THALES

cpl.thalesgroup.com

payShield 9000 v3.5

Host Command Reference Manual

Addendum for License LIC020 (SEED Algorithm Commands)

1270A590-038

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 provide support for the SEED key block cipher developed by KISA (Korea Information Security Agency).

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.

SEED Key Scheme

The HSM supports the use of SEED keys using the key scheme "J":

Key Scheme Tag	Notes
J	Encryption of 128-bit SEED keys using the Thales Variant LMK.

The following host commands support the use of SEED keys using the "J" key scheme:

A0, A6, A8, AI, AK, AM, AO, G2, G4, G6, G8

The following console commands support the use of SEED keys using the "J" key scheme:

GC, FK, KG, KE, IK

Note: The procedure for generating a key check value for a SEED key is not currently defined, and therefore all SEED keys will have a key check value of "000000".

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 an Interchange PIN using the comparison method with SEED encryption algorithm

Variant ☑	Key Block ☒
License: **HSM9-LIC020**	
Authorization: **Not required**	

Function: Verify a PIN received from interchange by comparing it with a value held on the host database

State: Online

Notes: This command is similar to standard host command "BE" in input/output and command processing. But PIN Block is encrypted using SEED algorithm.

SEED algorithm is a block cipher with 16 bytes output and input. As the standard PIN Block is 8 bytes, 8 bytes of pad character (0x08) is added at the end of the PIN Block (before encryption) as below:

Standard PIN Block (8 bytes) || 0x08 08 08 08 08 08 08 08

The command is not required to check the pad character (0x08) after decryption. The command will extract the standard PIN Block (8 bytes) and follow the standard processing/validation of the PIN Block.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'G2'.
ZPK	1A+32H	For a Variant LMK, the ZPK must be encrypted under LMK pair 06-07 variant 0. Note: All SEED keys must use the "J" key scheme.
PIN Block	32 H	The PIN block containing the PIN for verification; encrypted under the ZPK
PIN Block format code	2 N	One of the valid PIN block format codes – see Chapter 6 of the General Information Manual for details
Account Number	12 N or 18 H	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.
PIN	L N or L H	The PIN from the host database encrypted under the LMK
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 'G3'.
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 a Terminal PIN using the comparison method with SEED encryption algorithm

Variant ☑	Key Block ☒
License: **HSM9-LIC020**	
Authorization: **Not required**	

Function: Verify a PIN receive from an ATM (or terminal etc.) by comparing it with a value held on the host database

State: Online

Notes: This command is similar to standard host command "BC" in input/output and command processing. But PIN Block is encrypted using SEED algorithm.

SEED algorithm is block cipher with 16 bytes output and input. As standard PIN Block is 8 bytes, 8 bytes of pad character (0x08) is padded at the end of PIN Block (before encryption) as below:

Standard PIN Block (8 bytes) || 0x08 08 08 08 08 08 08 08

The command is not required to check the pad character (0x08) after decryption. The command will extract the standard PIN Block (8 bytes) and follow the standard processing/validation of the PIN Block.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'G4'.
TPK	1A+32H	For a Variant LMK, the TPK must be 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". Note: All SEED keys must use the "J" key scheme.
PIN Block	32 H	The PIN block containing the PIN for verification; encrypted under the ZPK
PIN Block format code	2 N	One of the valid PIN block format codes – see Chapter 6 of the General Information Manual for details
Account Number	12 N or 18 H	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.
PIN	L N or L H	The PIN from the host database encrypted under the LMK
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 'G5'.
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.

Translate a PIN from one ZPK to another ZPK with SEED encryption algorithm

Variant ☑	Key Block ☒
License: **HSM9-LIC020**	
Authorization: **Not required**	

Function: Translate a PIN Block from encryption under one ZPK to encryption under another ZPK and from one format to another. If the same ZPK is defined, only the PIN block is translated, and if the same PIN block format is defined, only the key is translated.

State: Online

Notes: This command is similar to standard host command "CC" in input/output and command processing. But PIN Block is encrypted using SEED algorithm.

SEED algorithm is block cipher with 16 bytes output and input. As standard PIN Block is 8 bytes, 8 bytes of pad character (0x08) is padded at the end of PIN Block (before encryption) as below:

Standard PIN Block (8 bytes) || 0x08 08 08 08 08 08 08 08

The command is not required to check the pad character (0x08) after decryption. The command will extract the standard PIN Block (8 bytes) and follow the standard processing/validation of the PIN Block.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'G6'.
Source ZPK	1A+32H	For a Variant LMK, the Source ZPK must be encrypted under LMK pair 06-07 variant 0. Note: All SEED keys must use the "J" key scheme.
Destination ZPK	1A+32H	For a Variant LMK, the Destination ZPK must be encrypted under LMK pair 06-07 variant 0. Note: All SEED keys must use the "J" key scheme.
Maximum PIN Length	2 N	Value '12'.
Source PIN Block	32 H	The source PIN block encrypted under the source ZPK.
Source PIN Block Format Code	2 N	One of the valid PIN block format codes for source PIN Block – see Chapter 6 of the General Information Manual for details.
Destination Source PIN Block Format Code	2 N	One of the valid PIN block format codes for destination PIN Block – see Chapter 6 of the General Information Manual for details
Account Number	12 N or 18 H	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.
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 'G7'.
Error Code	2 N	'00' : No error '88' : Warning: PIN Block contains a zero length PIN Or any standard error code
PIN Length	2 N	Length of the returned PIN
Destination PIN Block	32 H	The destination PIN block encrypted under the destination ZPK
Destination PIN Block Format code	2 N	As received in the command message
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 a PIN from TPK to ZPK with SEED encryption algorithm

Variant ☑	Key Block ☒
License: **HSM9-LIC020**	
Authorization: **Not required**	

Function: Translate a PIN Block from encryption under TPK to encryption under another ZPK and from one format to another. If the same PIN block format is defined, only the key is translated.

State: Online

Notes: This command is similar to standard host command "CA" in input/output and command processing. But PIN Block is encrypted using SEED algorithm.

SEED algorithm is block cipher with 16 bytes output and input. As standard PIN Block is 8 bytes, 8 bytes of pad character (0x08) is padded at the end of PIN Block (before encryption) as below:

Standard PIN Block (8 bytes) || 0x08 08 08 08 08 08 08 08

The command is not required to check the pad character (0x08) after decryption. The command will extract the standard PIN Block (8 bytes) and follow the standard processing/validation of the PIN Block.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'G8'.
Source TPK	1A+32H	For a Variant LMK, the Source TPK must be 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". Note: All SEED keys must use the "J" key scheme.
Destination ZPK	1A+32H	For a Variant LMK, the Destination ZPK must be encrypted under LMK pair 06-07. Note: All SEED keys must use the "J" key scheme.
Maximum PIN Length	2 N	Value '12'.
Source PIN Block	32 H	The source PIN block encrypted under the source TPK.
Source PIN Block Format Code	2 N	One of the valid PIN block format codes for source PIN Block – see Chapter 6 of the General Information Manual for details.
Destination Source PIN Block Format Code	2 N	One of the valid PIN block format codes for destination PIN Block – see Chapter 6 of the General Information Manual for details
Account Number	12 N or 18 H	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.
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 'G9'.
Error Code	2 N	'00' : No error '88' : Warning: PIN Block contains a zero length PIN Or any standard error code
PIN Length	2 N	Length of the returned PIN
Destination PIN Block	32 H	The destination PIN block encrypted under the destination ZPK
Destination PIN Block Format code	2 N	As received in the command message
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 Block with SEED algorithm

Variant ☑	Key Block ☒
License: **HSM9-LIC020**	
Authorization: **Not required**	

Function: Encrypt a block of data with SEED algorithm.

State: Online

Notes: This command is similar to standard host command "M0" in input/output and command processing. But the algorithm is SEED algorithm.

If a ZEK is used as the encryption key, the contents of the plaintext message must comply with the CS "ZEK encryption" setting. This imposes certain restrictions on the contents of the message.

There are no restrictions on the contents of the message when a DEK key is used.

The data to be encrypted by this command may be presented to the HSM in different formats, as indicated by the Input Format Flag field.

Note: When Input Format Flag = 2, the input message goes through a conversion process (from EBCDIC to ASCII) when the HSM is configured as using EBCDIC.

Note: No padding is applied – the input message must be a multiple of 16 (or 32 for hex-encoded messages).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AI'.
Mode Flag	2 N	Describes the encryption mode: '00' : ECB '01' : CBC (requires IV) '02' : CFB8 (requires IV) '03' : CFB128 (requires IV).
Input Format Flag	1 N	Describes the format of the input message: '0' : Binary '1' : Hex-Encoded Binary '2' : Text.
Output Format Flag	1 N	Describes the format of the output message: '0' : Binary '1' : Hex-Encoded Binary
Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be used. The following key types are permitted: '00A' : ZEK (encrypted under LMK pair 30-31) '00B' : DEK (encrypted under LMK pair 32-33).
Key	1A+32H	For a Variant LMK, the 'Key' is either a ZEK or DEK as specified above. Note: All SEED keys must use the "J" key scheme.
IV	32 H	The input IV, used in conjunction with the encryption Key. When encrypting the first of a series of blocks, this initial IV should be set by the caller – a typical initial IV is { 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 }. For subsequent blocks, this value should be the IV returned from encrypting the previous block. Only present if the Mode Flag is '01', '02' or '03'.

Field	Length & Type	Details
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes. This must be a multiple of 16 for binary and text formatted messages, or a multiple of 32 for hex-encoded binary messages.
Message	n B or n H or n A	The message to be encrypted. The length & type of the field will depend on the value of the Input Format Flag: Input Format Flag = '0' (Binary); n = multiple of 16. Input Format Flag = '1' (Hex-Encoded Binary); n = multiple of 32. Input Format Flag = '2' (Text); n = multiple of 16.
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 'AJ'.
Error Code	2 N	00 : No error 02 : Invalid Mode Flag field 03 : Invalid Input Format Flag field 04 : Invalid Output Format Flag field 05 : Invalid Key Type field 06 : Invalid Message Length field 35 : Illegal Message Format 67 : Command not licensed 68 : command disabled Any standard error code
IV	32 H	The output IV. When encrypting a series of blocks, this IV should be supplied as input when encrypting the next block. Only present if the Mode Flag is 01, 02 or 03.
Message Length	4 H	The length of the following field, in bytes.
Encrypted Message	n B or n H	The encrypted message. The length & type of the field will depend on the value of the Output Format Flag: Output Format Flag = '0' (Binary); n = multiple of 16. Output Format Flag = '1' (Hex-Encoded Binary); n = multiple of 32.
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 with SEED algorithm

Variant ☑	Key Block ☒
License: **HSM9-LIC020**	
Authorization: **Not required**	

Function: Decrypt a block of data with SEED algorithm.

State: Online

Notes: This command is similar to standard host command "M2" in input/output and command processing. But the algorithm is SEED algorithm.

If a ZEK is used as the encryption key, the contents of the plaintext message must comply with the CS "ZEK encryption" setting. This imposes certain restrictions on the contents of the message.

There are no restrictions on the contents of the message when a DEK key is used.

The decrypted data block may be returned to the host in different formats, as indicated by the Output Format Flag field.

Note: When Input Format Flag = 2, the input message goes through a conversion process (from EBCDIC to ASCII) when the HSM is configured as using EBCDIC.

Note: No padding is applied – the input message must be a multiple of 16 (or 32 for hex-encoded messages).

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AK'.
Mode Flag	2 N	Describes the encryption mode: '00' : ECB '01' : CBC (requires IV) 02' : CFB8 (requires IV) '03' : CFB128 (requires IV).
Input Format Flag	1 N	Describes the format of the output message: '0' : Binary '1' : Hex-Encoded Binary
Output Format Flag	1 N	Describes the format of the input message: '0' : Binary '1' : Hex-Encoded Binary '2' : Text.
Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be used. The following key types are permitted: '00A' : ZEK (encrypted under LMK pair 30-31) '00B' : DEK (encrypted under LMK pair 32-33).
Key	1A+32H	For a Variant LMK, the 'Key' is either a ZEK or DEK as specified above. Note: All SEED keys must use the "J" key scheme.
IV	32 H	The input IV, used in conjunction with the encryption Key. When encrypting the first of a series of blocks, this initial IV should be set by the caller – a typical initial IV is { 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 }. For subsequent blocks, this value should be the IV returned from encrypting the previous block. Only present if the Mode Flag is '01', '02' or '03'.

Field	Length & Type	Details
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes. This must be a multiple of 16 for binary and text formatted messages, or a multiple of 32 for hex-encoded binary messages.
Encrypted Message	n B or n H	The encrypted message. The type of the message will depend on the value of the Format Flag field: Input Format Flag = '0' (Binary); n = multiple of 16. Input Format Flag = '1' (Hex-Encoded Binary); n = multiple of 32.
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 'AL.
Error Code	2 N	00 : No error 02 : Invalid Mode Flag field 03 : Invalid Input Format Flag field 04 : Invalid Output Format Flag field 05 : Invalid Key Type field 06 : Invalid Message Length field 35 : Illegal Message Format 67 : Command not licensed 68 : command disabled Any standard error code
IV	32 H	The output IV. When decrypting a series of blocks, this IV should be supplied as input when encrypting the next block. Only present if the Mode Flag is 01, 02 or 03.
Message Length	4 H	The length of the following field, in bytes.
Decrypted Message	n B or n H or n A	The decrypted message. The type of the field will depend on the value of the Output Format Flag: Output Format Flag = '0' (Binary); n = multiple of 16. Output Format Flag = '1' (Hex-Encoded Binary); n = multiple of 32. Output Format Flag = '0' (Text); n = multiple of 16.
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 Data Block with SEED algorithm

Variant ☑	Key Block ☒
License: **HSM9-LIC020**	
Authorization: **Not required**	

Function: Translate a block of data from encryption under one key, to encryption under another key with SEED algorithm.

State: Online

Notes: This command is similar to standard host command "M4" in input/output and command processing. But the algorithm is SEED algorithm.

The data to be translated by this command may be presented to the HSM in different formats, as indicated by the Input Format Flag field.

The translated data block may be returned to the host in different formats, as indicated by the Output Format Flag field.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AM'.
Source Mode Flag	2 N	'00' : ECB '01' : CBC (requires IV) '02' : CFB8 (requires IV) '03' : CFB128 (requires IV).
Destination Mode Flag	2 N	'00' : ECB '01' : CBC (requires IV) '02' : CFB8 (requires IV) '03' : CFB128 (requires IV).
Input Format Flag	1 N	Describes the format of the output message: '0' : Binary '1' : Hex-Encoded Binary
Output Format Flag	1 N	Describes the format of the input message: '0' : Binary '1' : Hex-Encoded Binary
Source Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be used. The following key types are permitted: '00A' : ZEK (encrypted under LMK pair 30-31) '00B' : DEK (encrypted under LMK pair 32-33).
Source Key	1A+32H	For a Variant LMK, the 'Key' is either a ZEK or DEK as specified above. Note: All SEED keys must use the "J" key scheme.
Destination Key Type	3 H	For a Variant LMK: Indicates the key type of the key to be used. The following key types are permitted: '00A' : ZEK (encrypted under LMK pair 30-31) '00B' : DEK (encrypted under LMK pair 32-33).
Destination Key	1A+32H	For a Variant LMK, the 'Key' is either a ZEK or DEK as specified above. Note: All SEED keys must use the "J" key scheme.
Source IV	32 H	The source IV, used in conjunction with the source Key. When translating the first of a series of blocks, this initial Source IV should match the initial IV used to encrypt the original message. For subsequent blocks, this value should be the Source IV returned from translating the previous block.

Field	Length & Type	Details
		Only present if the Mode Flag is '01', '02' or '03'.
Destination IV	32 H	The input IV, used in conjunction with the Destination Key. When translating the first of a series of blocks, this initial Destination IV should be set by the caller – a typical value IV is { 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 }. For subsequent blocks, this value should be the Destination IV returned from translating the previous block. Only present if the Destination Mode Flag is '01', '02' or '03'.
Message Length	4 H	The length of the following field, in bytes. Maximum: X'7D00 (32000) bytes. This must be a multiple of 16 for binary and text formatted messages, or a multiple of 32 for hex-encoded binary messages.
Encrypted Message	n B or n H	The encrypted message. The type of the message will depend on the value of the Format Flag field: Input Format Flag = '0' (Binary); n = multiple of 16. Input Format Flag = '1' (Hex-Encoded Binary); n = multiple of 32.
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 'AN'.
Error Code	2 N	00 : No error 02 : Invalid Mode Flag field 03 : Invalid Input Format Flag field 04 : Invalid Output Format Flag field 05 : Invalid Key Type field 06 : Invalid Message Length field 35 : Illegal Message Format 67 : Command not licensed 68 : command disabled Any standard error code
Source IV	32 H	The output IV, calculated using the Source Key. When translating a series of blocks, this Source IV should be supplied as input when encrypting the next block. Only present if the Source Mode Flag is 01, 02 or 03.
Destination IV	32 H	The output IV, calculated using the Destination Key. When translating a series of blocks, this Destination IV should be supplied as input when encrypting the next block. Only present if the Destination Mode Flag is 01, 02 or 03.
Message Length	4 H	The length of the following field, in bytes.
Translated Message	n B or n H	The translated message. The length & type of the field will depend on the value of the Output Format Flag: Output Format Flag = '0' (Binary); n = multiple of 16. Output Format Flag = '1' (Hex-Encoded Binary); n = multiple of 32.
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 Round Key from SEED Key

Variant ☑	Key Block ☒
License: **HSM9-LIC020**	
Authorization: **Required** Activity: **command.AO.host**	

Function: Generate round key from SEED Key with key scheduling function in SEED algorithm.

State: Online

Notes: This command is used for testing purposes.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'AO'.
SEED Key	1A+32H	For a Variant LMK, the Seed Key must be encrypted under LMK pair 30-31 Note: All SEED keys must use the "J" key scheme.
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 'AP'.
Error Code	2 N	00 : No error 67 : Command not licensed 68 : command disabled Any standard error code
Round Key	256 H	Round 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.

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 <