field)
Delimiter	1 A	Optional field; present only if MAC Length field is present; value = ';'
MAC Length	1 N	Optional field; if field not present then value 0 is assumed: 0 = 32-bit MAC (single or double length TK) 1 = 48-bit MAC (double length TK only) 2 = 64-bit MAC (double length TK only)
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional field; must be present if a message trailer is present; value X'19
Message Trailer	n A	Optional field; maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the host unchanged
Response Code	2 A	Value 'RF'
Error Code	2 N	00: No errors 01: MAC verification failure 10: Terminal Key parity error 12: No keys loaded in user storage 13: LMK error – report to Supervisor 15: Error in input data 21: Invalid user storage index 65: Transaction Key Scheme set to None 80: Message length error 90: Communications link parity error 91: Communications link LRC error 92: Transparent asynch data length error
MARX	8 H or 16 H	Encrypted MAC Residue (X) for use in the transaction response message: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
End Message Delimiter	1 C	Optional field; present only if present in the command message; value X'19
Message Trailer	n A	Optional field; present only if present in the command message; maximum length 32 characters

RG/RH Verify a Transaction Request, with PIN, when CD Field Available

Command:

To verify a transaction Request Message, with PIN, and return the encrypted derived Terminal PIN Key (TPK), the PIN block encrypted under the TPK and the MAC Residue (MARX) for subsequent inclusion in the MAC calculation for the Response Message.

Notes:

The output encrypted TPK and PIN block can be used by the Acquirer to verify the PIN using a standard PIN verification command ('DA', 'CG', 'DC' or 'BC').

If the host system is unable to support binary communication then this command will use standard (ASCII) asynchronous mode, in which case the message text is in expanded hexadecimal format.

The PIN Block Pointer field represents the position of the first byte of the PIN block (8 bytes) in the binary representation of the Message Text (it is therefore independent of the communication protocol).

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the host unchanged
Command Code	2 A	Value 'RG'
TK	16 H or 1 A + 32 H	Single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting “Enforce key type 002 separation for PCI HSM compliance” has the value “N”, or under LMK pair 36-37 variant 8 if the setting has the value “Y”.
AB Field	16 H	AB field, as defined in AS2805.6.2
CD Field	16 H	CD field, as defined in AS2805.6.2
PIN Block Pointer	3 H	Pointer to first byte of encrypted PIN block in binary message text; value X’000 to X’310
EITHER (for binary communication) the following two fields		
Message Length	3 H	Length (in bytes) of the next field; max value X’320
Message Text	n B	Message text; the last 64 bits (8 bytes) contain the MAC field, of which the leftmost 4, 6 or 8 bytes contain the MAC (depends on value of optional MAC Length field)
OR (for standard asynchronous (ASCII) communication) the following two fields		
Message Length	3 H	Length (in characters) of the next field; max value X’320
Message Text	n H	Message text; the last 16 characters contain the MAC field, of which the leftmost 8, 12 or 16 characters contain the MAC (depends on value of optional MAC Length field)
Delimiter	1 A	Optional field; present only if MAC Length field is present; value = ';'
MAC Length	1 N	Optional field; if field not present then value 0 is assumed: 0 = 32-bit MAC (single or double length TK) 1 = 48-bit MAC (double length TK only) 2 = 64-bit MAC (double length TK only)
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.

Field	Length and 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	Optional field; must be present if a message trailer is present; value X'19
Message Trailer	n A	Optional field; maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the host unchanged
Response Code	2 A	Value 'RH'
Error Code	2 N	00: No errors 01: MAC verification failure 10: Terminal Key parity error 12: No keys loaded in user storage 13: LMK error – report to Supervisor 15: Error in input data 20: PIN block error 21: Invalid user storage index 65: Transaction Key Scheme set to None 80: Message length error 88: Warning: AS2805.3 "zero" PIN block received 90: Communications link parity error 91: Communications link LRC error 92: Transparent asynch data length error
TPK	16 H or 1 A + 32 H	Derived Terminal PIN Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y".
PIN Block	16 H	PIN block, encrypted under the derived TPK
MARX	8 H or 16 H	Encrypted MAC Residue (X) for use in the transaction response message: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
End Message Delimiter	1 C	Optional field; present only if present in the command message; value X'19
Message Trailer	n A	Optional field; present only if present in the command message; maximum length 32 characters

RI/RJ Verify a Transaction Request, with PIN, when CD Field not Available (*when selected Transaction Key Scheme is Australian*)

Command:

To verify a transaction Request Message, with PIN, and return the encrypted PIN Encipherment Key (PEK), for use in the 'RO' command, and the MAC Residue (MARX) for subsequent inclusion in the MAC calculation for the Response Message.

Notes:

a) This command is only available if Transaction Key Scheme has been set to Australian (using the CS Console command or HSM Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HI Host command can be used, which provides exactly the same functionality as the RI Host command described below.

b) If the host system is unable to support binary communication then this command will use standard (ASCII) asynchronous mode, in which case the message text is in expanded hexadecimal format.

c) This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the host unchanged
Command Code	2 A	Value 'RI'
TK	16 H or 1 A + 32 H	Single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
AB Field	16 H	AB field, as defined in AS2805.6.2
EITHER (for binary communication) the following two fields		
Message Length	3 H	Length (in bytes) of the next field; max value X'320
Message Text	n B	Message text; the last 64 bits (8 bytes) contain the MAC field, of which the leftmost 4, 6 or 8 bytes contain the MAC (depends on value of optional MAC Length field)
OR (for standard asynchronous (ASCII) communication) the following two fields		
Message Length	3 H	Length (in characters) of the next field; max value X'320
Message Text	n H	Message text; the last 16 characters contain the MAC field, of which the leftmost 8, 12 or 16 characters contain the MAC (depends on value of optional MAC Length field)
Delimiter	1 A	Optional field; present only if MAC Length field is present; value = ';'
MAC Length	1 N	Optional field; if field not present then value 0 is assumed: 0 = 32-bit MAC (single or double length TK) 1 = 48-bit MAC (double length TK only) 2 = 64-bit MAC (double length TK only)
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is

Field	Length and Type	Details
		present.
End Message Delimiter	1 C	Optional field; must be present if a message trailer is present; value X'19
Message Trailer	n A	Optional field; maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the host unchanged
Response Code	2 A	Value 'RJ'
Error Code	2 N	00: No errors 01: MAC verification failure 10: Terminal Key parity error 12: No keys loaded in user storage 13: LMK error – report to Supervisor 15: Error in input data 21: Invalid user storage index 65: Transaction Key Scheme set to None 80: Message length error 88: Warning: AS2805.3 "zero" PIN block received 90: Communications link parity error 91: Communications link LRC error 92: Transparent asynch data length error
PEK	16 H or 1 A + 32 H	PIN Encipherment Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y (for use with the "RO" command)
MARX	8 H or 16 H	Encrypted MAC Residue (X) for use in the transaction response message: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
End Message Delimiter	1 C	Optional field; present only if present in the command message; value X'19
Message Trailer	n A	Optional field; present only if present in the command message; maximum length 32 characters

HI/HJ Verify a Transaction Request, with PIN, when CD Field not Available (*when selected Transaction Key Scheme is Racal*)

Command:

To verify a transaction Request Message, with PIN, and return the encrypted PIN Encipherment Key (PEK), for use in the 'RO' command, and the MAC Residue (MARX) for subsequent inclusion in the MAC calculation for the Response Message.

Notes:

a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or HSM Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RI command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 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 Australian, 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 Host Command 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 commandø	Use the Rx variant of the commandø

* As described in the payShield 9000 Host Command Reference Manual

ø As described in this manual

b) If the host system is unable to support binary communication then this command will use standard (ASCII) asynchronous mode, in which case the message text is in expanded hexadecimal format.

c) This command supports Variant LMKs only.

RK/RL Generate Transaction Response, with Auth Para Generated by Acquirer (*when selected Transaction Key Scheme is Australian*)

Command:

To generate a transaction Response Message (when Auth Para is generated by the Acquirer) and to update the Terminal Key.

Notes:

a) This command is only available if Transaction Key Scheme has been set to Australian (using the CS Console command or HSM Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HK Host command can be used, which provides exactly the same functionality as the RK Host command described below. For further details, see Chapter 12 of the *payShield 9000 General Information Manual*.

b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')

c) If the host system is unable to support binary communication then this command will use standard (ASCII) asynchronous mode, in which case the message text is in expanded hexadecimal format.

d) The AT, STAN and CATID Pointer fields represent the position of the first byte of each of the relevant data items in the binary representation of the Message Text (they are therefore independent of the communication protocol). Note that the AT is 6 bytes (12 digits) in length, the STAN is 3 bytes (6 digits) and the CATID is 8 bytes (16 digits).

e) This function can also be used to generate a MAC and update the Terminal Key for an Administration Response Message. In this case the AP Include Flag should be set to 'E'.

f) This command supports Variant LMKs only.

Field	Length and Type	Details
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the host unchanged
Command Code	2 A	Value 'RK'
TK	16 H or 1 A + 32 H	Single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting “Enforce key type 002 separation for PCI HSM compliance” has the value “N”, or under LMK pair 36-37 variant 8 if the setting has the value “Y”.
AB Field	16 H	AB field, as defined in AS2805.6.2
MARX	8 H or 16 H	Encrypted MAC Residue (X) from the transaction request: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
AP Include Flag	1 A	Flag to indicate whether to include Auth Para in the MAC calculation; Value 'I' = include, 'E' = exclude
CD Field	16 H	CD field, as defined in AS2805.6.2; only present if AP Include Flag = 'I'
AT Pointer	3 H	Pointer to first byte of transaction amount in binary message text; value X’000 to X’31A only present if AP Include Flag = 'I'

Field	Length and Type	Details
STAN Pointer	3 H	Pointer to first byte of systems trace audit number in binary message text; value X'000 to X'31D; only present if AP Include Flag = 'I'
CATID Pointer	3 H	Pointer to first byte of card acceptor terminal identification in binary message text; value X'000 to X'318; only present if AP Include Flag = 'I'
EITHER (for binary communication) the following two fields		
Message Length	3 H	X'001 to X'320 indicating the length of the next field.
Message Text	n B	1 to 800 bytes of message.
OR (for standard asynchronous (ASCII) communication) the following two fields		
Message Length	3 H	Length (in characters) of the next field; max value X'320
Message Text	n H	Message text (maximum length = 800 hexadecimal characters, representing 400 bytes)
Delimiter	1 A	Optional field; present only if MAC Length field is present; value = ';'
MAC Length	1 N	Optional field; if field not present then value 0 is assumed: 0 = 32-bit MAC (single or double length TK) 1 = 48-bit MAC (double length TK only) 2 = 64-bit MAC (double length TK only)
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional field; must be present if a message trailer is present; value X'19
Message Trailer	n A	Optional field; maximum length 32 characters

Field	**Length and Type**	**Details**
RESPONSE MESSAGE		
Message Header	m A	Returned to the host unchanged
Response Code	2 A	Value 'RL'
Error Code	2 N	00: No errors 10: Terminal Key parity error 12: No keys loaded in user storage 13: LMK error – report to Supervisor 15: Error in input data 20: PIN block error 21: Invalid user storage index 65: Transaction Key Scheme set to None 80: Message length error 90: Communications link parity error 91: Communications link LRC error 92: Transparent asynch data length error
MARY	8 H or 16 H	Encrypted MAC Residue (Y) from the transaction response: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
MAC	8 H, 12H or 16 H	MAC (length dependent on value of MAC Length field)
New TK	16 H or 1 A + 32 H	New single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
End Message Delimiter	1 C	Optional field; present only if present in the command message; value X'19
Message Trailer	n A	Optional field; present only if present in the command message; maximum length 32 characters

HK/HL Generate Transaction Response, with Auth Para Generated by Acquirer (*when selected Transaction Key Scheme is Racal*)

Command:

To generate a transaction Response Message (when Auth Para is generated by the Acquirer) and to update the Terminal Key.

Notes:

a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or HSM Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RK command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 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 Australian, then the RK Host command (as described in this manual) must be used. (With this setting, the HK command code is as described in the *payShield 9000 Host Command 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 commandØ	Use the Rx variant of the commandØ

* As described in the payShield 9000 Host Command Reference Manual

Ø As described in this manual

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

b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')

c) If the host system is unable to support binary communication then this command will use standard (ASCII) asynchronous mode, in which case the message text is in expanded hexadecimal format.

d) The AT, STAN and CATID Pointer fields represent the position of the first byte of each of the relevant data items in the binary representation of the Message Text (they are therefore independent of the communication protocol). Note that the AT is 6 bytes (12 digits) in length, the STAN is 3 bytes (6 digits) and the CATID is 8 bytes (16 digits).

e) This function can also be used to generate a MAC and update the Terminal Key for an Administration Response Message. In this case the AP Include Flag should be set to 'E'.

f) This command supports Variant LMKs only.

RM/RN Generate Transaction Response with Auth Para Generated by Card Issuer (*when selected Transaction Key Scheme is Australian*)

Command:

To generate a transaction Response Message (when Auth Para has been generated by the Card issuer) and to update the Terminal Key.

Notes:

the CS Console command or HSM Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HM Host command can be used, which provides exactly the same functionality as the RM Host command described below. For further details, see Chapter 12 of the *payShield 9000 General Information Manual*.

b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')

c) If the host system is unable to support binary communication then this command will use standard (ASCII) asynchronous mode, in which case the message text is in expanded hexadecimal format.

d) This command supports Variant LMKs only.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the host unchanged
Command Code	2 A	Value 'RM'
TK	16 H or 1 A + 32 H	Single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting “Enforce key type 002 separation for PCI HSM compliance” has the value “N”, or under LMK pair 36-37 variant 8 if the setting has the value “Y”.
AB Field	16 H	AB field, as defined in AS2805.6.2
MARX	8 H or 16 H	Encrypted MAC Residue (X) from the transaction request: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
AP Include Flag	1 A	Flag to indicate whether to include Auth Para in the MAC calculation; Value 'I' = include, 'E' = exclude; must have value 'I' for double length TK
ZPK	16 H or 1 A + 32 H or 1 A + 48 H	Zone PIN Key, encrypted under LMK pair 06-07; only present if AP Include Flag = 'I'
Auth Para	16 H	Auth Para, encrypted under variant 1 of the ZPK; only present if AP Include Flag = 'I';
EITHER (for binary communication) the following two fields		
Message Length	3 H	Length (in bytes) of the next field; max value X’320
Message Text	n B	Message text (maximum length = 800 bytes)
OR (for standard asynchronous (ASCII) communication) the following two fields		
Message Length	3 H	Length (in characters) of the next field; max value X’320

Message Text	n H	Message text (maximum length = 800 hexadecimal characters, representing 400 bytes)
Delimiter	1 A	Optional field; present only if MAC Length field is present; value = ';'
MAC Length	1 N	Optional field; if field not present then value 0 is assumed: 0 = 32-bit MAC (single or double length TK) 1 = 48-bit MAC (double length TK only) 2 = 64-bit MAC (double length TK only)
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional field; must be present if a message trailer is present; value X’19
Message Trailer	n A	Optional field; maximum length 32 characters

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the host unchanged
Response Code	2 A	Value 'RN'
Error Code	2 N	00: No errors 04: AP include flag error 10: Terminal Key parity error 11: ZPK parity error 12: No keys loaded in user storage 13: LMK error – report to Supervisor 15: Error in input data 21: Invalid user storage index 65: Transaction Key Scheme set to None 80: Message length error 90: Communications link parity error 91: Communications link LRC error 92: Transparent asynch data length error
MARY	8 H or 16 H	Encrypted MAC Residue (Y) from the transaction response: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
MAC	8 H, 12 H or 16 H	MAC (length dependent on value of MAC Length field)
New TK	16 H or 1 A + 32 H	New single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting “Enforce key type 002 separation for PCI HSM compliance” has the value “N”, or under LMK pair 36-37 variant 8 if the setting has the value “Y”.
End Message Delimiter	1 C	Optional field; present only if present in the command message; value X’19
Message Trailer	n A	Optional field; present only if present in the command message; maximum length 32 characters

HM/HN Generate Transaction Response with Auth Para Generated by Card Issuer (*when selected Transaction Key Scheme is Racal*)

Command:

To generate a transaction Response Message (when Auth Para has been generated by the Card issuer) and to update the Terminal Key.

Notes:

a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or HSM Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RM command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 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 Australian, then the RM Host command (as described in this manual) must be used. (With this setting, the HM command code is as described in the *payShield 9000 Host Command 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 commandø	Use the Rx variant of the commandø

* As described in the payShield 9000 Host Command Reference Manual

ø As described in this manual

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

b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')

c) If the host system is unable to support binary communication then this command will use standard (ASCII) asynchronous mode, in which case the message text is in expanded hexadecimal format.

d) This command supports Variant LMKs only.

RO/RP Translate a PIN from PEK to ZPK Encryption (*when selected Transaction Key Scheme is Australian*)

Command:

To translate a PIN block from encryption under Card Key and a PIN Encipherment Key (PEK) to encryption under Card Key and a Zone PIN Key (ZPK).

Notes:

Australian (using the CS Console command or HSM Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HO Host command can be used, which provides exactly the same functionality as the RO Host command described below. For further details, see Chapter 12 of the *payShield 9000 General Information Manual*.

b) This command is used, by the Acquirer, with the 'RI' command. In this case, the Acquirer has no access to the CD field and hence is unable to calculate Card Key.

c) This command is essentially a standard PIN translation command, with the exception that no PIN block validation occurs. The processing described is independent of the AS2805.6.2 standard(s).

d) This command supports Variant LMKs only.

Field	**Length & Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the host unchanged
Command Code	2 A	Value 'RO'
PEK	16 H or 1 A + 32 H	PIN Encipherment Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 7 if the setting has the value "Y". (as returned from the 'RI' command)
ZPK	16 H or 1 A + 32 H or 1 A + 48 H	Zone PIN Key, encrypted under LMK pair 06-07
PIN Block	16 H	PIN block, doubly encrypted with Card Key and PEK
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional field; must be present if a message trailer is present; value X'19
Message Trailer	n A	Optional field; maximum length 32 characters

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the host unchanged
Response Code	2 A	Value 'RP'
Error Code	2 N	00: No errors 10: PEK parity error 11: ZPK parity error 12: No keys loaded in user storage 13: LMK error – report to Supervisor 15: Error in input data 21: Invalid user storage index 65: Transaction Key Scheme set to None
PIN Block	16 H	PIN block, doubly encrypted with Card Key and ZPK
End Message Delimiter	1 C	Optional field; present only if present in the command message; value X'19
Message Trailer	n A	Optional field; present only if present in the command message; maximum length 32 characters

HO/HP Translate a PIN from PEK to ZPK Encryption (*when selected Transaction Key Scheme is Racal*)

Command:

To translate a PIN block from encryption under Card Key and a PIN Encipherment Key (PEK) to encryption under Card Key and a Zone PIN Key (ZPK).

Notes:

a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or HSM Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RO command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 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 Australian, then the RO Host command (as described in this manual) must be used. (With this setting, the HO command code is as described in the *payShield 9000 Host Command 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 commandø	Use the Rx variant of the commandø

* As described in the payShield 9000 Host Command Reference Manual

Ø As described in this manual

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

b) This command is used, by the Acquirer, with the 'RI' command. In this case, the Acquirer has no access to the CD field and hence is unable to calculate Card Key.

c) This command is essentially a standard PIN translation command, with the exception that no PIN block validation occurs. The processing described is independent of the AS2805.6.2 standard(s).

d) This command supports Variant LMKs only.

RQ/RR Verify a Transaction Completion Confirmation (*when selected Transaction Key Scheme is Australian*)

Command:

To verify a transaction Completion Confirmation Message and return the MAC Residue (MARZ) for subsequent inclusion in the MAC calculation for the Completion Response Message.

Notes:

The CS Console command or HSM Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HQ Host command can be used, which provides exactly the same functionality as the RQ Host command described below. For further details, see Chapter 12 of the *payShield 9000 General Information Manual*.

b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')

c) If the host system is unable to support binary communication then this command will use standard (ASCII) asynchronous mode, in which case the message text is in expanded hexadecimal format.

d) This command supports Variant LMKs only.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the host unchanged
Command Code	2 A	Value 'RQ'
TK	16 H or 1 A + 32 H	Single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
AB Field	16 H	AB field, as defined in AS2805.6.2
MARY	8 H or 16 H	Encrypted MAC Residue (Y) from the transaction response: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
EITHER (for binary communication) the following two fields		
Message Length	3 H	Length (in bytes) of the next field; max value X'320
Message Text	n B	Message text; the last 64 bits (8 bytes) contain the MAC field, of which the leftmost 4, 6 or 8 bytes contain the MAC (depends on value of optional MAC Length field)
OR (for standard asynchronous (ASCII) communication) the following two fields		
Message Length	3 H	Length (in characters) of the next field; max value X'320
Message Text	n H	Message text; the last 16 characters contain the MAC field, of which the leftmost 8, 12 or 16 characters contain the MAC (depends on value of optional MAC Length field)
Delimiter	1 A	Optional field; present only if MAC Length field is present; value = ';'
MAC Length	1 N	Optional field; if field not present then value 0 is assumed: 0 = 32-bit MAC (single or double length TK) 1 = 48-bit MAC (double length TK only)

Field	Length & Type	Details
		2 = 64-bit MAC (double length TK only)
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	Optional field; must be present if a message trailer is present; value X'19
Message Trailer	n A	Optional field; maximum length 32 characters

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the host unchanged
Response Code	2 A	Value 'RR'
Error Code	2 N	00: No errors 01: MAC verification failure 10: Terminal Key parity error 12: No keys loaded in user storage 13: LMK error – report to Supervisor 15: Error in input data 21: Invalid user storage index 80: Message length error 65: Transaction Key Scheme set to None 90: Communications link parity error 91: Communications link LRC error 92: Transparent asynch data length error
MARZ	8 H or 16 H	Encrypted MAC Residue (Z) for use in the completion response message: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
End Message Delimiter	1 C	Optional field; present only if present in the command message; value X'19
Message Trailer	n A	Optional field; present only if present in the command message; maximum length 32 characters

HQ/HR Verify a Transaction Completion Confirmation (*when selected Transaction Key Scheme is Racal*)

Command:

To verify a transaction Completion Confirmation Message and return the MAC Residue (MARZ) for subsequent inclusion in the MAC calculation for the Completion Response Message.

Notes:

a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or HSM Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RQ command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 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 Australian, then the RQ Host command (as described in this manual) must be used. (With this setting, the HQ command code is as described in the *payShield 9000 Host Command 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 commandø	Use the Rx variant of the commandø

* As described in the payShield 9000 Host Command Reference Manual

Ø As described in this manual

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

b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')

c) If the host system is unable to support binary communication then this command will use standard (ASCII) asynchronous mode, in which case the message text is in expanded hexadecimal format.

d) This command supports Variant LMKs only.

RS/RT Generate a Transaction Completion Response (*when selected Transaction Key Scheme is Australian*)

Command:

To generate a transaction Completion Response Message.

Notes:

a) This command is only available if Transaction Key Scheme has been set to Australian (using the CS Console command or HSM Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HS Host command can be used, which provides exactly the same functionality as the RS Host command described below. For further details, see Chapter 12 of the *payShield 9000 General Information Manual*.

b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')

c) If the host system is unable to support binary communication then this command will use standard (ASCII) asynchronous mode, in which case the message text is in expanded hexadecimal format.

d) This command supports Variant LMKs only.

Field	**Length & Type**	**Details**
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the host unchanged
Command Code	2 A	Value 'RS'
TK	16 H or 1 A + 32 H	Single or double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
AB Field	16 H	AB field, as defined in AS2805.6.2
MARZ	8 H or 16 H	Encrypted MAC Residue (Z) from the transaction completion confirmation request: 8 hex characters if TK is single length, encrypted under LMK 10 16 hex characters if TK is double length, encrypted under LMK pair 10-11
EITHER (for binary communication) the following two fields		
Message Length	3 H	Length (in bytes) of the next field; max value X'320
Message Text	n B	Message text (maximum length = 800 bytes)
OR (for standard asynchronous (ASCII) communication) the following two fields		
Message Length	3 H	Length (in characters) of the next field; max value X'320
Message Text	n H	Message text (maximum length = 800 hexadecimal characters, representing 400 bytes)
Delimiter	1 A	Optional field; present only if MAC Length field is present; value = ';'
MAC Length	1 N	Optional field; if field not present then value 0 is assumed: 0 = 32-bit MAC (single or double length TK) 1 = 48-bit MAC (double length TK only) 2 = 64-bit MAC (double length TK only)
Delimiter	1 A	Value '%'. Optional; if present, the following field must 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	Optional field; must be present if a message trailer is present; value X'19
Message Trailer	n A	Optional field; maximum length 32 characters

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the host unchanged
Response Code	2 A	Value 'RT'
Error Code	2 N	00: No errors 10: Terminal Key parity error 12: No keys loaded in user storage 13: LMK error – report to Supervisor 15: Error in input data 21: Invalid user storage index 65: Transaction Key Scheme set to None 80: Message length error 90: Communications link parity error 91: Communications link LRC error 92: Transparent asynch data length error
MAC	8 H, 12 H or 16 H	MAC (length dependent on value of MAC Length field)
End Message Delimiter	1 C	Optional field; present only if present in the command message; value X'19
Message Trailer	n A	Optional field; present only if present in the command message; maximum length 32 characters

HS/HT Generate a Transaction Completion Response (*when selected Transaction Key Scheme is Racal*)

Command:

To generate a transaction Completion Response Message.

Notes:

a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or HSM Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RS command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 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 Australian, then the RS Host command (as described in this manual) must be used. (With this setting, the HS command code is as described in the *payShield 9000 Host Command 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 commandø	Use the Rx variant of the commandø

* As described in the payShield 9000 Host Command Reference Manual

ø As described in this manual

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

b) The Terminal Key used in this command is the original Terminal Key used when the initial Request Message was processed (see Commands 'RE', 'RG' and 'RI')

c) If the host system is unable to support binary communication then this command will use standard (ASCII) asynchronous mode, in which case the message text is in expanded hexadecimal format.

d) This command supports Variant LMKs only.

QQ/QR Verify a PIN at Card Issuer using IBM Method

Command:

To verify a PIN at the Card Issuer, using the IBM 3624 method and return Auth Para.

Notes:

The PIN block input to this command is doubly encrypted with Card Key and a Zone PIN Key (ZPK).

The input fields for this command are identical to those for the original 'QQ' command, as defined in the 40-1018-02 specification (Ref.4). Thus, an optional field ("Processing Flag") has been included. If the field is not present then the original processing occurs. If the field is present then either the original processing or the new processing described in this document occurs, depending on the value of the field.

If a double or triple length PVK is used in this command then processing will continue as normal, but a different error code ('02') will be returned.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the host unchanged
Command Code	2 A	Value 'QQ'
ZPK(S)	16 H or 1 A + 32 H or 1 A + 48 H	Source Zone PIN Key, encrypted under LMK pair 06-07
ZPK(D)	16 H or 1 A + 32 H or 1 A + 48 H	Destination Zone PIN Key, encrypted under LMK pair 06-07
PVK	16 H or 1 A + 32 H or 1 A + 48 H	PIN Verification Key, encrypted under LMK pair 14-15 variant 0
AB Field	16 H	AB field, as defined in AS2805.6.2
CD Field	16 H	CD field, as defined in AS2805.6.2
STAN	6 N	Systems trace audit number
CATID	16 H	Card acceptor terminal identification
AT	12 H	Transaction amount
Maximum PIN Length	2 N	Value = 12
PIN Block	16 H	PIN block, doubly encrypted with Card Key and ZPK(S)
PIN Block Format Code	2 N	Valid formats are: 01, 05 & 46
Check Length	2 N	Minimum PIN length
Account Number	12 N	Rightmost 12 digits of the card account number, excluding the check digit
Decimalization Table	16 N or 1 A + 3 H	16 N if console CS cmd is set for Plaintext decimalisation tables. 'K' + 3 H if the decimalization table is held in the HSM's User Storage Area
PIN Validation Data	16 H	The 16 character field used as input to the IBM PIN

Field	Length and Type	Details
		verification algorithm
Offset	12 H	PIN offset, left justified and padded with X'F
Delimiter	1 A	Optional field, if present then the following field is present. value = ';'
Processing Flag	1 N	Optional field; if not present then value = 0 is assumed; values: 0 = old processing (1988 standard) 1 = new processing (2002 standard)
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional field; must be present if a message trailer is present; value X'19
Message Trailer	n A	Optional field; maximum length 32 characters

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the host unchanged
Response Code	2 A	Value 'QR'
Error Code	2 N	00: No errors 01: PIN verification failure 02: Warning: PVK not single length (PIN OK) 10: ZPK(S) parity error 11: ZPK(D) or PVK parity error 12: No keys loaded in user storage 13: LMK error – report to Supervisor 15: Error in input data 20: PIN block error 21: Invalid user storage index 23: Invalid PIN block format code 24: PIN length error 25: Invalid decimalization table 65: Transaction Key Scheme set to None
Auth Para	16 H	Auth Para, encrypted under variant 1 of ZPK(D)
End Message Delimiter	1 C	Optional field; present only if present in the command message; value X'19
Message Trailer	n A	Optional field; present only if present in the command message; maximum length 32 characters

QS/QT Verify a PIN at Card Issuer using the Diebold Method

Command:

To verify a PIN at the Card Issuer, using the Diebold method and return Auth Para.

Notes:

The PIN block input to this command is doubly encrypted with Card Key and a Zone PIN Key (ZPK).

The input fields for this command are identical to those for the original 'QS' command, as defined in the 40-1018-02 specification (Ref.9). Thus, an optional field ("Processing Flag") has been included. If the field is not present then the original processing occurs. If the field is present then either the original processing or the new processing described in this document occurs, depending on the value of the field.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the host unchanged
Command Code	2 A	Value 'QS'
ZPK(S)	16 H or 1 A + 32 H or 1 A + 48 H	Source Zone PIN Key, encrypted under LMK pair 06-07
ZPK(D)	16 H or 1 A + 32 H or 1 A + 48 H	Destination Zone PIN Key, encrypted under LMK pair 06-07
AB Field	16 H	AB field, as defined in AS2805.6.2
CD Field	16 H	CD field, as defined in AS2805.6.2
STAN	6 N	Systems trace audit number
CATID	16 H	Card acceptor terminal identification
AT	12 H	Transaction amount
Index Flag	1 A	Value 'K'
Index Pointer	3 N	Index to stored Diebold table
Algorithm Number	2 N	Diebold algorithm required
PIN Block	16 H	PIN block, doubly encrypted with Card Key and ZPK(S)
PIN Block Format Code	2 N	Valid formats are: 01, 05 & 46
Account Number	12 N	Rightmost 12 digits of the card account number, excluding the check digit
PIN Validation Data	20 H	The 20 character field used as input to the PIN verification algorithm
Offset	4 N	PIN offset
Delimiter	1 A	Optional field, if present then the following field is present. value = ';'
Processing Flag	1 N	Optional field; if not present then value = 0 is assumed; values: 0 = old processing (1988 standard) 1 = new processing (see this document)
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.

Field	Length and 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	Optional field; must be present if a message trailer is present; value X'19
Message Trailer	n A	Optional field; maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the host unchanged
Response Code	2 A	Value 'QT'
Error Code	2 N	00: No errors 01: PIN verification failure 10: ZPK(S) parity error 11: ZPK(D) or PVK parity error 12: No keys loaded in user storage 13: LMK error – report to Supervisor 15: Error in input data 20: PIN block error 21: Invalid user storage index 23: Invalid PIN block format code 24: PIN length error 65: Transaction Key Scheme set to None
Auth Para	16 H	Auth Para, encrypted under variant 1 of ZPK(D)
End Message Delimiter	1 C	Optional field; present only if present in the command message; value X'19
Message Trailer	n A	Optional field; present only if present in the command message; maximum length 32 characters

QU/QV Verify a PIN at Card Issuer using Visa Method

Command:

To verify a PIN at the Card Issuer, using the Visa method and return Auth Para.

Notes:

The PIN block input to this command is doubly encrypted with Card Key and a Zone PIN Key (ZPK).

The input fields for this command are identical to those for the original 'QU' command, as defined in the 40-1018-02 specification (Ref.4). Thus, an optional field ("Processing Flag") has been included. If the field is not present then the original processing occurs. If the field is present then either the original processing or the new processing described in this document occurs, depending on the value of the field.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the host unchanged
Command Code	2 A	Value 'QU'
ZPK(S)	16H or 1 A + 32 H or 1 A + 48 H	Source Zone PIN Key, encrypted under LMK pair 06-07
ZPK(D)	16 H or 1 A + 32 H or 1 A + 48 H	Destination Zone PIN Key, encrypted under LMK pair 06-07
PVK	32 H or 1 A + 32 H	PIN Verification Key, encrypted under LMK pair 14-15 variant 0
AB Field	16 H	AB field, as defined in AS2805.6.2
CD Field	16 H	CD field, as defined in AS2805.6.2
STAN	6 N	Systems trace audit number
CATID	16 H	Card acceptor terminal identification
AT	12 H	Transaction amount
PIN Block	16 H	PIN block, doubly encrypted with Card Key and ZPK(S)
PIN Block Format Code	2 N	Valid formats are: 01, 05 & 46
Account Number	12 N	Rightmost 12 digits of the card account number, excluding the check digit
PVKI	1 N	PVK indicator; value 0 to 6
PVV	4 N	PIN verification value
Delimiter	1 A	Optional field, if present then the following field is present. value = ';'
Processing Flag	1 N	Optional field; if not present then value = 0 is assumed; values: 0 = old processing (1988 standard) 1 = new processing (see this document)
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is

Field	Length and Type	Details
		present.
End Message Delimiter	1 C	Optional field; must be present if a message trailer is present; value X'19
Message Trailer	n A	Optional field; maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the host unchanged
Response Code	2 A	Value 'QV'
Error Code	2 N	00: No errors 01: PIN verification failure 10: ZPK(S) parity error 11: ZPK(D) or PVK parity error 12: No keys loaded in user storage 13: LMK error – report to Supervisor 15: Error in input data 20: PIN block error 21: Invalid user storage index 23: Invalid PIN block format code 24: PIN length error 27: PVK not double length 65: Transaction Key Scheme set to None
Auth Para	16 H	Auth Para, encrypted under variant 1 of ZPK(D)
End Message Delimiter	1 C	Optional field; present only if present in the command message; value X'19
Message Trailer	n A	Optional field; present only if present in the command message; maximum length 32 characters

QW/QX Verify a PIN at Card Issuer using the Comparison Method

Command:

To verify a PIN at the Card Issuer, using the Comparison method and return Auth Para.

Notes:

The PIN block input to this command is doubly encrypted with Card Key and a Zone PIN Key (ZPK).

The input fields for this command are identical to those for the original 'QW' command, as defined in the 40-1018-02 specification (Ref.4). Thus, an optional field ("Processing Flag") has been included. If the field is not present then the original processing occurs. If the field is present then either the original processing or the new processing described in this document occurs, depending on the value of the field.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the host unchanged
Command Code	2 A	Value 'QW'
ZPK(S)	16 H or 1 A + 32 H or 1 A + 48 H	Source Zone PIN Key, encrypted under LMK pair 06-07
ZPK(D)	16 H or 1 A + 32 H or 1 A + 48 H	Destination Zone PIN Key, encrypted under LMK pair 06-07
AB Field	16 H	AB field, as defined in AS2805.6.2
CD Field	16 H	CD field, as defined in AS2805.6.2
STAN	6 N	Systems trace audit number
CATID	16 H	Card acceptor terminal identification
AT	12 H	Transaction amount
PIN Block	16 H	PIN block, doubly encrypted with Card Key and ZPK(S)
PIN Block Format Code	2 N	Valid formats are: 01, 05 & 46
Account Number	12 N	Rightmost 12 digits of the card account number, excluding the check digit
Encrypted PIN	L N	PIN, encrypted using the account number and LMK pair 02-03, stored on host database
Delimiter	1 A	Optional field, if present then the following field is present. value = ';'
Processing Flag	1 N	Optional field; if not present then value = 0 is assumed; values: 0 = old processing (1988 standard) 1 = new processing (see this document)
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional field; must be present if a message trailer is

Field	Length and Type	Details
		present; value X’19
Message Trailer	n A	Optional field; maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the host unchanged
Response Code	2 A	Value 'QX'
Error Code	2 N	00: No errors 01: PIN verification failure 10: ZPK(S) parity error 11: ZPK(D) parity error 12: No keys loaded in user storage 13: LMK error – report to Supervisor 14: Database PIN error 15: Error in input data 20: PIN block error 21: Invalid user storage index 23: Invalid PIN block format code 24: PIN length error 65: Transaction Key Scheme set to None
Auth Para	16 H	Auth Para, encrypted under variant 1 of ZPK(D)
End Message Delimiter	1 C	Optional field; present only if present in the command message; value X’19
Message Trailer	n A	Optional field; present only if present in the command message; maximum length 32 characters

RU/RV Generate Auth Para at the Card Issuer (when selected Transaction Key Scheme is Australian)

Command:

To generate Auth Para at the Card Issuer and return it encrypted under variant 1 of a Zone PIN Key (ZPK).

Notes:

a) This command is only available if Transaction Key Scheme has been set to Australian (using the CS Console command or HSM Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HU Host command can be used, which provides exactly the same functionality as the RU Host command described below. For further details, see Chapter 12 of the *payShield 9000 General Information Manual*.

b) This command allows the Card Issuer to generate Auth Para when no PIN is to be verified, but the CD fields are not known to the Acquirer.

c) The input fields for this command are identical to those for the original 'RU' command, as defined in the 40-1018-02 specification (Ref.4). Thus, an optional field ("Processing Flag") has been included. If the field is not present then the original processing occurs. If the field is present then either the original processing or the new processing described in this document occurs, depending on the value of the field.

d) This command supports Variant LMKs only.

Field	**Length and Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the host unchanged
Command Code	2 A	Value 'RU'
ZPK	16 H or 1 A + 32 H or 1 A + 48 H	Zone PIN Key, encrypted under LMK pair 06-07
AB Field	16 H	AB field, as defined in AS2805.6.2
CD Field	16 H	CD field, as defined in AS2805.6.2
STAN	6 N	Systems trace audit number
CATID	16 H	Card acceptor terminal identification
AT	12 H	Transaction amount
Delimiter	1 A	Optional field, if present then the following field is present. value = ';'
Processing Flag	1 N	Optional field; if not present then value = 0 is assumed; values: 0 = old processing (1988 standard) 1 = new processing (see this document)
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional field; must be present if a message trailer is present; value X'19
Message Trailer	n A	Optional field; maximum length 32 characters
Field	**Length and Type**	**Details**
	RESPONSE MESSAGE	
Message Header	m A	Returned to the host unchanged
Response Code	2 A	Value 'RV'

Field	**Length and Type**	**Details**
Error Code	2 N	00: No errors 10: ZPK parity error 12: No keys loaded in user storage 13: LMK error – report to Supervisor 15: Error in input data 21: Invalid user storage index 65: Transaction Key Scheme set to None 90: Communications link parity error 91: Communications link LRC error 92: Transparent asynch data length error
Auth Para	16 H	Auth Para, encrypted under LMK pair 06-07 variant 1
End Message Delimiter	1 C	Optional field; present only if present in the command message; value X'19
Message Trailer	n A	Optional field; present only if present in the command message; maximum length 32 characters

HU/HV Generate Auth Para at the Card Issuer (*when selected Transaction Key Scheme is Racal*)

Command:

To generate Auth Para at the Card Issuer and return it encrypted under variant 1 of a Zone PIN Key (ZPK).

Notes:

a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or HSM Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RU command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 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 Australian, then the RU Host command (as described in this manual) must be used. (With this setting, the HU command code is as described in the *payShield 9000 Host Command 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 commandØ	Use the Rx variant of the commandØ

* As described in the payShield 9000 Host Command Reference Manual

Ø As described in this manual

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

b) This command allows the Card Issuer to generate Auth Para when no PIN is to be verified, but the CD fields are not known to the Acquirer.

c) The input fields for this command are identical to those for the original 'RU' command, as defined in the 40-1018-02 specification (Ref.4). Thus, an optional field (“Processing Flag”) has been included. If the field is not present then the original processing occurs. If the field is present then either the original processing or the new processing described in this document occurs, depending on the value of the field.

d) This command supports Variant LMKs only.

RW/RX Generate an Initial Terminal Key (when selected Transaction Key Scheme is Australian)

Command:

To generate an initial double length Terminal Key (TK) and return the result encrypted under the appropriate LMK pair.

Note:

a) This command is only available if Transaction Key Scheme has been set to Australian (using the CS Console command or HSM Manager Initial Settings). If access to this functionality is required when Transaction Key Scheme has been set to Racal then the HW Host command can be used, which provides exactly the same functionality as the RW Host command described below. For further details, see Chapter 12 of the *payShield 9000 General Information Manual*.

b) This command uses a previously established double length Acquirer Initialization Key (KIA) and the Card Acceptor Terminal Identification (CATID) to generate the initial TK for the terminal.

c) This command supports Variant LMKs only.

Field	**Length and Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the host unchanged
Command Code	2 A	Value 'RW'
KIA	1 A + 32 H	Double length Acquirer Initialization Key, encrypted under LMK pair 14-15 variant 6
CATID	16 H	Card acceptor terminal identification
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Optional field; must be present if a message trailer is present; value X'19
Message Trailer	n A	Optional field; maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the host unchanged
Response Code	2 A	Value 'RX'
Error Code	2 N	00: No errors 10: KIA parity error 12: No keys loaded in user storage 13: LMK error – report to Supervisor 15: Error in input data 21: Invalid user storage index 65: Transaction Key Scheme set to None
Initial TK	1 A + 32 H	Initial double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
End Message Delimiter	1 C	Optional field; present only if present in the command message; value X'19
Message Trailer	n A	Optional field; present only if present in the command message; maximum length 32 characters

HW/HX Generate an Initial Terminal Key (when selected Transaction Key Scheme is Racal)

Command:

To generate an initial double length Terminal Key (TK) and return the result encrypted under the appropriate LMK pair.

Note:

a) This command code should be used where the Transaction Key Scheme has been set to Racal (using the CS Console command or HSM Manager Initial Settings) but it is also required to process commands for the Australian Transaction Key Scheme.

In this environment, the HI commands acts exactly like the RW command described in this manual. This allows both Australian and Racal Transaction Key Schemes to be used on the same payShield 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 Australian, then the RW Host command (as described in this manual) must be used. (With this setting, the HW command code is as described in the *payShield 9000 Host Command 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 commandø	Use the Rx variant of the commandø

* As described in the payShield 9000 Host Command Reference Manual

ø As described in this manual

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

b) This command uses a previously established double length Acquirer Initialization Key (KIA) and the Card Acceptor Terminal Identification (CATID) to generate the initial TK for the terminal.

c) This command supports Variant LMKs only.

QM/QN Data Encryption Using a Derived Privacy Key

Command:

To encrypt a block of data, using a double length Privacy Key (KP) derived from the Terminal Key (KT), the Systems Trace Audit Number (STAN) and the Card Acceptor Terminal Identification (CATID).

Notes:

The modes of encryption supported by this command are Electronic Codebook (ECB), Cipher Block Chaining (CBC), 8-bit Cipher Feedback (CFB-8), and OFB (8-bit or 8-byte) - see AS2805.5.2 (Ref.8.2).

The HSM input and output buffers can support 2K bytes of data. It is recommended that the Plaintext Data field in the command message is no greater than 1800 bytes.

If the Host communication link is configured for standard asynchronous communications then the input Plaintext Data and the output Encrypted Data will be in expanded hexadecimal format, with two hexadecimal characters representing each 8 bits of data. Thus 400 bytes of data would be represented by 800 hexadecimal characters.

If the Host communication link is configured for transparent asynchronous communications then the input Plaintext Data and the output Encrypted Data will be in binary format, with each byte representing 8 bits of data.

The Plaintext Data field must be an exact multiple of 16 hexadecimal characters if standard asynchronous communications are used or an exact multiple of 8 bytes if the transparent asynchronous mode is used. The Encrypted Data field will be the same length as the Plaintext Data field.

This command supports Variant LMKs only.

Field	Length and Type	Details
COMMAND MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'QM'
TK	1 A + 32 H	Double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
STAN	6 N	Systems Trace Audit Number
CATID	16 H	Card Acceptor Terminal Identification
Encryption Mode	1 N	Flag to indicate the mode of encryption 0 = ECB mode of encryption 1 = CBC mode of encryption 2 = CFB-8 mode of encryption 3 = OFB mode of encryption
Initialization Value	16 H	Initialization value, used when Encryption Mode = 1, 2 or 3 (CBC, CFB-8 or OFB)
Plaintext Value (j)	1 N	Only used when Encryption Mode = 3 (OFB); j = 1 for 8-bit feedback or j = 8 for 8-byte (64-bit) feedback
Length	3 H	Length (in bytes) of data to be encrypted
Plaintext Data	n H or n B	Data to be encrypted (asynchronous mode) Data to be encrypted (transparent asynchronous mode)
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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
RESPONSE MESSAGE		
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'QN'
Error Code	2 N	00 - No errors 10 - TK parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index 65: Transaction Key Scheme set to None 80 - Invalid data length
Encrypted Data	n H or n B	Encrypted data (asynchronous mode) Encrypted data (transparent asynchronous mode)
OCV	16 H	Output Chaining Value, only returned when Encryption Mode = 3 (OFB)
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

QO/QP Data Decryption Using a Derived Privacy Key

Command:

To decrypt a block of data, using a double length Privacy Key (KP) derived from the Terminal Key (KT), the Systems Trace Audit Number (STAN) and the Card Acceptor Terminal Identification (CATID).

Notes:

The modes of encryption supported by this command are Electronic Codebook (ECB), Cipher Block Chaining (CBC), 8-bit Cipher Feedback (CFB-8), and OFB (8-bit or 8-byte) - see AS2805.5.2 (Ref.8.2).

The HSM input and output buffers can support 2K bytes of data. It is recommended that the Encrypted Data field in the command message is no greater than 1800 bytes.

If the Host communication link is configured for standard asynchronous communications then the input Encrypted Data and the output Plaintext Data will be in expanded hexadecimal format, with two hexadecimal characters representing each 8 bits of data. Thus 400 bytes of data would be represented by 800 hexadecimal characters.

If the Host communication link is configured for transparent asynchronous communications then the input Encrypted Data and the output Plaintext Data will be in binary format, with each byte representing 8 bits of data.

The Encrypted Data field must be an exact multiple of 16 hexadecimal characters if standard asynchronous communications are used or an exact multiple of 8 bytes if the transparent asynchronous mode is used. The output Plaintext Data field will be the same length as the Encrypted Data field.

This command supports Variant LMKs only.

Field	Length and Type	Details
	COMMAND MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Command Code	2 A	Value 'QO'
TK	1 A + 32 H	Double length Terminal Key, encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", or under LMK pair 36-37 variant 8 if the setting has the value "Y".
STAN	6 N	Systems Trace Audit Number
CATID	16 H	Card Acceptor Terminal Identification
Encryption Mode	1 N	Flag to indicate the mode of encryption 0 = ECB mode of encryption 1 = CBC mode of encryption 2 = CFB-8 mode of encryption 3 = OFB mode of encryption
Initialization Value	16 H	Initialization value, used when Encryption Mode = 1, 2 or 3 (CBC, CFB-8 or OFB)
Plaintext Value (j)	1 N	Only used when Encryption Mode = 3 (OFB); j = 1 for 8-bit feedback or j = 8 for 8-byte (64-bit) feedback
Length	3 H	Length (in bytes) of data to be decrypted
Encrypted Data	n H or n B	Data to be decrypted (asynchronous mode) Data to be decrypted (transparent asynchronous mode)

Field	Length and 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	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters

Field	Length and Type	Details
	RESPONSE MESSAGE	
Message Header	m A	Will be returned to the Host unchanged
Response Code	2 A	Value 'QP'
Error Code	2 N	00 - No errors 10 - TK parity error 12 - No keys loaded in user storage 13 - LMK error; report to supervisor 15 - Error in input data 21 - Invalid user storage index 65: Transaction Key Scheme set to None 80 - Invalid data length
Plaintext Data	n H or n B	Decrypted data (asynchronous mode) Decrypted data (transparent asynchronous mode)
OCV	16 H	Output Chaining Value, only returned when Encryption Mode = 3 (OFB)
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters

Appendix A – One-Way Functions

OWF - 1988

One-way functions for single and double length keys are defined as follows:

Single Length Key

Let K be a single length key and let D be a 64-bit data block.

Step 1 Decrypt D with K.

Step 2 Combine the result of Step 1 with D using the exclusive-or operation.

The result of Step 2 is the required value, denoted OWF(K,D).

Double Length Key

Let *K be a double length key and let D be a 64-bit data block.

Step 1 Decrypt D with the left half of *K.

Step 2 Encrypt the result of Step 1 with the right half of *K.

Step 3 Decrypt the result of Step 2 with the left half of *K.

Step 4 Combine the result of Step 3 with D using the exclusive-or operation.

The result of Step 4 is the required value, denoted *OWF(*K,D).

OWF - 2000

Described in Appendix N.

Appendix B – Derivation of the Privacy Key

The Privacy Key (denoted KD) is derived from the Transaction Key (KT) and two 64-bit fields (known as the E Field and the F Field) as described below.

The E Field is derived from the Systems Trace Audit Number (STAN) and the F Field is derived from the Card Acceptor Terminal Identification (CATID) as follows:

E Field: The 6 digits (24 bits) of the STAN, left justified and right zero filled to a total length of 64 bits, shifted left 1 bit.

F Field: The 16 characters (64 bits) of the CATID, shifted left 1 bit and zero filled.

Step 1 Combine the E Field and the F Field using the exclusive-or operation.

Step 2 Combine the KT and the constant value 2222222222222222 (hex) using the exclusive-or operation.

Step 3 The KD is the result of the OWF (see Appendix A) with the result of step 1 as the key and the result of step 2 as the data.

Appendix C – Key Check Value

Check values for single and double length keys are defined as follows:

Single Length Key

Let K be a single length key.

Step 1 Encrypt a block of 64 binary zeros with K.

The leftmost 24 bits of the result of Step 1 is the required check value, denoted KCV(K).

Double Length Key

Let K be a double length key.

Step 1 Encrypt a block of 64 binary zeros with the left half of K.

Step 2 Decrypt the result of Step 1 with the right half of K.

Step 3 Encrypt the result of Step 2 with the left half of K.

The leftmost 24 bits of the result of Step 3 is the required check value, denoted KCV(K).

See Ref.8.4 - AS2805.6.3,

See Ref.8.5 - AS2805.6.4,

Appendix D – Key Encrypting Key Variants

Different variants of key encrypting keys (ZMK or TMK) are required to encrypt different types of session keys during distribution between communicating entities. These variants are defined as follows:

NOTE: The variant used is determined by the length of the key being encrypted, NOT the length of the key performing the encryption

Zone or Terminal Authentication keys

ZAK / TAK (Variant A)

variant Single length = 2424 2424 2424 2424 (hex)

variant Double length = 2424 2424 2424 2424 2424 2424 2424 2424 (hex)

variant Triple length = N /A

ZAKs / TAKs (Variant B)

Generate variant Single Length = 2424 2424 2424 2424 (hex)

Generate variant Double Length = 24C0 24C0 24C0 24C0 24C0 24C0 24C0 24C0 (hex)

Generate variant Triple Length = 2430 2430 2430 2430 2430 2430 2430 2430 2430 2430 2430 2430 (hex)

ZAKr / TAKr (Variant C)

Verify variant Single Length = 4848 4848 4848 4848 (hex)

Verify variant Double Length = 48C0 48C0 48C0 48C0 48C0 48C0 48C0 48C0 (hex)

Verify variant Triple Length = 4830 4830 4830 4830 4830 4830 4830 4830 4830 4830 4830 4830 (hex)

Zone or Terminal Encryption keys

ZEK / TEK (Variant E)

variant Single Length= 2222 2222 2222 2222 (hex)

variant Double Length = 2222 2222 2222 2222 2222 2222 2222 2222 (hex)

variant Triple Length = N / A

ZEKs / TEKs (Variant F)

Encipher variant Single Length = 2222 2222 2222 2222 (hex)

Encipher variant Double Length = 22C0 22C0 22C0 22C0 22C0 22C0 22C0 22C0 (hex)

Encipher variant Triple Length = 2230 2230 2230 2230 2230 2230 2230 2230 2230 2230 2230 2230 (hex)

ZEKr / TEKr / KA / KCA (Variant G)

Decipher variant Single Length = 4444 4444 4444 4444 (hex)

Decipher variant Double Length = 44C0 44C0 44C0 44C0 44C0 44C0 44C0 44C0 (hex)

Decipher variant Triple Length = 4430 4430 4430 4430 4430 4430 4430 4430 4430 4430 4430 4430 (hex)

Zone or Terminal PIN keys (ZPK or TPK) (Variant H)

variant Single Length = 2828 2828 2828 2828 (hex)

variant Double Length = 28C0 28C0 28C0 28C0 28C0 28C0 28C0 28C0 (hex)

variant Triple Length = 2830 2830 2830 2830 2830 2830 2830 2830 2830 2830 2830 2830 (hex)

Zone or Terminal PIN keys (ZPK or TPK) (Alternate Variant Hb)

variant Single Length = 4242 4242 4242 4242 (hex)

variant Double Length = 42C0 42C0 42C0 42C0 42C0 42C0 42C0 42C0 (hex)

variant Triple Length = 4230 4230 4230 4230 4230 4230 4230 4230 4230 4230 4230 4230 (hex)

Variant 7 (Variant I)

variant Single Length = 8282 8282 8282 8282 (hex)

variant Double Length = 8282 8282 8282 8282 8282 8282 8282 8282 (hex)

variant Triple Length = N /A

Note: When key scheme type is H

variant Double Length = 82C0 82C0 82C0 82C0 82C0 82C0 82C0 82C0 (hex)

Variant 8 (Variant J)

variant Single Length = 8484 8484 8484 8484 (hex)

variant Double Length = 8484 8484 8484 8484 8484 8484 8484 8484 (hex)

variant Triple Length = N /A

Note: When key scheme type is H

variant Double Length = 84C0 84C0 84C0 84C0 84C0 84C0 84C0 84C0 (hex)

Variant 88 (Variant K)

variant = 88888888888888888888888888888888 (hex)
{Used for enciphering PPASN under KIA}

In each case the appropriate variant is combined with the double length key encrypting key using the exclusive-or operation and the result is used to encrypt the session key.

Variant 0 (Variant M)

variant = 00000000 00000000 00000000 00000000 (hex)
{Used for enciphering TMK* under KIA}

In each case the appropriate variant is combined with the double length key encrypting key using the exclusive-or operation and the result is used to encrypt the session key.

Appendix G – Definition of Card Values

Card Values CV_1 - CV_5 are generated from four values, each 8 hexadecimal characters in length, known as the A Field, B Field, C Field and D Field.

CV_1 - CV_5 are formed from the concatenation of pairs of these fields as follows:

CV_1: concatenation of A and B

CV_2: concatenation of B and A

CV_3: concatenation of A and C

CV_4: concatenation of B and D

CV_5: concatenation of C and D

See Ref.8.5 - AS2805.6.4,.

Appendix H – Generation of Initial Terminal Master Keys

Initial double length Terminal Master Keys (TMKs) are derived from the Card Values CV_1 - CV_6 and the PIN Pad Acquirer Security Number (PPASN). CV_1 - CV_5 are derived from the A, B, C and D Fields, as defined in Appendix G.

Step 1 - Derive a Temporary TMK_1

This value is formed from the concatenation of OWF(CV_6,CV_1) and OWF(CV_6,CV_5), where OWF(K,D) is defined in Appendix A.

Step 2 - Derive a Temporary TMK_2

This value is formed from the concatenation of OWF(CV_6,CV_2) and OWF(CV_6,CV_4), where OWF(K,D) is defined in Appendix A.

Step 3 - Form Initial TMK_1

Let K_L and K_R denote, respectively, the left and right halves of the result of Step 1. The Initial TMK_1 is formed from the concatenation of OWF(K_L,PPASN) and OWF(K_R,PPASN), where OWF(K,D) is defined in Appendix A.

Step 4 - Form Initial TMK_2

Let K_L and K_R denote, respectively, the left and right halves of the result of Step 2. The Initial TMK_2 is formed from the concatenation of OWF(K_L,PPASN) and OWF(K_R,PPASN), where OWF(K,D) is defined in Appendix A.

See Ref.8.5 - AS2805.6.4

Appendix I – Terminal Master Key Update

There are two possibilities for the update of the Terminal Master Keys - either TMK_1 only needs to be updated or else both TMK_1 and TMK_2 need to be updated.

AS2805 – 1988 Method

Update TMK_1 only

The inputs in this case are Old TMK_1 and the PIN Pad Acquirer Security Number (PPASN). The output is the New TMK_1.

Let K_L and K_R denote, respectively, the left and right halves of Old TMK_1, then New TMK_1 is formed from the concatenation of OWF(K_L,PPASN) and OWF(K_R,PPASN), where OWF(K,D) is defined in Appendix A.

Update TMK_1 and TMK_2

The inputs in this case are Old TMK_2 and the PIN Pad Acquirer Security Number (PPASN). The output is the New TMK_1 and New TMK_2.

Step 1

Form an Intermediate TMK, by combining each half of the Old TMK_2 with PPASN, using the exclusive-or operation. Let K_L and K_R denote, respectively, the left and right halves of Intermediate TMK, then New TMK_1 is formed from the concatenation of OWF(K_L,PPASN) and OWF(K_R,PPASN), where OWF(K,D) is defined in Appendix A.

Step 2

Let K_L and K_R denote, respectively, the left and right halves of Old TMK_2, then New TMK_2 is formed from the concatenation of OWF(K_L,PPASN) and OWF(K_R,PPASN), where OWF(K,D) is defined in Appendix A.

AS2805 – 2001 Method

Update TMK_1 only

The inputs in this case are Old TMK_1 and the PIN Pad Acquirer Security Number (PPASN). The output is the New TMK_1.

See AS2805.6.4 – 2001 section 6.4.3 as follows, for method. (uses OWF – 2000 {AS2805.4 – 2000 section 6})

Update TMK_1 and TMK_2

The inputs in this case are Old TMK_2 and the PIN Pad Acquirer Security Number (PPASN). The output is the New TMK_1 and New TMK_2.

See AS2805.6.4 – 2001 section 6.4.4 as follows, for method. (uses OWF – 2000 {AS2805.4 – 2000 section 6})

Terminal KEK update

General

The terminal maintains two terminal master keys for each acquirer with which it is required to communicate. These are known as KEK1 and KEK2

Inputs

The inputs to the key enciphering key update procedure shall be PPASN and the existing terminal key enciphering keys.

Algorithm KEK1 update

KEK1 shall be update as follows

(a) Concatenate PPASN with itself to form the temporary value D.

(b) Use the OWF with the existing KEK1 as the key and the temporary value D as the data to produce the new 128-bit value of KEK1.

(c) The new value of KEK1 replaces the existing value in storage.

The process is illustrated in Figure 1.

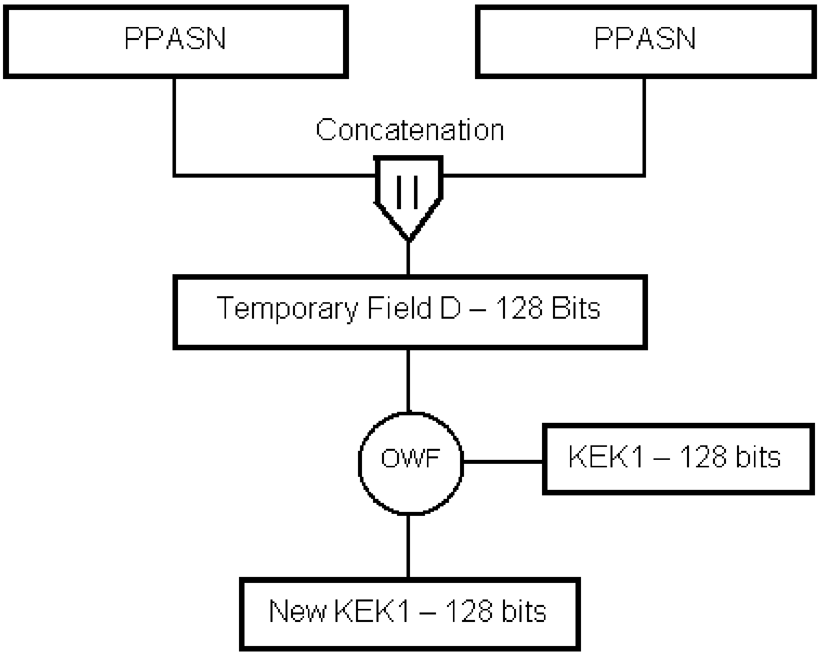


FIGURE 1 KEK1 UPDATE PROCEDURE

Algorithm KEK2 update

KEK2 shall be updated as follows:

Concatenate PPASN with itself to form the temporary value D.

Create a temporary new KEK by the modulo 2 addition of D to the existing KEK2.

Use the OWF with the existing KEK2 as the key and the D as the data to produce the new 128-bit value of KEK2.

The new value of KEK2 replaces the existing value in storage.

Use the OWF with the temporary KEK produced in Step (b) as the key and the value D as the data to produce the new 128-bit value of KEK1.

The new value of KEK1 replaces the old KEK1 in storage.

The process is illustrated in Figure 2.

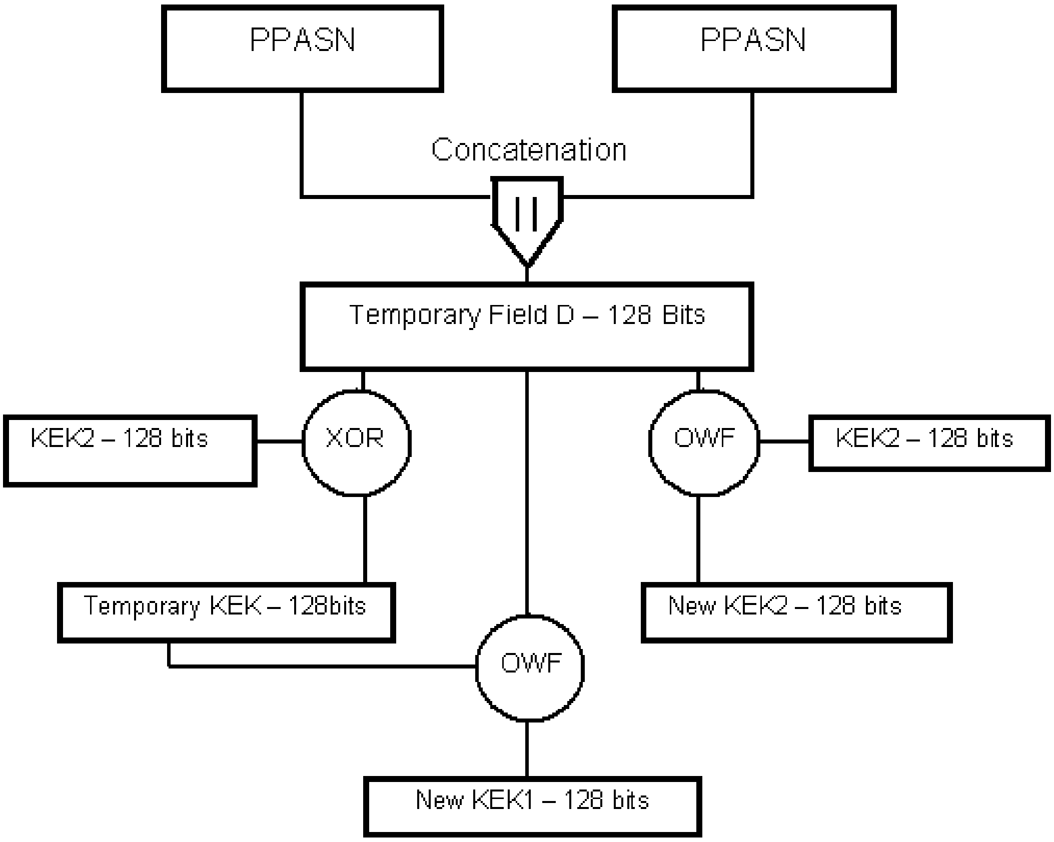


FIGURE 2 KEK2 UPDATE PROCEDURE

Appendix J – Derivation of the PIN Encryption Key

Single Length TPK

The PIN Encryption Key (KPE) is formed by combining a single length Terminal PIN Key (TPK) with two 64-bit fields (known as the E Field and the F Field) using the exclusive-or operation.

The E Field is derived from the Systems Trace Audit Number (STAN) and the F Field is derived from the transaction amount, as follows:

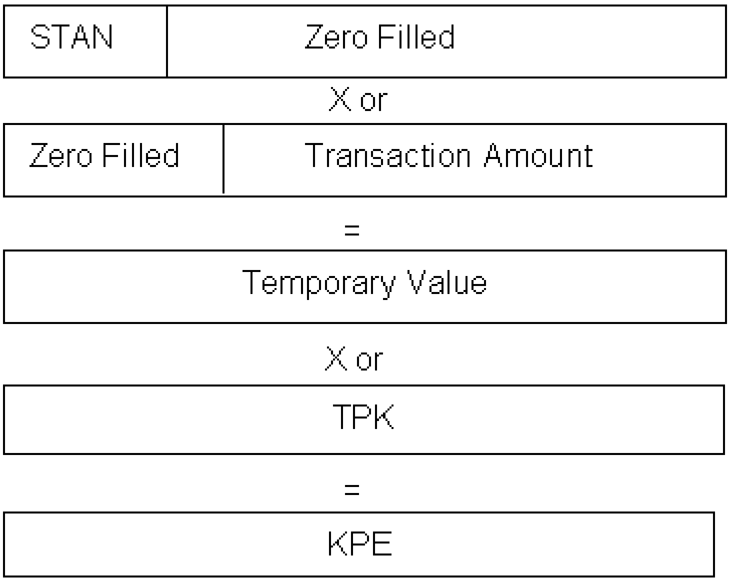
E Field: The 6 digits (24 bits) of the STAN, left justified and right zero filled to a total length of 64 bits, shifted left 1 bit.

F Field: The 12 digits (48 bits) of the transaction amount, right justified and left zero filled to a total length of 64 bits, shifted left 1 bit.

Fields E & F are X'or ed to form a temporary value.

This temporary value is then X'or ed with the TPK to form the KPE

Example:



See - AS2805.6.4, Section 6.9. (1988)

Double Length TPK

See Ref.8.5 - AS2805.6.4 section 6.6.3 (2001) as follows:

PIN enciphering key (KPE)

General

The PIN enciphering key (KPE) is used to encipher the PIN block.

Inputs

The inputs to the KPE calculation shall be the systems trace audit number (STAN), transaction amount, and PIN protection key (KPP)

Algorithm

KPE shall be calculated as follows:

Field E comprises the 6 digits (24 bits) of the STAN, left justified, and right zero-filled to a total length of 64 bits.

Field F comprises the 12 digits (48 bits) of the transaction amount, right justified and left zero-filled to a total length of 64 bits.

Field E and F are concatenated to produce the temporary value D.

Use the OWF with the KPP as the key and D as the data.

The result is KPE.

The process is illustrated in Figure 3.

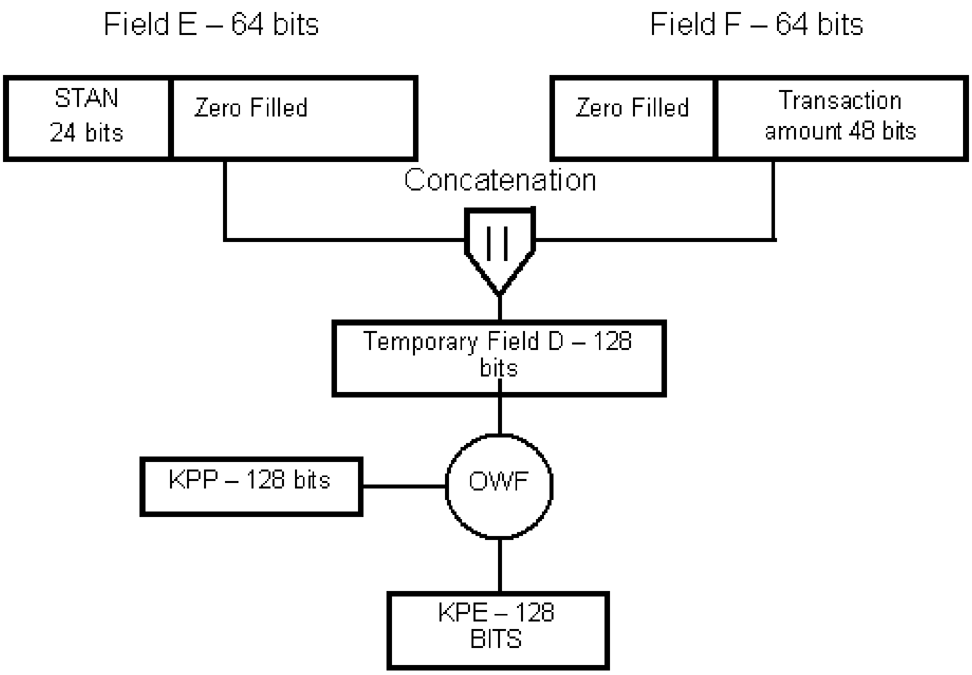


FIGURE 3 KPE CALCULATION

Appendix K – AS2805.3 PIN block formats

AS2805 Format 1 PIN block

The AS2805 Format 1 PIN block is used in situations where the account number is not available. The PIN block is formed by concatenation of the PIN and other data.

The AS2805 Format 1 PIN block has the format;

C	N	P	P	P	P	P/ T	P/ T	P/ T	P/ T	P/ T	P/ T	P/ T	P/ T	T	T

Where;

C	= Control field = binary 0001	
N	= PIN length	= binary 0100 to 1100
P	= PIN digit	= binary 0000 to 1001
P/T	= PIN/other	= determined by PIN length
T	= Other data	= binary 0000 to 1111

This format is accommodated by using the standard Format 05 for the PIN block and entering all "zero's" in place of the account number in PIN functions.

AS2805.3 Format 8 PIN block (format 46)

Support for "zero" length PIN block

The zero length PIN block format is identical to format 01 with the following exceptions.

If the Control Field is 0, then the PIN block is processed as a standard format 01 PIN block. If the Control Field is not 0 then the following rules apply.

If the second character is 0 then the PIN block is a Zero PIN block. No checking of the PIN block is required in this case.

If the second character is not 0 or in the range 4 to C (hex), inclusive, then return error code 24 and terminate processing.

If the input command is a verify PIN command and the second character is 0 then return error code 88 and terminate processing.

If the input command is a translate PIN command and the second character is 0, form a new PIN block as follows:

The new PIN block has the format 80RRRRRRRRRRRRFF (hex), where R denotes a random hexadecimal character.

When a Zero PIN block is encountered in a standard PIN verify or PIN translate command, error code 88 will be returned as notification only. Processing will continue.

The individual standard commands affected by this PIN Block format are:

CA, CC, DA, DC, EA and EC

Appendix L – Error messages

Most error messages are standard across all commands. Each command lists those errors specifically for it, but some standard checking functions may produce other errors that are only shown in this table. Some codes have more than one description where the error condition is more specific in a particular command; this is detailed in the command response.

Code : Description

00 : No errors

01 : Verification failure. CAM validation error. Data Length error.

02 : Key inappropriate length for algorithm. Hash validation failure. Invalid MK length.

03 : Invalid message type. Invalid secret key type. Data Length error. Zero PINblock received.

04 : Invalid key type code. Invalid secret key flag. Public key does not conform to encoding rules. Key Length invalid

05 : Invalid key length flag. Invalid message block number. Invalid hash identifier. Invalid number of Input pairs or not even.

06 : Invalid signature identifier. Invalid public key Algorithm Identifier

07 : Public exponent length error. MAC mode, key length mismatch.

08 : Invalid public exponent

09 : Secret key error, report to supervisor

10 : Source key parity error. Or other input key parity error.

11 : Destination key parity error. Key all 0s.

12 : Contents of user storage not available. Reset, power down or

16 : Console or printer not ready / not connected

17 : HSM not in authorized state

18 : Document definition format not loaded

19 : Specified Diebold table is invalid

20 : PIN block error.

21 : Invalid index value, or index / block count would cause overflow condition

22 : Invalid account number

23 : Invalid PIN block format code

24 : PIN is fewer than 4 or more than 12 digits long. PIN is not 4 digits.

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

33 : LMK key change storage is corrupt

40 : Invalid firmware checksum

41 : Internal hardware / software error: bad RAM, invalid error codes, etc.

overwrite. 13 : LMK error - report to Supervisor 14 : PIN encrypted under LMK pair 02-03 is invalid 15 : Invalid input data – unable to identify the individual fields in the input 78 : SK length error 80 : Data length error. The MAC or other data amount is not as expected 81 : Signature length error 82 : Invalid trailer 83 : Invalid certificate format 84 : Invalid subject ID 88 : Zero PIN block encountered; advice only.	42 : DES failure 47 : DSP error; report to supervisor (RG7000 series only) 49 : Corrupt SK 50 : Key comprises all zeros 51 : KV parity error 76 : Signature/KEK length <> modulus length 77 : Decrypted Signature/KEK blocks corrupt 90 : Data parity error in the request message received by the HSM 91 : Longitudinal Redundancy Check (LRC) failure on input date (transparent async only) 92 : Count value is incorrect or outside limits (transparent async only) 97 : RSA key generation error

Appendix M – Australian Key Schemes

Five key schemes (G, H, I, K and L) are specified for this firmware. They are used for the import and export of keys under Zone Master keys, Terminal Master Keys and Key Encrypting Keys.

The Key scheme G applies to single length keys. The Key schemes H & K apply to double length keys. The key schemes I & L apply to triple length keys.

The mechanism for the key schemes G, H and I is to apply an appropriate variant (see Appendix D) to the encrypting key then to encrypt the working key using the CBC method.

Key schemes K and L also use the CBC mode of encryption, but do not apply a variant prior to encrypting the key.

NOTE: The variant used is determined by the length of the key being encrypted, **NOT** the length of the key performing the encryption

Examples:

G Scheme. (Single Length Data/Session Key)

With the 'G' scheme regardless of the length of the key encrypting the Data/Session key the variant applied from Appendix D is the single length variant.

e.g.

ZMK – 0404 0404 0404 0404 0808 0808 0808 0808

ZAK– 2020 2020 2020 2020

ZAK Variant - 2424 2424 2424 2424 2424 2424 2424 2424 (from Appendix D)

Encrypting Key (ZMK with variant applied) – 2020 2020 2020 2020 2C2C 2C2C 2C2C 2C2C

ZAK Encrypted under ZMK (ZAK CBC encrypted using ZMK with variant applied)

G 7B19 0BFF 522D E15D

H Scheme. (Double Length Data/Session Key)

With the 'H' scheme regardless of the length of the key encrypting the Data/Session key the variant applied from Appendix D is the double length variant.

e.g.

ZMK – 0404 0404 0404 0404 0808 0808 0808 0808

ZAK– 2020 2020 2020 2020 4040 4040 4040 4040

ZAK Variant - 24C0 24C0 24C0 24C0 24C0 24C0 24C0 24C0 (from Appendix D)

Encrypting Key (ZMK with variant applied) – 20C4 20C4 20C4 20C4 2CC8 2CC8 2CC8 2CC8

ZAK Encrypted under ZMK (ZAK CBC encrypted using ZMK with variant applied)

H 27C9 B3BA C267 FEA7 1BF6 8BC1 5837 5F8C

I Scheme. (Triple Length Data/Session Key)

With the 'I' scheme regardless of the length of the key encrypting the Data/Session key the variant applied from Appendix D is the triple length variant.

e.g.

ZMK – 0404 0404 0404 0404 0808 0808 0808 0808

ZAK– 2020 2020 2020 2020 4040 4040 4040 4040 0D0D 0D0D 0D0D 0D0D 0D0D

ZAK Variant - 2430 2430 2430 2430 2430 2430 2430 2430 (Appendix D)

Encrypting Key (ZMK with variant applied) – 2034 2034 2034 2034 2C38 2C38 2C38 2C38

ZAK Encrypted under ZMK (ZAK CBC encrypted using ZMK with variant applied)

I E2D5 D40F 9433 DBCB 77AB 8654 D404 1AAF 4F53 4FE0 C7C0 E103

K Scheme. (Double Length Data/Session Key)

This scheme uses the CBC mode of encryption, and no variant is applied to the key encryption key.

e.g.

ZMK – 0404 0404 0404 0404 0808 0808 0808 0808

ZAK – 2020 2020 2020 2020 4040 4040 4040 4040

ZAK encrypted under ZMK (ZAK CBC encrypted using ZMK with no variant applied) –

K C1FB 7F83 BA2E 91C0 C466 7057 C58A 1A72

L Scheme. (Triple Length Data/Session Key)

This scheme uses the CBC mode of encryption, and no variant is applied to the key encryption key.

e.g.

ZMK – 0404 0404 0404 0404 0808 0808 0808 0808

ZAK – 2020 2020 2020 2020 4040 4040 4040 4040 0D0D 0D0D 0D0D 0D0D 0D0D

ZAK Encrypted under ZMK (ZAK CBC encrypted using ZMK with no variant applied) –

L C1FB 7F83 BA2E 91C0 C466 7057 C58A 1A72 99D4 E6AE 4BEB 49CD 29C3 7CE6 F6AB CB0B

Commands that support Australian key schemes

Standard console commands

KG, IK, KE

Standard host commands

A0, A6, A8, BW, EA, EC, CC, BU

Custom host commands

OI, OK, OO, OQ, CO, OY, PI, D6, E0, E2, E8, H8

Appendix N – AS 2805.6.2 Support Appendices

Appendix N-A: One-way Function

The One-way Function (OWF) used in the commands specified in this document is defined in the AS2805.5.4 standard (Ref.8). It is described below.

Let K be a DES key and let D be a data block, of arbitrary length, n bits.

If n is not a multiple of 64 then append a single binary "1" followed by as many binary zeros as necessary to make the data a multiple of 64 bits (possibly none). Let D* denote the padded data. Two distinct cases exist:

Case 1 – D* has length 64 (and so n ≤ 64)

Decrypt D* with K.

Combine the result of step 1 with D*, using the exclusive-or operation.

Discard the rightmost (64-n) bits of the result of step 2 and denote the result by X, so that X has length n bits.

Then:

X = OWF(K, D).

Case 2 – D* has length greater than 64 (and so n > 64)

Let V denote the final 64-bit block of CBC encryption of D* with K, with a zero initial value.

Encrypt D* with K, using CBC encryption and an initial vector = V.

Combine the result of step 2 with D*, using the exclusive-or operation.

Discard the number of padding bits originally appended to D from the result of step 3 and denote the result by Y, so that Y has length n bits.

Then:

Y = OWF(K, D).

Appendix N-B: Derivation of Data Values

A number of 128-bit Data Values (DV1, DV2, DV4, DV5 and DV6) are derived from data fields on track 2 of the card. These fields are each 32 bits in length and are known as fields A, B, C and D. They are defined as follows, where "|" denotes concatenation:

"A | B" denotes the 16 character PAN, including the check digit, immediately preceding the Field Separator.

"C | D" denotes the 16 character "Other Card Data", immediately following the YYMM field.

From fields A, B, C and D, five Card Values (CV1 – CV5) are formed:

CV1 = A | B

CV2 = B | A

CV3 = A | C

CV4 = B | D

CV5 = C | D

Then,

DV1 = CV1 | CV1

DV2 = CV2 | CV2

DV4 = CV3 | CV4

DV5 = CV4 | CV3

DV6 = CV5 | CV5

Finally, two other Data Values DV3 (128 bits) and DV7 (64 bits) are defined as follows.

Define the 64-bit values (left justified and zero padded, if necessary):

STAN = Systems Trace Audit Number

CATID = Card Acceptor Terminal Identification

AT = Transaction Amount

Then,

DV3 = STAN | CATID

DV7 = (STAN ⊕ CATID ⊕ AT),

where "⊕" denotes the exclusive-or operation.

Appendix N-C: MAC Key Derivation

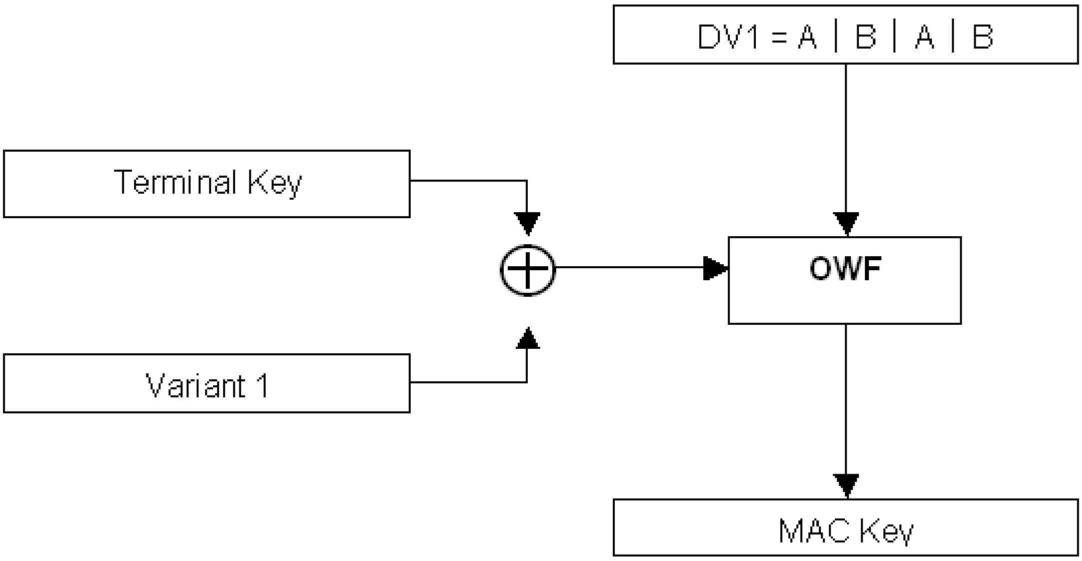
The transaction MAC Key is derived from the Data Value DV1 (see Appendix N-B) and a variant of the Terminal Key, via:

MAC Key = OWF((Terminal Key) ⊕ (Variant 1), DV1),

where ⊕ denotes the exclusive-or operation and Variant 1 is defined as

Variant 1 = X'24C024C024C024C024C024C024C024C0.

In diagrammatic form:



Appendix N-D: PIN Encipherment Key Derivation

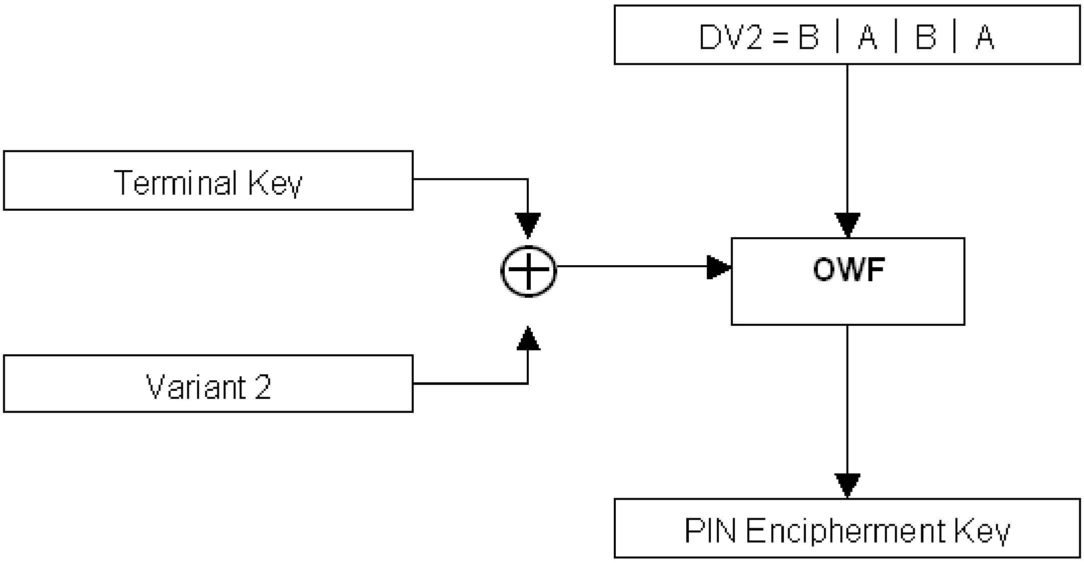
The transaction PIN Encipherment Key is derived from the Data Value DV2 (see Appendix N-B) and a variant of the Terminal Key, via:

PIN Encipherment Key = OWF((Terminal Key) ⊕ (Variant 2), DV2),

where ⊕ denotes the exclusive-or operation and Variant 2 is defined as

Variant 2 = X'28C028C028C028C028C028C028C028C0.

In diagrammatic form:



Appendix N-E: Privacy Key Derivation

The Privacy Key derivation used with the QM & QO commands specified at Section 10.15 and 10.16 respectively.

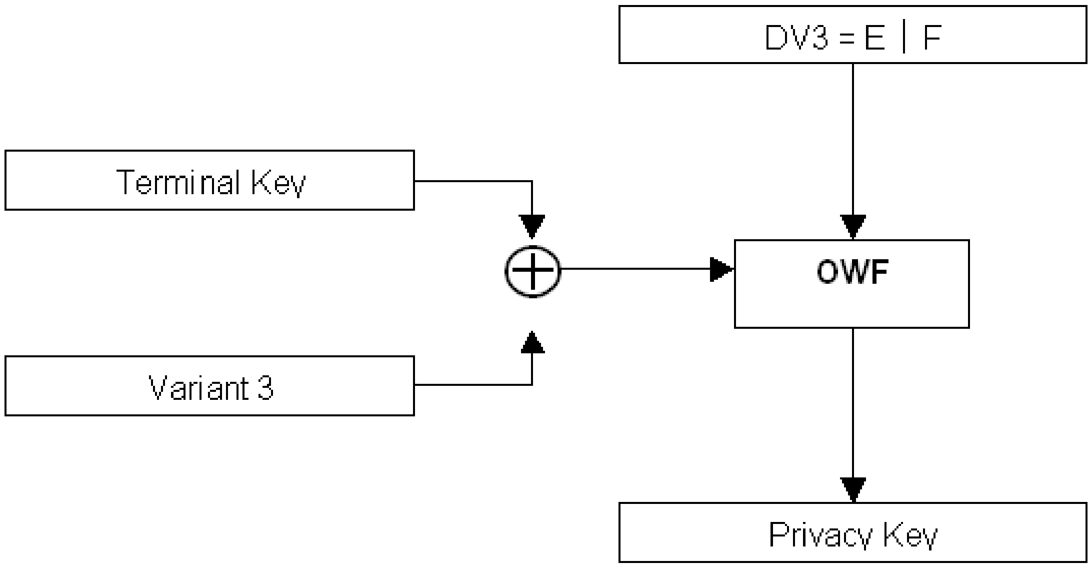
The transaction Privacy Key is derived from the Data Value DV3 (see Appendix N-B) and a variant of the Terminal Key, via:

Privacy Key = OWF((Terminal Key) ⊕ (Variant 3), DV3),

where ⊕ denotes the exclusive-or operation and Variant 3 is defined as

Variant 3 = X'22C022C022C022C022C022C022C022C0.

In diagrammatic form:



Appendix N-F: Terminal Key Update (AS2805.6.2)

A Terminal Key is updated as follows:

Concatenate the 64-bit MAC Residue (X) from the Request Message and the 64-bit MAC Residue (Y) from the Response Message, to form a 128-bit value, Data. Then,

New Terminal Key = OWF(Current Terminal Key, Data).

Appendix N-G: MAC and MAC Residue Calculation

A Message Authentication Code (MAC) is calculated over a data block D, using a double length key K. A MAC may be 32, 48 or 64 bits in length, as required.

1. Append as many binary zeros to D as necessary to produce a data block D* with length a multiple of 64 bits.
2. Let C denote the last ciphertext block obtained by encrypting D* with K, using the CBC mode of encryption with a zero initial value.
3. Then

   C = MAB(K, D)

   and

   MAC(K, D) = leftmost 32, 48 or 64 bits of MAB(K, D), as required.
4. Encrypt C with K, using the ECB mode of encryption to produce the MAB Extension.
5. Concatenate MAB(K, D) and the MAB Extension to form the Extended MAB.
6. Then the MAC Residue, MAR(K, D), is defined as the **next** 64 bits of the Extended MAB after MAC(K, D).

Three cases are possible:

MAC Length	**MAR(K, D)**
32 bits	Bits 33 – 96 of the Extended MAB, where the leftmost bit is bit 1
48 bits	Bits 49 – 112 of the Extended MAB, where the leftmost bit is bit 1
64 bits	Bits 65 – 128 of the Extended MAB, where the leftmost bit is bit 1

Appendix N-H: Authentication Parameter

The Authentication Parameter (AP or Auth Para) is a 64-bit value constructed by the Card Issuer, or his agent, to confirm the approval of a transaction and, specifically, the amount of the transaction. AP is calculated using the One-way Function (OWF), defined in Appendix N-A and various Data Values, defined in Appendix N - B, as follows:

Let

Card Key = OWF(DV4, DV5),

then

Decoupling Key = OWF(Card Key, DV6)

and

AP = OWF(Decoupling Key, DV7).

Appendix O – AS 2805.6.2 (Single DES) Support Appendices

Appendix O-A: One-way Function

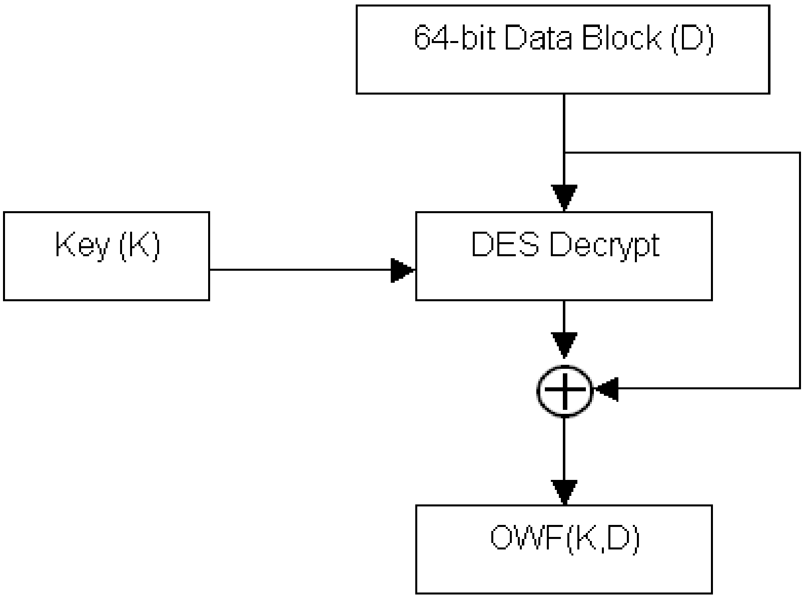
The One-way Function (OWF) used in the commands specified in this document is described below.

Let K be a single length DES key and let D be a 64-bit data block.

1. Decrypt D with K.
2. Combine the result of step 1 with D, using the exclusive-or operation, and denote the result by X.
3. Then:

   X = OWF(K, D).

In diagrammatic form:



Appendix O-B: Derivation of Card and Data Values

A number of Card Values (CV1, CV2, CV3, CV4 and CV5) are derived from data fields on track 2 of the card. These fields are each 32 bits in length and are known as fields A, B, C and D. They are defined as follows, where "|" denotes concatenation:

"A | B" denotes the 16 character PAN, including the check digit, immediately preceding the Field Separator.

"C | D" denotes the 16 character "Other Card Data", immediately following the YYMM field.

From fields A, B, C and D, the five Card Values (CV1 – CV5) are formed:

CV1 = A | B

CV2 = B | A

CV3 = A | C

CV4 = B | D

CV5 = C | D

One further Data Value DV6 (64 bits) is defined as follows.

Define the 64-bit values:

STAN = Systems Trace Audit Number (6 digits (24 bits), left shifted one bit and right filled with binary zeros);

CATID = Card Acceptor Terminal Identification (8 characters (64 bits), left shifted one bit and right filled with binary zeros);

AT = Transaction Amount (12 digits (48 bits), right justified and left filled with binary zeros).

Then,

DV6 = (STAN ⊕ CATID ⊕ AT),

where "⊕" denotes the exclusive-or operation.

where "⊕" denotes the exclusive-or operation.

Appendix O-C: MAC Key Derivation

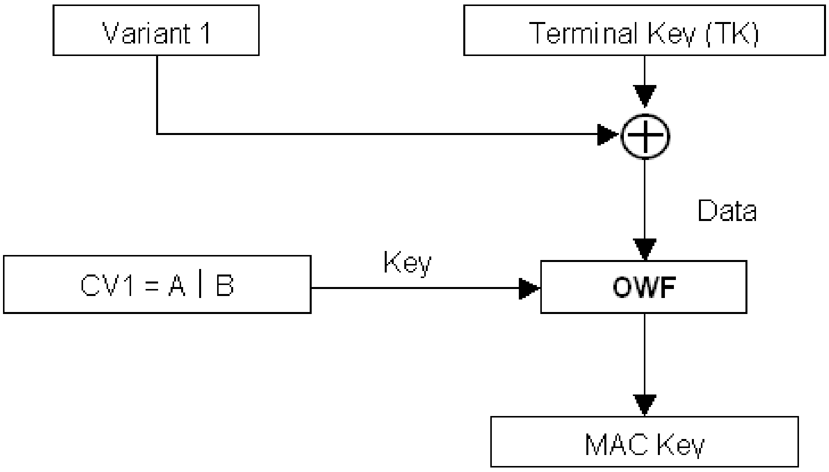
The transaction MAC Key is derived from the Card Value CV1 (see Appendix O-B) and a variant of the Terminal Key, via:

MAC Key = OWF(CV1, (Terminal Key) ⊕ (Variant 1)),

where ⊕ denotes the exclusive-or operation and Variant 1 is defined as

Variant 1 = X'2424242424242424.

In diagrammatic form:



Important Note:

In the MAC Key derivation, above, CV1 is used as the key input to the OWF and ((Terminal Key) ⊕ (Variant 1)) is used as the data input to the OWF.

Appendix O-D: PIN Encipherment Key Derivation

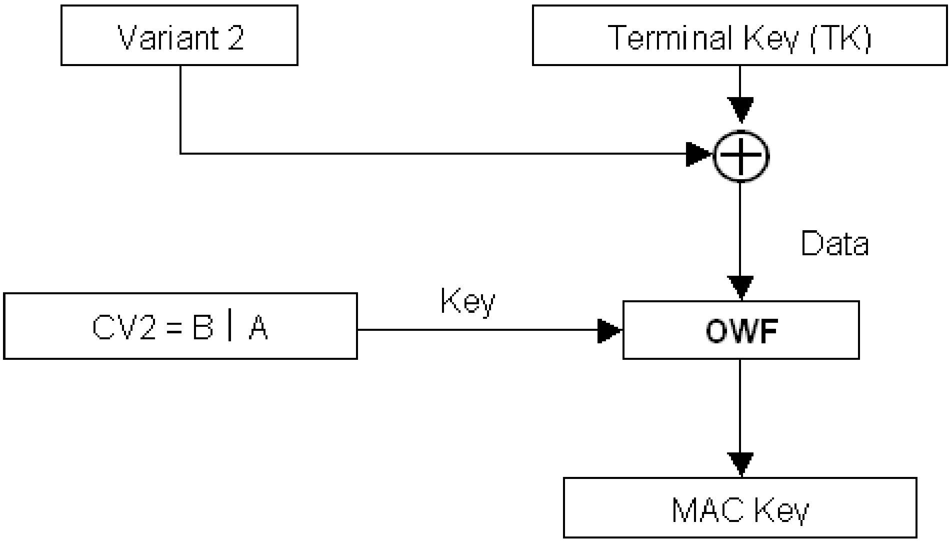
The transaction PIN Encipherment Key is derived from the Card Value CV2 (see Appendix O-B) and a variant of the Terminal Key, via:

PIN Encipherment Key = OWF(CV2, (Terminal Key) ⊕ (Variant 2)),

where ⊕ denotes the exclusive-or operation and Variant 2 is defined as

Variant 2 = X'2828282828282828.

In diagrammatic form:



Important Note:

In the PIN Encipherment Key derivation, above, CV2 is used as the key input to the OWF and ((Terminal Key) ⊕ (Variant 2)) is used as the data input to the OWF.

Appendix O-E: Terminal Key Update

A Terminal Key is updated as follows:

Concatenate the 32-bit MAC Residue (MARX) from the Request Message and the 32-bit MAC Residue (MARY) from the Response Message, to form a 64-bit value, Data. Then,

New Terminal Key = OWF(Current Terminal Key, Data).

Important Note:

The New Terminal Key must **not** be adjusted for parity.

Important Note:

In the New Terminal Key derivation, above, the Current Terminal Key is used as the **key** input to the OWF and the concatenation of the MARX and MARY is used as the **data** input to the OWF.

Appendix O-F: MAC and MAC Residue Calculation

A 32-bit Message Authentication Code (MAC) is calculated over a data block D, using a single length key K. This process also produces a 32-bit MAC Residue (MAR).

1. Append as many binary zeros to D as necessary to produce a data block D* with length a multiple of 64 bits.

2. Let C denote the last ciphertext block obtained by encrypting D* with K, using the Cipher Block Chaining (CBC) mode of encryption with a zero initial value.

3. Then

MAC(K, D) = leftmost 32 bits of C and MAR(K, D) = rightmost 32 bits of C.

Appendix O-G: Card Key and Authentication Parameter

The Authentication Parameter (AP or Auth Para) is a 64-bit value constructed by the Card Issuer, or his agent, to confirm the approval of a transaction and, specifically, the amount of the transaction. AP is calculated using the One-way Function (OWF), defined in Appendix O-A and various Card and Data Values, defined in Appendix O-B, as follows:

Let

Card Key = OWF(CV3, CV4),

then

Decoupling Key = OWF(CV5, Card Key)

and

AP = OWF(Decoupling Key, DV6).

Important Note:

In the above calculations, CV3, CV5 and Decoupling Key are used as the key inputs to the OWF and CV4, Card Key and DV6 used as the data inputs to the OWF, respectively.

Appendix S – APCA Functional Specification Comparison Guide

APCA SCM Function	APCA Command Code	Thales Command Code	
		Base HSM F/W	This Specification
General			
1.1.1 Echo Test	0000	B2	
1.1.2 SCM Status Extended	0002	NO	
1.1.2 Function Status	0005	None	None
1.1.4 KM Status	0006	NC	
1.1.5 Format Status	0007	None	None
1.1.6 Set Clock	0015	Console: SETTIME	None
1.1.7 Get Clock	0016	Console: GETTIME	None
1.1.8 MD5Gen	0020	GM	
1.1.9 SHAGen	0021	GM	
Interchange			
1.2.1 Encipher	2500		PU
1.2.2 Decipher	2600		PW
1.2.3 KEKGEN – 6.3	D501		F6
1.2.4 KEKREC – 6.3	D502		F8
1.2.5 NodeKeyGen - 6.3	3A00		OI
1.2.6 RTMK (Key Translation - Receive)	4500		OK
1.2.7 VISA REC	4501	A6	
1.2.8 KEKGEN –VISA	4502	A0	
1.2.9 VISA-REC-IWK	4503	A6	
1.2.10 VISA-REC-AWK	4504	A6	
1.2.11 Kmmigrate (KM Translation)	4600	BW	
1.2.12 MACGen - 6.3 and 6.4	5500		C2
1.2.13 MACVerify - 6.3 and 6.4	5600		C4
1.2.14 NodeProof	E520		E0
1.2.15 NodeResp	E530		E2
1.2.16 KVC request	7510	BU	
1.2.17 ENCIPHER – OFB	2700		PU
1.2.18 DECIPHER – OFB	2800		PW
Terminal to node AS 2805.6.4			
2.1 TermKeyGen1-2000	3500		PI & OU
2.2 TermKeyGen2-2000	3510		PI & OW
2.3 TermKeyInit - 6.4-2000	3630		C0
2.4 PINVerify - 6.4-2000	6510		F0
2.5 PINVerify VISA 6.4-2000	6511		F2
2.6 KACalc-2000	B520		C8

2.7 KAExport-2000	B530	FE	
2.8 KAImport-2000	B540	FC	
2.9 VerifyPPID-2000	E540		D2
2.10 TermProof-2000 – 6.4 2000	E500		E4
2.11 HostProof-2000 – 6.4 2000	E510		E6
2.12 KIA Send	B550	A8	
2.13 KIA Receive	B560	A6	
2.14 TKEYGEN	3144	None	None
Terminal to node AS 2805.6.2			
3.1 PINKEYCHANGE	46A0	None	
3.2 ENCIPHER CBC	2511		PU
3.3 DECIPHER CBC	2611		PW
3.4 ENCIPHER ECB	2501		PU
3.5 DECIPHER ECB	2601		PW
3.6 PINBLOCKTRANS 6.2 -> 6.3	6640	None	None
3.7 TERMKEYUPDATE	3710	None	None
3.8 ENCIPHER OFB	25A0		PU
3.9 DECIPHER OFB	26A0		PW
3.10 MAC GENERATE	5510	None	None
3.11 MAC VERIFY	5610		RE
3.12 MAC VERIFY (Completion Confirmation Message)	5620		RQ
3.13 TERMKEYINIT	3640		RW
3.14 APGEN	E600		RU
3.15 MAC GENERATE NDC+	5530	None	None
3.16 MAC VERIFY NDC+	5630	None	None
ATM			
4.1 ABKeyGen-2000	3B00	HC	
4.2 CkeyGen-2000	3B10	HC	
4.3 MkeyGen-2000	3B20	HC	
4.4 ATMKEYGEN	3B30	A0	
Public Key			
5.5 KMMigrate DEA2	4610	EM	
5.6 GetPublic-2000	C500	None	None
5.7 NodeKEKSend-2000	C600		H4
5.8 NodeKEKRec-2000	C610		H6
5.9 GetDEA2Pair	C620		EO & EI
5.10 NodeKEKSend-2000-Export	C700		H4
5.11 NodeKEKRec-2000-Export	C710		H6
5.12 Load Public	C6A0	None	None
5.13 Load Public-NDC+	C6B0	None	None
5.14 SignPublic NDC+	C6C0	None	None
5.15 Verify EPP NDC+	C6D0	None	None
5.16 NodeKEKsend-NDC+	C720	A0, GK & EW	
5.17 Verify Certificate	C800	ES	
5.18 SignPublic PKCS#10	C810		

5.19 Construct Key Token B1	C850	None	None
5.20 Verify Key Token A2	C860	None	None
Retained			
6.1 CHESSKEKGEN – 6.3	D001	F6	F6
6.2 CHESSKEKREC – 6.3	D002	F8	F8
6.3 APGEN (old replaced by 3.14)			
PIN and CARD Functions			
7.1 PINTrans - IBM3624 to 6.3	6680	CA	
7.2 PINTrans - 6.3 to 6.3	6600	CC	
7.4 PVVGen - using given PIN	65B4	DG	
7.5 PINVerify VISA 6.3	6501	DC	
7.6 PINVerify 6.3	6500	EC	
7.7 PPASNVerify	F013		E4
7.8 PPIDEncrypt	F014		D0
7.9 PINTrans - 6.4 to 6.3	6610		PO
7.10 CVVGEN	8500	CW	
7.11 CVVKEYGEN	8600	AS	
7.12 CVVKEYIMPORT	8510	AW	
7.13 CVVVERIFY	8520	CY	
Terminal Remote Initialisation			
8.1 SponsorKeyGen	B510	A0	
8.2 InitialKeyRec	B580		I0
8.3 LoadKCA	B590	A8	
8.4 GetPublicPair -TCU	C630	EI	
8.5 TCUPublicRec	C640		H0
8.6 TermKeyInit - remote	3633		PI & PK & F4
8.7 TermKeyReinit - remote	3634		PI & D0
8.8 RandGen	B570		C6
8.9 TermKeyInit Remote – 6.2	3643		RW & PK & F4
Approved Extensions			
9.1 KTKALC	B510	None	

Notes:

Other commands available in this specification which have no equivalent in the APCA specification but which are required for Thales customers include:

C0, C2, C4, D4, D6, D8, E8, OO, OQ, OU, OY, PM, H8

Appendix T – Key Notation comparison table

Australian Standards		Thales	
Code	**Meaning**	**Code**	**Meaning**
A	ATM A Key	TMK1	Terminal Master Key
B	ATM B Key	TMK2	Terminal Master Key
C	Communications Key	C	Communications Key
CATID	Card Acceptor terminal Identification	CATID	Card Acceptor terminal Identification
CVV	Card Verification Value	CVV	Card Verification Value
KCA	Cross Acquirer Key	KCA	Cross Acquirer Key encrypting Key
KCVV	Card Verification Value Keys	CVK	Card Verification Key
KD	Data Key	KD	Privacy Key (Denoted KD)
KEK	Key Encrypting Key	KEK	Key Encrypting Key
KIA	Acquirer Initialization Key	TMK/TEK	Terminal Master/Encryption Key
KM	Domain Master Key	LMK	Local Master Key
KMAC	MAC Key	TAK/ZAK	Terminal/Zone Authentication Key
KMACH	HouseKeeping MAC Key	TAK	Terminal Authentication Key
KMACI	Initial MAC Key	TAK	Terminal Authentication Key
KPE	Pin Encryption Key	TPK	Terminal Pin Key
KPP	Pin Protect Key	TPK / ZPK	Terminal / Zone Pin Key
KPV	Pin Verification Key	PVK	Pin Verification Key
KPVVA	Visa Pin Verification Key A	PVK	Pin Verification Key
KPVVB	Visa Pin Verification Key B	PVK	Pin Verification Key
KT	Terminal Key	KT	Transaction Key
KTK	Key Transport Key	ZMK	Zone Master Key
KVC	Key Verification Code	KCV	Key Check Value
M	ATM M Key (Master)	TMK	Terminal Master Key
PK	Public Keys	PK	Public Key
PPASN	Pin Pad Security Number	PPASN	Pin Pad Acquirer Secret Number
PPID	Pinpad Identification Number	PPID	Pin Pad Identification Number
PVC	Verification Code of Public Key	PVC	Public Key Verification Code
PVV	Pin Verification Value	PVV	Pin Verification Value
SK	Secret Key	SK	Secret Key
STAN	System Trace Audit Number	STAN	System Trace Audit Number
KMA	Acquirer Master Key Encrypting Key	KMA	Acquirer Master Key Encrypting Key
		ZEK	Zone Encryption Key
Note: 1= Variant1, 2=Variant2 e.g TMK1 or TMK2			
Note: s=Send r=Receive e.g KEKs or KEKr			

Appendix U1 – DEA 2 Text Block - DFormat 1

The RSA datablock format conforms to the APCA Dformat1 specifications (described in APCA2000 Specification Version 3 , section 5.4.4.1), Reference 10.

The clear datablock has the following format:

Byte	Bits	Description
0	7-6	00 = Always less than modulus.
	5-1	00001 = block format 1.
	0	0 = no padding used, 1 = padding used.
1	Normally zero unless an identity transform (concealing) would have occurred.	
2	Number n of 8 byte blocks in the modulus of the key enciphering this data.	
3-4	Checksum of bytes 5through 8*n*-1.	
Var (5 to 8*n*-1)	Up to 8*n*-5 bytes of data, left justified. If data is less than (8*n*-5) bytes, append random pad bytes and pad byte count in byte 8*n*-1. The pad count includes byte 8*n*-1.	

Notes:

1. 8n represents the size of the modulus of the DEA 2 key that enciphers the DFormat 1 textblock.
2. The leftmost byte of a block (byte 0) is the most significant byte and the rightmost byte (e.g. byte 63) is the least significant byte.
3. A short data sequence will be padded to the right with random bits, and a pad count.
4. The checksum is calculated as the 16-bit sum of bytes 4 to 8n-1 with a rotate left of 1 bit to the working total before each byte is added in.
5. The maximum amount of data that can be enciphered is 8n-6 bytes. The actual data block size is 8n-6-[8n-1] (where [x] means "contents of byte x").

Validation of this block includes the following steps:

The length of the data to be validated is equal to the length (in bytes) of the modulus of the key to be used for the validation - if not, return error code 76.

1. Byte 0 of the clear data block is 0x02 or 0x03 - if not, return error code 77.
2. Byte 1 of the clear data block is 0x00 - if not, return error code 77.
3. Byte 2 of the clear data block must be equal to the modulus length in bytes - if not return error code 77.
4. Compute a checksum on the clear data; if not equal to bytes 3-4 of the clear data block return error code 77.

Appendix U2 – Public Key Encoding

The HSM supports the following public key encoding types:

Type = 01 (DER encoding for an ASN.1 public key)

An ASN.1 RSAPublicKey has the following definition (see Ref.6):

```
RSAPublicKey : : = SEQUENCE {
        modulus INTEGER, - - n
        publicExponent INTEGER - - e }
```

Appendix V – Plaintext Data Block Formats

This Appendix describes the Plaintext Data Block Formats used in the H8 and I0 commands.

Format 01:

The Plaintext Data Block is the same length (in bits) as the input KHSK Modulus Length and has the following binary format, with the *rightmost* byte, the least significant byte, labelled byte 0:

Byte 0-19	All 0x'00
Byte n	0x'1D or 0x'1E
Byte n+1 to n+8	Random Number
Byte n+9 to n+13	DTS
Byte n+14 to n+21	PPSN
Byte n+22 to n+37	KTI

Format 02:

The Plaintext Data Block is the same length (in bits) as the input KHSK Modulus Length and has the following binary format, with the *leftmost* byte, the least significant byte, labelled byte 0:

Byte 0-19	All 0x'00
Byte n	0x'1D or 0x'1E
Byte n+1 to n+8	Random Number
Byte n+9 to n+13	DTS
Byte n+14 to n+21	PPSN
Byte n+22 to n+37	KTI

Format 03:

Byte	**Value**	**Comment**
0	03	Indicates checksum and padding are present (1 byte)
1	00	Null transform byte (1 byte)
2	…	Variable field specifying the number of 64 bit blocks in the modulus (1byte) (NOTE: It is the total number of bits of this Data Block.)
3..4	…	Checksum of the rest of the data (2 bytes)
5..20	…	KT (16 bytes)
21..28	…	PPID (8 bytes)
29..34	…	DTS (YYMMDDHHmmss) (6 bytes)
35..42	…	RN (8 bytes)
43..(N-1)	…	Padding (any value)
N	(N-42)	Variable field specifying the length of Padding including this byte (1 byte)

Where N = 47 or above AND
N = (number of Bytes in Byte 2 of Data Block -1) i.e. [(value in Byte 2) / 8] - 1

e.g. Format 03 Data Block = 112 Bytes
Byte 2 = 0x0E (14 decimal)
N = (0x0E) x 64 / 8 - 1
= 14 x 64 / 8 – 1
= 111

Then the last two fields become:

43..110	0x00..0x00
111	(N-42) = (111-42) = 69 = 0x45

e.g. Format 03 Data Block = 184 Bytes
Byte 2 = 0x17 (23 decimal)
N = (0x17) x 64 / 8 - 1
= 23 x 64 / 8 - 1
= 183

Then the last two fields become:

43..182	0x00..0x00
183	(N-42) = (183-42) = 141 = 0x8D

Format 04:

Byte	**Value**	**Comment**
0	03	Indicates checksum and padding are present (1byte)
1	00	Null transform byte (1 byte)
2	..	Variable field specifying the number of 64 bit blocks in the modulus (1byte) (NOTE: It is the total number of bits of this Data Block.)
3..4	….	Checksum of the rest of the data (2 bytes)
5..20	….	KT (16 bytes)
21..28	….	PPID (8 bytes)
29..34	….	DTS (YYMMDDHHmmss) (6 bytes)
35..42	….	RN (8 bytes)
43..58	0x00 or private data	Optional user numeric data (16 bytes)
59..(N-1)	….	Padding (any value)
N	(N-58)	Variable field specifying the length of Padding including this byte (1 byte)

Where N = (Byte 2 of Data Block x 64 / 8) - 1

e.g. Format 04 Data Block = length of 112 Bytes
Byte 2 = 0x0E (14 decimal)
N = (0x0E x 64 / 8) - 1
= (14 x 64 / 8) - 1
= 111

Then the last two fields become:

59..110	00..00
111	(N-58) = (111-58) = 53 = 0x35

e.g. Format 04 Data Block = length of 184 Bytes
Byte 2 = 0x17 (23 decimal)
N = (0x17 x 64 / 8) - 1
= (23 x 64 / 8) - 1
= 183

Then the last two fields become:

59..182	00..00
183	(N-58) = (183-58) = 125 = 0x7D

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211
E-mail: CPL_Sales_AMS_TG@thalesgroup.com

Asia Pacific
Unit 904-906A, Core D
Cyberport 3, 100 Cyberport Road
Pokfulam, Hong Kong | Tel: +852 3157 7111
Fax: +852 2815 8141 | E-mail: apacsales.cpl@thalesgroup.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: CPL_Sales_EMEA_TG@thalesgroup.com

> cpl.thalesgroup.com <