

payShield 9000 v3.5

Host Command Reference Manual Addendum for Optional License LIC017 (HE & HG Commands)

1270A589-038

26 July 2021



Contents

CONTENTS	2
END USER LICENSE AGREEMENT.....	3
REVISION STATUS.....	4
REFERENCES.....	5
CHAPTER 1 – INTRODUCTION.....	6
PURPOSE OF THESE HOST COMMANDS	6
KEY TYPE CODES	6
KEY TYPE TABLE	6
KEY BLOCK LMK SUPPORT	6
LIST OF HOST COMMANDS (ALPHABETICAL)	6
CHAPTER 2 – HOST COMMANDS.....	7
GENERAL.....	7
<i>Encrypt Data Block.....</i>	<i>8</i>
<i>Decrypt Data Block</i>	<i>9</i>

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
1270A589-038	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 HE and HG commands implemented in the RG6000 Host Security Module to encrypt and decrypt data using key type TAK. They support the encryption and decryption of a single 64-bit block of data. This must be passed to the HSM as 16 hexadecimal characters. The HSM returns the result also as 16 hexadecimal characters.

These commands may be used only where backwards compatibility with old HSMs and Host applications is required. In all other cases, the M0 and M2 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)

Host Command (Response)	Function	Page
HE (HF)	Encrypt Data Block	8
HG (HH)	Decrypt Data Block	9

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.

Encrypt Data Block

Variant <input checked="" type="checkbox"/>	Key Block <input checked="" type="checkbox"/>
License: HSM9-LIC017	
Authorization: Not required	

Function: Encrypt a 64-bit data block with a TAK.

Notes: This command has been superseded by the M0 command, and should only be used where compatibility with legacy Host applications is required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'HE'.
TAK	16 H or 1 A + 32/48 H	The TAK encrypted under LMK pair 16-17 variant 0.
Data	16 H	The data to be encrypted.
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 'HF'.
Error Code	2 N	'00' : No error '10' : 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 or a standard error code.
Data	16 H	The data received in the command message encrypted under the LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.

Decrypt Data Block

Variant <input checked="" type="checkbox"/>	Key Block <input checked="" type="checkbox"/>
License: HSM9-LIC017	
Authorization: Not required	

Function: Decrypt a 64-bit data block with a TAK.

Notes: This command has been superseded by the M2 command, and should only be used where compatibility with legacy Host applications is required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'HG'.
TAK	16 H or 1 A + 32/48 H	The TAK encrypted under LMK pair 16-17 variant 0.
Data	16 H	The data to be decrypted.
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 'HH'.
Error Code	2 N	'00' : No error '10' : 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 or a standard error code.
Data	16 H	The data received in the command message decrypted under the LMK.
End Message Delimiter	1 C	Present only if present in the command message. Value X'19.
Message Trailer	n A	Present only if present in the command message. Maximum length 32 characters.



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](mailto: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](mailto:CPL_Sales_EMEA_TG@thalesgroup.com)

> cpl.thalesgroup.com <

