THALES

cpl.thalesgroup.com

payShield 9000 v3.5

Host Command Reference Manual

Addendum for Optional License LIC014 (WebPIN Commands)

1270A592-038

26 July 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
1270A592-038	Issue 38	payShield 9000 v3.5	July 2120

References

The following documents are referenced in this document:

1	payShield 9000 Host Command Reference Manual Document Number: 1270A546
2	WebPIN API User's Guide Document Number: 1270A302
3	payShield 9000 Host Programmer's Manual Document Number: 1270A542

Chapter 1 – Introduction

Purpose of these Host commands

These payShield 9000 Host commands provide support for the WebPIN product. This document describes only the payShield 9000 Host commands – for additional information about WebPIN see document 1270A302 WebPIN API User's Guide

Key Type Codes

The list of key type codes can be found in Chapter 4 of the payShield 9000 General Information Manual.

Key Type Table

The Key Type Table can be found in Chapter 4 of the payShield 9000 General Information Manual.

Key Block LMK Support

Key Block LMKs are not supported by the commands in this addendum.

List of Host Commands (Alphabetical)

Chapter 2 – Host Commands

General

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

A number of abbreviations are used throughout. They are:

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

For example:

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

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

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

In a command to the payShield 9000 HSM, any key can be replaced by a reference to internal user storage. In the details that follow, a key is always shown as if it is to be sent with each command; in every case the key can be replaced by the index flag K and a three-digit pointer value.

The payShield 9000 can be used in systems where there may be Atalla security equipment at other network nodes. This is achieved by the inclusion of an Atalla variant in those commands that translate a key from/to encryption under a ZMK. This has the effect of modifying the ZMK before it is used to decrypt/encrypt in accordance with the method used by the Atalla equipment. The payShield 9000 can support 1 or 2 digit Atalla variants.

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

Verify ISO PIN Block from Internet and Verify MAC using ANSI X9.19

Variant ☑	Key Block ☒
License: **HSM9-LIC002 & HSM9-LIC014**	
Authorization: **Not required**	

Function: To verify ISO PIN Block from Internet and verify MAC using ANSI X9.19.

State: Online

Notes: The PIN Block format is ANSI X9.8 (ISO95641-format 0). The PIN Block is encrypted by a 128-bit session PIN key (Triple-DES: Encrypt - Decrypt - Encrypt). The Session PIN Key and MAC Keys (both 128-bit) are derived from a Master Key encrypted under public key.

The PIN and MAC Message format together with the Key derivation algorithm are specified in Appendix A.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'XM'.
Encryption Identifier	2 N	Identifier of the algorithm used to encrypt the Master Key. Must be 01 for RSA. Provided for compatibility with standard HSM RSA Host commands. See payShield 9000 Host Programmer's Manual, Chapter 5 (Ref. 3)
Pad Mode Identifier	2 N	Identifier of the pad mode used in the encryption process. Must be 01 for PKCS#1. Provided for compatibility with standard HSM RSA Host commands. See payShield 9000 Host Programmer's Manual, Chapter 5 (Ref. 3)
Private Key Flag	2 N	Flag, indicates the location of the Private key. The number is the index of the stored private key, except 99 which means using the key supplied in the command.
Private Key length	4 N	Length (in bytes) of the next field (present only if the private key flag is 99).
Private Key	n B	Private Key, encrypted using LMK pair 34-35 (present only if the private key flag is 99).
Delimiter	1 A	Delimiter, indicates the end of the Private Key field. Value; (present only if the private key flag is 99).
Account Number	12 N	Account number for formation of locally stored encrypted PIN.
PIN	L N or L H	The locally stored PIN encrypted under LMK pair 02-03.
PIN and MAC Message Length	4 N	Length of PIN and MAC Message
PIN and MAC Message	n A	PIN and MAC Message as received from client – see Appendix A for Format
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'XN'.
Error Code	2 N	'00' : No errors. '01' : PIN verification failure. '02' : MAC Verification Failure. '03' : Invalid private key type. '04' : Invalid private key flag. '06' : Invalid encryption identifier. '07' : Invalid pad mode identifier. '13' : LMK error; report to supervisor. '14' : Error in PIN from Host. '15' : Error in input data. '20' : PIN Block Error. '21' : Invalid user storage index. '24' : PIN Length error. '47' : DSP error; report to supervisor. '49' : Private Key error; report to supervisor. '76' : Key block length error. '77' : Clear data block error. '78' : Private Key length error. '80' : Incorrect Message Length. '83' : Invalid Ver or Type in Message '84' : Invalid Ver or Usage in Master Key Or any standard error 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	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify ISO PIN Block from Internet, Verify MAC using ANSI X9.19 and Return New Encrypted PIN

Variant ☑	Key Block ☒
License: **HSM9-LIC002 & HSM9-LIC014**	
Authorization: **Not required**	

Function: To verify ISO PIN Block from Internet, verify MAC using ANSI X9.19 and return New PIN.

State: Online

Notes: The PIN Block format is ANSI X9.8 (ISO95641-format 0). The PIN Block is encrypted by a 128-bit session PIN key (Triple-DES: Encrypt - Decrypt – Encrypt). The Session PIN Key and MAC Key (both 128-bit) are derived from a Master Key encrypted under the public key.

Both old PIN and new PIN are supplied. After successful verification of old PIN, new PIN is translated to encryption under the LMK.

The Change PIN and MAC Message format together with the Key derivation algorithm are specified in Appendix A.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'XK'.
Encryption Identifier	2 N	Identifier of the algorithm used to encrypt the Master Key. Must be 01 for RSA. Provided for compatibility with standard HSM RSA Host commands. See payShield 9000 Host Programmer's Manual, Chapter 5 (Ref. 3)
Pad Mode Identifier	2 N	Identifier of the pad mode used in the encryption process. Must be 01 for PKCS#1. Provided for compatibility with standard HSM RSA Host commands. See payShield 9000 Host Programmer's Manual, Chapter 5 (Ref. 3)
Private Key Flag	2 N	Flag, indicates the location of the Private key. The number is the index of the stored private key, except 99 which means using the key supplied in the command.
Private Key length	4 N	Length (in bytes) of the next field (present only if the private key flag is 99).
Private Key	n B	Private Key, encrypted using LMK pair 34-35 (present only if the private key flag is 99).
Delimiter	1 A	Delimiter, indicates the end of the Private Key field. Value; (present only if the private key flag is 99).
Account Number	12 N	Account number for formation of locally stored encrypted PIN.
PIN	L N or L H	The locally stored PIN encrypted under LMK pair 02-03.
Change PIN and MAC Message Length	4 N	Length of Change PIN and MAC Message
Change PIN and MAC Message	n A	Change PIN and MAC Message as received from client – see Appendix A for Format
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'XL'.
Error Code	2 N	'00' : No error '01' : PIN verification failure Or any standard error code
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify MAC using ANSI X9.19

Variant ☑	Key Block ☒
License: **HSM9-LIC002 & HSM9-LIC014**	
Authorization: **Not required**	

Function: To verify MAC using ANSI X9.19.
State: Online
Notes: The Session MAC Key (128-bit) is itself encrypted under public key.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'XO'.
Encryption Identifier	2 N	Identifier of the algorithm used to encrypt the DES Key.
Pad Mode Identifier	2 N	Identifier of the pad mode used in the encryption process.
Encrypted MAC Key Length	4 N	Encrypted MAC Key Length (in bytes).
MAC Key	n B	MAC Key, encrypted under the public key.
Delimiter	1 A	Delimiter, indicates the end of the encrypted PIN Key field. Value ;
Private Key Flag	2 N	Flag, indicates the location of the Private key. The number is the index of the stored private key, except 99 which means using the key supplied in the command.
Private Key length	4 N	Length (in bytes) of the next field (present only if the private key flag is 99).
Private Key	n B	Private Key, encrypted using LMK pair 34-35 (present only if the private key flag is 99).
Delimiter	1 A	Delimiter, indicates the end of the Private Key field. Value; (present only if the private key flag is 99).
MAC	8 H	MAC.
Authentication Data Length	4 N	Length of Data to be authenticated.
Authentication Data	n A	Data to be authenticated.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'XP'.
Error Code	2 N	'00' : No errors. '02' : MAC Verification Failure. '03' : Invalid private key type. '04' : Invalid private key flag. '06' : Invalid encryption identifier. '07' : Invalid pad mode identifier. '10' : MAC Key parity error. '13' : LMK error; report to supervisor. '15' : Error in input data. '21' : Invalid user storage index. '47' : DSP error; report to supervisor. '49' : Private Key error; report to supervisor. '76' : Key block length error. '77' : Clear data block error. '78' : Private Key length error. '80' : Incorrect Data Length. Or any standard error code
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate MAC using ANSI X9.19

Variant ☑	Key Block ☒
License: **HSM9-LIC002 & HSM9-LIC014**	
Authorization: **Not required**	

Function: To Generate MAC using ANSI X9.19.

State: Online

Notes: The Session MAC Key (128-bit) is itself encrypted under public key.

The Encryption Identifier should be 01 (i.e. RSA algorithm). The Pad Mode Identifier should also be 01 (i.e. PKCS#1).

All message authentication functions supported by the HSM use ASCII characters. If the host is using EBCDIC character set and the HSM is configured using EBCDIC, the HSM will convert the incoming EBCDIC MAC data to ASCII characters, prior to MAC verification/generation. (Please refer to the EBCDIC-to-ASCII translation table in HSM Programmer's Manual.) If the final message block of the authentication data is not an exact multiple of 64 bits, it will be padded, to the right, with binary zeros.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'XQ'.
Encryption Identifier	2 N	Identifier of the algorithm used to encrypt the DES Key.
Pad Mode Identifier	2 N	Identifier of the pad mode used in the encryption process.
PK MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37 with Variant 1.
Public Key	n B	Public Key, DER encoded in ASN.1 format (sequence of modulus, exponent).
PK Authentication Data	n A	Optional. Additional data to be included in the PK MAC calculation for Public Key (must not include ;).
Delimiter	1 A	Delimiter, indicates the end of the PK authentication data field. Value ;
Authentication Data Length	4 N	Length of Data to be authenticated.
Authentication Data	n A	Data to be authenticated.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value XR'.
Error Code	2 N	'00' : No errors. '01' : Public Key MAC Verification failure. '04' : Public key does not conform encoding rules. '06' : Invalid encryption identifier. '07' : Invalid pad mode identifier. '13' : LMK error; report to supervisor. '15' : Error in input data. '47' : DSP error; report to supervisor. '76' : Public Key length error. '80' : Incorrect Data Length. Or any standard error code
MAC	8 H	MAC.
Encrypted MAC Key Length	4 N	Encrypted MAC Key Length (in bytes).
MAC Key	n B	MAC Key, encrypted under the public key.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate ISO PIN Block from Internet Verify MAC and Optionally Generate a MAC

Variant ☑	Key Block ☒
License: **HSM9-LIC002 & HSM9-LIC014**	
Authorization: **Not required**	

Function: To translate ISO PIN Block from Internet, verify MAC using ANSI X9.19 and optionally generate MAC using ANSI X9.9 or X9.19. The ZPK and ZAK can be 1, 2 or 3DES in the form of 16Hex, 1A+32Hex or 1A+48Hex.

State: Online

Notes: The PIN Block format is ANSI X9.8 (ISO95641-format 0). The input PIN Block is encrypted by a 128-bit session PIN key (Triple-DES: Encrypt - Decrypt - Encrypt). The Session PIN Key and MAC Keys (both 128-bit) are derived from a Master Key encrypted under public key.

The Encryption Identifier should be 01 (i.e. RSA algorithm). The Pad Mode Identifier should also be 01 (i.e. PKCS#1).

All message authentication functions supported by the HSM use ASCII characters. If the host is using EBCDIC character set and the HSM is configured using EBCDIC, the HSM will convert the incoming EBCDIC MAC data to ASCII characters, prior to MAC verification/generation. (Please refer to the EBCDIC-to-ASCII translation table in HSM Programmer's Manual.) If the final message block of the authentication data is not an exact multiple of 64 bits, it will be padded, to the right, with binary zeros.

The PIN and MAC Message format together with the Key derivation algorithm are specified in Appendix A.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'XS'.
Encryption Identifier	2 N	Identifier of the algorithm used to encrypt the Master Key. Must be 01 for RSA. Provided for compatibility with standard HSM RSA Host commands. See payShield 9000 Host Programmer's Manual, Chapter 5 (Ref. 3)
Pad Mode Identifier	2 N	Identifier of the pad mode used in the encryption process. Must be 01 for PKCS#1. Provided for compatibility with standard HSM RSA Host commands. See payShield 9000 Host Programmer's Manual, Chapter 5 (Ref. 3)
Private Key Flag	2 N	Flag, indicates the location of the Private key. The number is the index of the stored private key, except 99 which means using the key supplied in the command.
Private Key length	4 N	Length (in bytes) of the next field (present only if the private key flag is 99).
Private Key	n B	Private Key, encrypted using LMK pair 34-35 (present only if the private key flag is 99).
Delimiter	1 A	Delimiter, indicates the end of the Private Key field. Value; (present only if the private key flag is 99).
MAC Flag	1 N	Flag to indicate MAC Generation 1 = MAC Verification only 3 = MAC Verification and Generation
Destination ZPK	16 H or 1A+32H or 1A+48H	Destination ZPK, encrypted under LMK pair 06-07.
PIN and MAC Message	4 N	Length of PIN and MAC Message

Field	Length & Type	Details
Length		
PIN and MAC Message	n A	PIN and MAC Message as received from client – see Appendix A for Format
Delimiter	1 A	Value ";"
Destination ZAK	16 H or 1A+32H or 1A+48H	Destination ZAK, encrypted under LMK pair 26-27. (only present if MAC Flag is 3)
Output Authentication Data Length	4 N	Length of output authentication data to be authenticated (only present if MAC Flag is 3)
Output Authentication Data	n A	Output data to be authenticated. (only present if MAC Flag is 3)
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'XT'.
Error Code	2 N	'00' : No errors. '02' : MAC Verification Failure. '03' : Invalid private key type. '04' : Invalid private key flag. '06' : Invalid encryption identifier. '07' : Invalid pad mode identifier. '10' : Destination ZPK parity error. '11' : Destination ZAK 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. '47' : DSP error; report to supervisor. '49' : Private Key error; report to supervisor. '76' : Key block length error. '77' : Clear data block error. '78' : Private Key length error. '80' : Incorrect input message length. '81' : Incorrect output data length. '83' : Invalid Ver or Type in Message '84' : Invalid Ver or Usage in Master Key Or any standard error code
PIN Block	16 H	PIN Block, encrypted under Destination ZPK.
Destination MAC	8 H	Destination MAC, calculated using Destination ZAK. (only present if MAC Flag is 3)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Decrypt Data using TDES Data key

Variant ☑	Key Block ☒
License: **HSM9-LIC002 & HSM9-LIC014**	
Authorization: **Not required**	

Function: To decrypt data from Internet.

State: Online

Notes: The input Data Block is encrypted by a 128-bit session data key (Triple-DES: Encrypt - Decrypt - Encrypt). The Session Data Key (128-bit) from Internet is encrypted under public key. The data key should be translated to LMK pair 30-31 encryption by standard command "GI".

The TDES Electronic code book (TECB) and Cipher block chaining (TCBC) modes are supported. Both are defined in the ANSI X9.52 standard.

The TCBC mode requires an Initialization Value (IV) to be input with the command. When more than one message block needs to be decrypted, then the final 8 bytes of ciphertext obtained from the previous message block will be returned to the host for use as the IV for the next message block.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'XU'.
Message Block Number	1 N	Message block processing number 0 – Only block 1 – First block 2 – Second block 3 – Last block
Decryption Mode	1 N	Mode of operation 0 – ECB 1 – CB
Data Key	32 H	TDES Data Key encrypted under LMK pair 30-31.
IV	16 H	Initialization Value.
Encrypted Message Length	5 N	Message length, in bytes.
Encrypted Message Block	n B	The cipher text message block
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'XV.
Error Code	2 N	'00' : No errors. '04' : Invalid mode of operation. '05' : Invalid Message Block Number. '09' : Data 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. Or any standard error code
Decrypted Message Block	n B	The decrypted message block.
IV	16 H	Initialization Value, to be used as IV for the next message block. (only returned if Message Block Number = 1 or 2)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Encrypt Data using TDES Data key

Variant ☑	Key Block ☒
License: **HSM9-LIC002 & HSM9-LIC014**	
Authorization: **Not required**	

Function: To encrypt data.

State: Online

Notes: The input Data Block will be encrypted by a 128-bit session data key (Triple-DES: Encrypt - Decrypt - Encrypt). The Session Data Key (128-bit) from Internet is encrypted under public key. The data key should be translated to LMK pair 30-31 encryption by standard command "GI".

The TDES Electronic code book (TECB) and Cipher block chaining (TCBC) modes are supported. Both are defined in the ANSI X9.52 standard.

The TCBC mode requires an Initialisation Value (IV) to be input with the command. When more than one message block needs to be encrypted, then the final 8 bytes of ciphertext obtained from the previous message block will be returned to the host for use as the IV for the next message block.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'XW'.
Message Block Number	1 N	Message block processing number 0 – Only block 1 – First block 2 – Second block 3 – Last block
Decryption Mode	1 N	Mode of operation 0 – ECB 1 – CBC
Data Key	32 H	TDES Data Key encrypted under LMK pair 30-31.
IV	16 H	Initialization Value.
Message Length	5 N	Message length, in bytes.
Message Block	n B	The plaintext message block
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'XX'.
Error Code	2 N	'00' : No errors. '04' : Invalid mode of operation. '05' : Invalid Message Block Number. '09' : Data 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. Any standard error code
Encrypted Message Block	n B	The encrypted message block.
IV	16 H	Initialization Value, to be used as IV for the next message block. (only returned if Message Block Number = 1 or 2)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate a Random Alphanumeric PIN (AN-PIN)

Variant ☑	Key Block ☒
License: **HSM9-LIC014**	
Authorization: **Not Required**	

Function: Generate a Random Alphanumeric PIN and encrypt it under LMK pair 36-37 with Variant 1.

State: Online

Notes: A Random Alphanumeric PIN with character set 0 – 9, A – Z and a – z. It should not contain characters "0" (ASCII 30H), "O" (ASCII 4FH), "1" (ASCII 31H) and "l" (ASCII 49H and 6CH) to avoid confusion. No digits should occur more than 4 times.

The Alphanumeric PIN is left justified and padded with 0x20 (i.e. space character).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'ZA'.
Encrypted AN-PIN Length	1 N	Encrypted Alphanumeric PIN length 0 = 32 Hex - select this value when using the MD5 hash algorithm at the client 1 = 48 Hex - select this value when using the SHA-1 hash algorithm at the client
AN-PIN length	2 N	Length of Alphanumeric PIN to be generated. If Encrypted AN-PIN Length = 0, 06 <= AN-PIN Length <= 16 If Encrypted AN-PIN Length = 1, 06 <= AN-PIN Length <= 20
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ZB'.
Error Code	2 N	'00' : No errors. '04' : Invalid Encrypted AN-PIN Length. '13' : LMK error; report to supervisor. '15' : Error in input data. Or any standard error code
Encrypted AN-PIN	32 H or 48 H	The Alphanumeric PIN encrypted under LMK pair 36-37 with Variant 1. Length depends on Encrypted AN-PIN Length.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Print Alphanumeric PIN/Alphanumeric PIN and Solicitation Data

Variant ☑	Key Block ☒
License: **HSM9-LIC014**	
Authorization: **Required**	

Function: Print the Alphanumeric PIN/Alphanumeric PIN and solicitation data at the HSM-attached terminal.

State: Online

Notes: The HSM must be in Authorised state.
A printer must be attached to the HSM Auxiliary port.
The HSM must have a print format already defined.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'ZE'.
Document Type	1 A	A : for 1st mailer on a 2-up form. B : for 2nd mailer on a 2-up form. C : for a 1-up form.
Encrypted AN-PIN Length	1 N	Encrypted Alphanumeric PIN length 0 = 32 Hex 1 = 48 Hex
Encrypted AN-PIN	32 H or 48 H	The Alphanumeric PIN encrypted under LMK pair 36-37 with Variant 1.
Print Field 0	n A	The print field defined as Print Field 0 in the print format definition (must not contain a ; character).
Delimiter	1 A	Value ;.
Print Field 1	n A	The print field defined as Print Field 1 in the print format definition (must not contain a ; character).
.	.	.
.	.	.
.	.	.
Last Print Field	n A	The last print field defined in the print format definition (must not contain a ; character).
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (before printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ZF'.
Error Code	2 N	'00' : No errors. '04' : Invalid Encrypted AN-PIN Length. '13' : LMK error; report to supervisor. '14' : Error in encrypted PIN. '15' : Error in input data. '16' : Printer not ready. '17' : HSM not in authorised state. '18' : Document definition not loaded. Or any standard error code
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE (after printing)		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ZZ'.
Error Code	2 N	'00' : No errors. '16' : Printer not ready.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate Encrypted PIN to Encrypted Alphanumeric PIN (AN-PIN)

Variant ☑	Key Block ☒
License: **HSM9-LIC014**	
Authorization: **Not Required**	

Function: To translate encrypted PIN to encrypted Alphanumeric PIN under LMK pair 36-37 with Variant 1.

State: Online

Notes: Error 50 is returned, if this command is used to convert Original Encrypted PIN (OEP) encrypted under LMK pair 36-37 with Variant 1 to PIN Format Required (PFR) with input parameter = 0.

Also note that the PIN Format Required (PFR) parameter matches the Hash Mode given in Appendix A.1.5. A PFR value of 4 is not used in this command but is reserved for use as defined in the Appendix.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'ZM'.
Original Encrypted PIN (OEP)	1 N	Original encrypted PIN 0 = PIN encrypted under LMK pair 02-03 1 = Non-hashed AN-PIN encrypted under LMK pair 36-37 with variant (generated by "ZA" command)
PIN Format Required (PFR)	1 N	PIN Format to be returned to host 0 = Padding with "0x20"; used for JETCO 1 = MD5 for JETCO 2 = MD5 for WebPIN 3 = SHA-1 for WebPIN (Note, 4 = Reserved)
Account Number	12 N	The 12 right-most digits of the account number, excluding the check digit. (Only present when OEP = 0 "OR" PFR = 2 or 3)
Encrypted PIN	L N or L H	The PIN encrypted under LMK pair 02-03. (Only present when OEP = 0)
Encrypted AN-PIN	32 H	The AN-PIN encrypted under LMK pair 36-37 with Variant 1. (Only present when OEP = 1 "AND" PFR = 0, 1 or 2)
Encrypted AN-PIN	48 H	The AN-PIN encrypted under LMK pair 36-37 with Variant 1. (Only present when OEP = 1 "AND" PFR = 3)
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ZN'.
Error Code	2 N	'00' : No errors. '03' : Invalid Original Encrypted PIN code. '05' : Invalid PIN Format Required code. '13' : LMK error; report to supervisor. '14' : Error in encrypted PIN. '15' : Error in input data. '50' : Invalid combination. Or any standard error code
Encrypted AN-PIN	32 H	The Alphanumeric PIN encrypted under LMK pair 36-37 with Variant 1. (Only present when PIN Format Required (PFR) = 0 or 1 or 2)
Encrypted AN-PIN	48 H	The Alphanumeric PIN encrypted under LMK pair 36-37 with Variant 1. (Only present when PIN Format Required (PFR) = 3)
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Translate an Alphanumeric PIN from old LMK to new LMK Encryption

Variant ☑	Key Block ☒
License: **HSM9-LIC014**	
Authorization: **Not Required**	

Function: To translate an Alphanumeric PIN from encryption under the LMK pair held in "key change storage" to encryption under LMK pair 36-37 with Variant 1.

State: Online

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'ZK'.
Encrypted AN-PIN Length	1 N	Encrypted Alphanumeric PIN length 0 = 32 Hex 1 = 48 Hex
Encrypted AN-PIN	32 H or 48 H	The Alphanumeric PIN encrypted under the LMK pair in "key change storage".
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ZL'.
Error Code	2 N	'00' : No errors. '04' : Invalid Encrypted AN-PIN Length. '13' : LMK error; report to supervisor. '14' : Error in encrypted PIN. '15' : Error in input data. Or any standard error code
Encrypted AN-PIN	32 H or 48 H	The Alphanumeric PIN encrypted under new LMK pair 36-37 with Variant 1.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify Alphanumeric PIN Block from Internet and optionally, return new encrypted PIN and verify MAC using ANSI X9.19

Variant ☑	Key Block ☒
License: **HSM9-LIC002 & HSM9-LIC014**	
Authorization: **Not Required**	

Function: To verify AN-PIN Block from Internet and optionally, return new encrypted AN-PIN and verify MAC using ANSI X9.19.

State: Online

Notes: The Message is either in Alphanumeric PIN and MAC format, where only verification is carried out, or Alphanumeric Change PIN and MAC format where both verification of the old AN-PIN and return of the new AN-PIN is carried out. The Type field in these messages determines the format. The formats of these messages are defined in the Appendix.

The Alphanumeric PIN Block in the message is encrypted by a 128-bit session PIN key (Triple-DES: Encrypt - Decrypt - Encrypt). The Session PIN Key, the IV and also the MAC Key are derived from a Master Key which is in turn encrypted under a public key.

The TDES Electronic code book (TECB) and Cipher block chaining (TCBC) modes are supported. Both are defined in the ANSI X9.52 standard. The TCBC mode requires an Initialisation Value (IV) to be used when decrypting the Alphanumeric PIN.

The Master Key is delivered in a PKCS#1 HSM Key Block formatted as defined in Reference 2 HSM Programmer's Manual – RSA Section. The Master Key Format, is specified in Appendix A.2 and the Key Derivation Algorithm and Key Block Format are defined in Appendix A.3.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'ZU'.
Encryption Identifier	2 N	Identifier of the algorithm used to encrypt the Master Key. Must be 01 for RSA. Provided for compatibility with standard HSM RSA Host commands. See payShield 9000 Host Programmer's Manual, Chapter 5 (Ref. 3)
Pad mode identifier	2 N	Identifier of the pad mode used in the encryption process. Refer to the payShield 9000 Host Programmer's Manual, Chapter 5 (Ref. 3) for a description of this parameter.
Private Key Flag	2 N	Flag, indicates the location of the Private key. The number is the index of the stored private key, except 99 which means using the key supplied in the command.
Private Key length	4 N	Length (in bytes) of the next field (present only if the private key flag is 99).
Private Key	n B	Private Key encrypted using LMK pair 34-35 (present only if the private key flag is 99).
Delimiter	1 A	Delimiter indicates the end of the Private Key field. Value ;.
Encrypted AN-PIN Length	1 N	Encrypted Alphanumeric PIN length 0 = 32 Hex 1 = 48 Hex
Stored Alphanumeric PIN	32 H or 48 H	The alphanumeric PIN encrypted under LMK pair 36-37 with Variant 1. (from local storage) Depends on Encrypted AN-PIN Length.
Message Length	4 N	Length of AN-PIN and MAC Message (if Message Type = "10") OR

Field	Length & Type	Details
Message	n A	Length of A-N Change PIN and MAC Message (if Message Type = "11"). AN-PIN and MAC Message as received from client (if Message Type = "10") OR AN Change PIN and MAC Message as received from client (if Message Type = "11").
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'ZV'.
Error Code	2 N	'00' : No errors. '01' : PIN verification failure. '02' : MAC Verification Failure. '03' : Invalid private key index. '04' : Invalid private key flag. '06' : Invalid Encryption Identifier. '07' : Invalid pad mode identifier. '08' : Invalid IV. '13' : LMK error; report to supervisor. '14' : Error in Stored PIN from Host. '15' : Error in input data. '20' : Current AN-PIN Block Error. '21' : Invalid user storage index. '23' : Invalid Encrypted AN-PIN Length '24' : PIN Length error. '50' : New AN-PIN Block Error. '53' : Invalid AN-PIN Block Encryption Mode. '47' : DSP error; report to supervisor. '49' : Private Key error; report to supervisor. '76' : Key block length error. '77' : Clear data block error. '78' : Private Key length error. '80' : Incorrect Message Length '82' : Private Key field length error or missing field delimiter '83' : Invalid Ver or Type in Message '84' : Invalid Ver or Usage in Master Key '85' : Invalid Hash Mode or invalid Hash Mode and Encrypted AN-PIN Length combination Or any standard error code
New encrypted AN-PIN	32 H or 48 H	The new alphanumeric PIN encrypted under LMK pair 36-37 with Variant 1. (only present if Message Type is "11")
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Appendix A - Message Formats

A.0 Definitions and Conventions

Definitions

ASCII-Hex Encoded : this is a printable ASCII string representation of a byte array expressed in base 16 (i.e. HEX). For example, a unsigned long decimal value of 1234567 would be represented in ASCII-Hex encoding as the string "12D687"

Conventions

Array indexing in this document will begin from index 0. That is to say, that it will follow the normal conventions of the 'C' language.

Additionally, array ranges will be noted with the ellipse '..' characters. For example, indexing between 0 and 5 would be noted as, message[0..5]. The upper bound value can be parameterized for indeterminant upper range values. For example, a message of indeterminate length can be referenced as, message[2..n] with 2 being the starting index value and 'n' being the ending index value.

A.1 Message Formats

A.1.1 PIN and MAC Message Format

A PIN and MAC message has the following structure:

Ver	Type	HEMK	HEPB	Acct #	Data	Msg MAC

* **Ver** is the message version. Current version is "1".

* **Type** is the message type. The pin and mac message type is "05". This means that the message contains a hex encrypted master key, the hex encrypted pin block, the account number, the data, and the X9.19 DES-CBC MAC.

* **HEMK** is the Hex Encrypted Master Key. This field is 256 bytes long.

* **HEPB** is the Hex Encrypted PIN Block. This field is 16 bytes long.

* **Acct #** is the 12 digit account number (in ASCII form) used to form the PIN block. This field is 12 bytes long.

* **Data** is the message data. This field is variable length.

* **Msg MAC** is the X9.19 DES-CBC generated MAC of the entire message packet using the key derived from the HEMK. This field is the ASCII-Hex Encoded string of the resulting message MAC. This field will be 8 bytes in length.

A.1.2 Change PIN and MAC Message Format

A Change PIN and MAC message has the following structure:

Ver	Type	HEMK	HEPB-o	HEPB-n	Acct #	Data	Msg MAC

* **Ver** is the message version. Current version is "1".

* **Type** is the message type. The change pin and mac message type is "06". This means that the message contains a hex encrypted master key, the hex encrypted old pin block, the hex encrypted new pin block, the account number, the data, and the X9.19 DES-CBC MAC.

* **HEMK** is the Hex Encrypted Master Key. This field is 256 bytes long.

* **HEPB-o** is the old Hex Encrypted PIN Block. This field is 16 bytes long.

* **HEPB-n** is the new Hex Encrypted PIN Block. This field is 16 bytes long.

* **Acct #** is the 12 digit account number (in ASCII form) used to form the PIN block. This field is 12 bytes long.

* **Data** is the message data. This field is variable length.

* **Msg MAC** is the X9.19 DES-CBC generated MAC of the entire message packet using the key derived from the HEMK. This field is the ASCII-Hex Encoded string of the resulting message MAC. This field will be 8 bytes in length.

A.1.3 Alphanumeric PIN and MAC

An Alpha-numeric PIN and MAC message has the following structure:

Ver	Type	HEMK	HM	EM	HEANPB	Data	Msg MAC

* **Ver** is the message version. Current version is "1".

* **Type** is the message type. The Alpha-numeric pin and mac message type is "10". This means that the message contains a hex encrypted master key, the hex encrypted A-N pin block, the account number, the data, and the X9.19 DES-CBC MAC.

* **HEMK** is the Hex Encrypted Master Key. This field is 256 bytes long.

* **HM** is the Hash Mode used to generate the HEANPB. This field contains a ASCII character indicating the hash mode used to generate the HEANPB. This will also imply the length of the HEANPB field. Valid values for this field are:

  * "0" for NONE-SHORT (HEANPB will be 32 bytes long)
  * "1" for MD5-CLEAR (HEANPB will be 32 bytes long)
  * "2" for MD5-XOR (HEANPB will be 32 bytes long)
  * "3" for SHA1-XOR (HEANPB will be 48 bytes long)
  * "4" for NONE-LONG (HEANPB will be 48 bytes long)

This field is one byte long.

* **EM** is the encryption mode used for encrypting the pin block. Valid values for this field are:

  * "1" for DES-ECB
  * "2" for DES-CBC

This field is one byte long.

* **HEANPB** is the Hex Encrypted Alpha-Numeric PIN Block. This field is either 32 or 48 bytes long. See the HM field above for a description of how to determine the length of this field.

* **Data** is the message data. This field is variable length.

* **Msg MAC** is the X9.19 DES-CBC generated MAC of the entire message packet using the key derived from the HEMK. This field is the ASCII-Hex Encoded string of the resulting message MAC. This field will be 8 bytes in length.

A.1.4 Alphanumeric Change PIN and MAC

An Alpha-numeric Change PIN and MAC message has the following structure:

Ver	Type	HEMK	HM	EM	HEANPB-o	HEANPB-n	Data	Msg MAC

* **Ver** is the message version. Current version is "1".

* **Type** is the message type. The change A-N pin and mac message type is "11". This means that the message contains a hex encrypted master key, the hex encrypted old A-N pin block, the hex encrypted new A-N pin block, the account number, the data, and the X9.19 DES-CBC MAC.

* **HEMK** is the Hex Encrypted Master Key. This field is 256 bytes long.

* **HM** is the Hash Mode used to generate the HEANPB. This field contains a ASCII character indicating the hash mode used to generate the HEANPB. This will also imply the length of the HEANPB field. Valid values for this field are:

  * "0" for NONE-SHORT (HEANPB will be 32 bytes long)
  * "1" for MD5-CLEAR (HEANPB will be 32 bytes long)
  * "2" for MD5-XOR (HEANPB will be 32 bytes long)
  * "3" for SHA1-XOR (HEANPB will be 48 bytes long)
  * "4" for NONE-LONG (HEANPB will be 48 bytes long)

  This field is one byte long.

* **EM** is the encryption mode used for encrypting the pin block. Valid values for this field are:

  * "1" for DES-ECB
  * "2" for DES-CBC

  This field is one byte long.

* **HEANPB-o** is the old Hex Encrypted Alpha-Numeric PIN Block. This field is either 32 or 48 bytes long. See the HM field above for a description of how to determine the length of this field.

* **HEANPB-n** is the new Hex Encrypted Alpha-Numeric PIN Block. This field is either 32 or 48 bytes long. See the HM field above for a description of how to determine the length of this field.

* **Data** is the message data. This field is variable length.

* **Msg MAC** is the X9.19 DES-CBC generated MAC of the entire message packet using the key derived from the HEMK. This field is the ASCII-Hex Encoded string of the resulting message MAC. This field will be 8 bytes in length.

A.1.5 Hex Encrypted Alphanumeric PIN Block (HEANPB)

A Hex Encrypted Alphanumeric PIN Block (HEANPB) is a PIN block containing a transformed Alphanumeric PIN and (sometimes) the account number. The format and size of this PIN block will change, based upon its construction. There are 5 separate formats (or constructions) for this PIN block. These are:

* Hash Mode NONE-SHORT -- this is the AN-PIN, left-justified, and right-padded with 0x20 bytes out to a total length of 16 bytes. The AN-PIN must be <= 16 bytes. The resulting PIN block is ASCII-Hex encoded.

* Hash Mode NONE-LONG -- this is the AN-PIN, left-justified, and right-padded with 0x20 bytes out to a total length of 20 bytes. The AN-PIN must be <= 20 bytes. The resulting PIN block is ASCII-Hex encoded.

* Hash Mode MD5 -- this is the AN-PIN, hashed by MD5. The AN-PIN can be of arbitrary length. The resulting PIN block is 32 ASCII-Hex encoded bytes.

* Hash Mode MD5-XOR -- this is the AN-PIN, hashed by MD5. The result is then ASCII-Hex encoded, XOR'd with the right most 12 digits of the account number, and finally TDES encrypted. The resulting PIN block is 32 ASCII-Hex encoded bytes.

* Hash Mode SHA1-XOR -- this is the AN-PIN, hashed by SHA1. The result is then ASCII-Hex encoded, XOR'd with the right most 12 digits of the account number, padded with 8 random bytes, and finally TDES encrypted. The resulting PIN block is 48 ASCII-Hex encoded bytes.

A.2 Master Key Format and Hex Encrypted Master Key Format

A.2.1 Master Key Format

A Master Key is a piece of data which is used to derive subsequent related key sets and IVs.

It will have the following structure:

Ver	Usage	Key

Where:

* **Ver** is a single binary value representing the master key version. The Version field will be used for managing forwards compatibility issues. Currently, the only supported version value is 1.

* **Usage** is a single binary value representing the master key usage. This field will indicate the number, type, and usage parameters describing the keyset to be generated. Here are the supported usage types:

0x01 = keyset containing 1 double-length DES key for PIN encryption, a DES PIN IV, and 1 double-length MAC key for ANSI X9.19 MACing.
0x02 = Reserved
0x03 = Reserved
0x04 = Reserved

* **Key** is an array containing the actual master key bytes to be used for key derivation. The length of this value will always be 48 bytes.

A.2.2 Hex Encrypted Master Key (HEMK) Format

A Hex Encrypted Master Key (HEMK) is an RSA wrapped Master Key. This method always uses a 1024 bit RSA key.

The method employed is RSA v1.5 encryption with block type 02 of bytes making up the Master Key.

The resulting ciphertext is then converted into ASCII-Hex encoded form. Because this method always uses a 1024 bit RSA public key for wrapping, the resulting length of this field will always be 256 bytes.

A.3 Key Derivation Algorithm and Key Block Format

A.3.1 Key Derivation Algorithm

The key bytes derivation algorithm is based upon the mechanism defined in the SSL 3.0 specification. Specifically, we utilize a variation on their mechanism to generate the bytes used to populate the key buffers.

Here is the process:

1) Identify the total number of bytes necessary to be generated. This is done by adding up all of the related key bytes and IVs. Let's call this value KeyBlockLen.

2) Next, we'll generate the actual KeyBlock using the following algorithm:

```
KeyBlock =  SHA1('A' + Master Key) +
            SHA1('BB' + Master Key) +
            SHA1('CCC' + Master Key) + [...];
```

Until enough data has been generated (i.e. KeyBlockLen) to fill the KeyBlock. Any extra KeyBlock data is discarded.

3) Finally, partition the KeyBlock as needed for the required operation. Any unused or unallocated KeyBlock data is discarded. See the following subsection for details on the allocation schemes.

A.3.2 Key Block Format

How the KeyBlock is partitioned is based upon the usage byte of the Master Key. It is partitioned as follows:

Usage	Partitions
0x01	KeyBlock[0..15] = 2DES Key[16] (for PIN encryption) KeyBlock[16..23] = DES IV[8] KeyBlock[24..39] = X9.19 MAC Key[16]
0x02	Reserved.
0x03	Reserved.
0x04	Reserved.

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 <