THALES

cpl.thalesgroup.com

payShield 9000 v3.5

Host Command Reference Manual

Addendum For License LIC031 (Union Pay Commands)

1270A591-038

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
1270A591-038	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

Chapter 1 – Introduction

Purpose of these Host commands

These commands support the China UnionPay (CUP) IC Card specification for terminal, card, issuer requirements etc. The issuer is required to support online transaction processing from CUP IC card. It involves key management, application cryptogram calculation, message integrity and confidentiality for secure messaging.

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.

ARQC Verification and/or ARPC Generation (CUP)

Variant ☑	Key Block ☒
License: **HSM9-LIC031**	
Authorization: **Not required**	

Function: Validate an ARQC (or TC/AAC) and, optionally, generate an ARPC. Alternatively, the command can be used to generate an ARPC alone.

Notes: Diagnostic data is produced by this command only if the HSM is in Authorised State. The diagnostic data consists of a generated ARQC, which is returned to the host if verification of the supplied ARQC fails.

Padding:

According to Part 5 of CUP doc (JR/T 0025.5-2010) Appendix D.2 and clarification from CUP, the data for ARQC calculation should be padded. If the data is multiple of 8 bytes, the padding bytes "hex 80 00 00 00 00 00 00 00" should be padded at the end of data. If the data is not multiple of 8 bytes, a padding byte "hex 80" and multiple bytes of hex 00 (between 0 and 7) to make padded data in multiple of 8 bytes.

A flag in this command allows application to control if the above padding rule is applied to the transaction data in the command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'JS'.
Mode Flag	1 H	Mode of operation: 0 = Perform ARQC verification only 1 = Perform ARQC Verification and ARPC generation 2 = Perform ARPC Generation only
Scheme ID	1 N	Identifier of the CUP scheme 1 = CUP Card Key Derivation method (CUP ver4.2)
*MK-AC(LMK)	32H or 1A+32H	The Issuer Master Key for Application Cryptograms encrypted under Variant 1 of LMK pair 28-29.
PAN/PAN Sequence No	8 B	Pre-formatted PAN/PAN Sequence No.
ATC	2 B	Application Transaction Counter.
Padding Flag	1 N	Padding Flag to indicate if padding is applied to Transaction Data 0 = Input Transaction Data is not padded 1 = Input Transaction Data is padded Only present for Modes 0 and 1.
Transaction Data Length	2 H	Length of next field. Can be any length from 1 to 255 bytes. Only present for Modes 0 and 1.
Transaction Data	n B	Variable length data. Only present for Modes 0 and 1. If the data supplied is a multiple of 8 bytes, no extra padding is added. If it is not a multiple of 8 bytes, additional padding is added.
Delimiter	1A	Delimiter, to indicate end of Transaction Data, value ";". Only present for Modes 0 and 1.
ARQC/TC/AAC	8 B	ARQC/TC/AAC to be validated and/or used for ARPC generation. Present for Mode 0, 1 and 2.

Field	Length & Type	Details
ARC	2 B	Authorisation Response Code to be used for ARPC Generation. Not required for Mode Flag 0. Must be present for Mode Flag values '1' and '2'
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 'JT'.
Error Code	2 N	00 : No error 01 : Warning: ARQC/TC/AAC verification failed 03 : Invalid Padding Flag 04 : Mode Flag not 0, 1 or 2 05 : Unrecognized Scheme ID 10 : MK parity error 67 : Command not licensed 80 : Data length error 81 : Zero length Transaction Data 82 : Transaction Data length not multiple of 8 bytes Any standard error code
ARPC	8 B	The calculated ARPC. Only present for Modes 1 and 2 if no error is encountered.
Diagnostic data	8 B	Calculated ARQC/TC/AAC returned only if the error code is 01 and the HSM is in Authorised State.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Generate Secure Message with Integrity and optional Confidentiality for Message or Offline PIN Change (CUP)

Variant ☑	Key Block ☒
License: **HSM9-LIC031**	
Authorization: **Not required**	

Function: Generate a Secure Message with Integrity over data to be sent from the Issuer back to the Card. Optionally, Secure Messaging with Confidentiality for Message or Offline PIN Change.

Notes: Padding:
According to Part 5 of CUP doc (JR/T 0025.5-2010) Appendix C.2.4, the data for MAC calculation should be padded. If the data is multiple of 8 bytes, the padding bytes "hex 80 00 00 00 00 00 00 00" should be padded at the end of data. If the data is not multiple of 8 bytes, a padding byte "hex 80" and multiple bytes of hex 00 (between 0 and 7) to make padded data in multiple of 8 bytes.
A flag in this command allows application to control if the above padding rule is applied to the transaction data in the command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'JU'.
Mode Flag	1 N	Mode of operation: 0 = Provide only Integrity functionality 1 = Provide Integrity and Confidentiality for message, using the same Issuer Master Key. 2 = Provide Integrity and Confidentiality for message, using different Issuer Master Keys 3 = Provide Integrity and Confidentiality for PIN Change, using the same Issuer Master Key. 4 = Provide Integrity and Confidentiality for PIN Change, using different Issuer Master Keys.
Scheme ID	1 N	Identifier of the CUP scheme; 1 = CUP using Card Key Derivation method (CUP ver 4.2)
*MK-SMI(LMK)	32 H or 1A+32H	The Master Key for Secure Messaging with Integrity encrypted under Variant 2 of LMK pair 28-29.
PAN/PAN Sequence No	8 B	Pre-formatted PAN/PAN Sequence number
ATC	2 B	Application Transaction Counter.
Padding Flag	1 N	Padding Flag to indicate if padding is applied to Plaintext Message Data 0 = Input Plaintext Message Data is not padded 1 = Input Plaintext Message Data is padded
MAC Message Data Length	4 H	Length in bytes of data in next field.
MAC Message Data	n B	MAC Message Data.
Delimiter	1 A	Delimiter of previous field, ";".
*MK-SMC(LMK)	32 H or 1A+32H	The Master Key for Secure Messaging with Confidentially encrypted under Variant 3 of LMK pair 28-29. Only present if Mode Flag = 2 or 4.
Offset	4 H	Position within MAC message data to insert Encrypted New PIN Block or re-encrypted data. Must be between 0000 and MAC Message Data length. If Offset = n,

Field	Length & Type	Details
		Encrypted New PIN Block or re-encrypted data is inserted AFTER the nth byte of the MAC message data. (i.e. if length of Plaintext data or re-encrypted data is 0039, and Offset is 39, Encrypted New PIN Block is placed at the end of the plaintext message.) Only present if Mode Flag = 1, 2, 3 or 4.
Plaintext Message Data Length	4 H	Length in bytes of data in next field. Only present if Mode Flag = 1 or 2
Plaintext Message Data	n B	Plaintext Message Data. Only present if Mode Flag = 1 or 2
Delimiter	1 A	Delimiter of previous field, ";". Only present if Mode Flag = 1 or 2
Source PIN Encryption Key Type	1 N	0 = ZPK 1 = TPK Only present if Mode Flag = 3 or 4
Source PIN Encryption Key	16 H or 1A+32H or 1A+48H	Source PIN Encryption Key, encryption depending on the Source PIN Encryption Key Type:- ZPK: encrypted under LMK pair 06-07 variant 0 TPK: encrypted under LMK pair 14-15 variant 0 if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N" or LMK pair 36-37 variant 7 if the setting has the value "Y" Only present if Mode Flag = 3 or 4
Source PIN Block Format	2 N	The format code for the source PIN block. Only Present if Mode Flag = 3 or 4.
Account Number	12 N or 18 H	Only Present if Mode Flag = 3 or 4. This field is used for PIN block translation. For a Source PIN Block Format ≠ 04, this field has length 12 N, and specifies the 12 right most digits of the account number, excluding the check digit. For a Source PIN Block Format = 04, this field has length 18 N, and specifies the entire 18 digit account number, excluding the check digit, padded with X'Fs on the left.
Destination PIN Block Format	1 N	The format code for the destination PIN block. 1 : destination PIN block with current (old) PIN 2 : destination PIN block without current (old) PIN Only Present if Mode Flag = 3 or 4.
Source New PIN Block	16 H	Source New PIN Block Only Present if Mode Flag = 3 or 4.
Source Current PIN Block	16 H	Source Current PIN Block Only Present if Mode Flag = 3 or 4 and Destination PIN Block Format = 1.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'JV'.
Error Code	2 N	00 : No error 03 : Invalid Padding Flag 04 : Mode flag not set to 0, 1, 2, 3 or 4 05 : Unrecognised Scheme-ID 06 : Invalid Offset 09 : ZPK/TPK parity error 10 : MK-SMI parity error 11 : MK-SMC parity error 23 : Invalid Source PIN block format 50 : Source PIN Encryption Key Type, not set to 0 or 1 51 : Invalid Destination PIN Block Format 52 : Invalid Source New PIN Block 53 : Invalid Source Current PIN Block 67 : Command not licensed 80 : MAC Message Data length error 81 : Plaintext Message Data Length error 82 : Data length not multiple of 8 bytes Any standard error code
MAC	8 H	The calculated 4 byte MAC.
Encrypted Destination New PIN Block Data	32 H	Encrypted Destination New PIN Block Data Only Present if Mode Flag = 3 or 4.
Ciphertext Message Data Length	4 H	Ciphertext Message Data Length (i.e. length of next field) Only Present if Mode Flag = 1 or 2.
Ciphertext Message Data	n B	Ciphertext Message Data Only Present if Mode Flag = 1 or 2.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

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 <