THALES

cpl.thalesgroup.com

payShield 9000 v3.5

Host Command Reference Manual Addendum for License LIC034 (MU & MW Commands)

1270A614-038

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
1270A614-038	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 provide legacy support for the MU and MW host commands implemented in the RG6000 Host Security Module to generate and verify MACs on binary messages.

These commands may be used only where backwards compatibility with old HSMs and Host applications is required. In all other cases, the M6 and M8 commands available in Optional License LIC008 Data Protection should be used.

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.

Generate a MAC on a Binary Message

Variant ☑	Key Block ☒
License: **HSM9-LIC034**	
Authorization: **Not required**	

Function: Generate a MAC on a binary message.

Note: This command is superseded by host command 'M6'.
If the Host is unable to support binary data transfers, the command can be used in standard (ASCII character) asynchronous mode (in which the message to be MACed is transferred in expanded hexadecimal notation).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MU'.
Mode number	1 N	The MAC calculation mode number: 0 to 3. 0: The only block. 1: The first block. 2: A middle block. 3: The last block.
TAK	16 H or 1 A + 32/48 H	The TAK used to generate the MAC, encrypted under LMK 16-17.
Initialization Vector	16 H	Modes 2, 3. IV returned from either mode 1 or 2 encrypted under variant 1 of LMK pair 16-17.
EITHER		
For Binary Communications Modes:		
Message length	3 H	'001' ... '320' indicating the length of the next field.
Message text	n B	1 to 800 bytes of message.
OR		
For Standard Async Communications Mode:		
Message length	3 H	'002' ... '320' indicating the length of the next field.
Message	n H	2 to 800 hexadecimal characters representing 1 to 400 bytes of message.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'MV'.
Error Code	2 A	'00' : No error '10' : TAK parity error '68' : Command disabled or a standard error code.
IV	16 H	Present only in modes 1 and 2. The IV encrypted under variant 1 of LMK pair 16-17.
MAC	8 H	Present only in modes 0 and 3.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Verify a MAC on a Binary Message

Variant ☑	Key Block ☒
License: **HSM9-LIC034**	
Authorization: **Not required**	

Function: Verify a MAC on a binary message.

Note: This command is superseded by host command 'M8'.
If the Host is unable to support binary data transfers, the command can be used in standard 7-bit asynchronous mode, whereupon the message to be MACed is transferred in expanded hexadecimal notation.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'MW'.
Mode number	1 N	The MAC calculation mode number: 0 to 3. 0: The only block. 1: The first block. 2: A middle block. 3: The last block.
TAK	16 H or 1 A + 32/48 H	TAK encrypted under LMK 16-17.
Initialization Vector	16 H	Modes 2, 3. IV returned from either mode 1 or 2 encrypted under variant 1 of LMK pair 16-17.
MAC	8 H	Modes 0, 3. The MAC received with the unsolicited message.
EITHER		
For Binary Communications Modes:		
Message length	3 H	'001' ... '320' indicating the length of the next field.
Message text	n B	1 to 800 bytes of message.
OR		
For Standard Async Communications Mode:		
Message length	3 H	'002' ... '320' indicating the length of the next field.
Message	n H	2 to 800 hexadecimal characters representing 1 to 400 bytes of message.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value 'MX'.
Error Code	2 A	'00' : No error '01' : MAC verification failure '10' : TAK parity error '68' : Command disabled or a standard error code.
IV	16 H	Present only in modes 1 and 2. The IV encrypted under variant 1 of LMK pair 16-17.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

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 <