THALES

cpl.thalesgroup.com

payShield 9000 v3.5

Host Command Reference Manual

Addendum for License LIC004 (OBKM & CEPS Commands)

1270A541-038

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
1270A541-038	Issue 38	payShield 9000 v3.5	July 2120

References

The following documents are referenced in this document:

1	1270A543 Thales payShield 9000 Installation Manual
2	1270A546 Thales payShield 9000 Host Command Reference Manual
3	1270A542 Thales payShield 9000 Host Programmer's Manual
4	1270A544 Thales payShield 9000 Console Reference Manual
5	1270A545 Thales payShield 9000 Security Operations Manual
6	MasterCard ESP Document Set (Publication Code: ZS, September 2002)

Chapter 1 – Introduction

General

The following commands have been implemented in the payShield 9000 HSM to meet the requirements specified in the MasterCard OBKM and CEPS specifications [6].

- Specific commands to support MasterCard OBKM are described in Chapter 2
- Specific commands to support MasterCard CEPS are described in Chapter 3 & 4.

PCI HSM Certification and Compliance

See Chapter 10 of the payShield 9000 General Information Manual for information about PCI HSM certification of the payShield 9000.

Host Commands

This document details all the host commands available with optional License LIC004, together 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’-‘Z’).
N	:	Numeric Field.
C	:	Control character.
B	:	Binary data (byte), X’00 to X’FF.

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, 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. When a disabled console command is invoked, the message "Function not defined or not allowed" is displayed.

Key Type Table

See the Key Type Table in Chapter 4 of the General Information Manual.

List of Host Commands (Alphabetical)

Host Command (Response)	Function	Page
J0 (J1)	Generate an Issuer RSA Key Set	11
JO (JP)	Validate a CA Self-Signed Certificate	13
R2 (R3)	Export Electronic Purse Card Key Set	27
R4 (R5)	Export Chip Card Key Set (2002 & 2003 Version)	19
R4 (R5)	Export Chip Card Key Set (2007 Version)	23
R6 (R7)	Export Magnetic Stripe Card Key Set	17
R8 (R9)	Import Transport Key Set	15
T0 (T1)	Unlinked Load Transaction Request	51
T2 (T3)	Release RLSAM	53
T4 (T5)	Release R2LSAM	54
T6 (T7)	Verify RCEP	55
U0 (U1)	Decrypt R1 and validate the MACLSAM	33
U2 (U3)	Compute HCEP	35
U4 (U5)	Validate the S1 MAC (Load and Unload)	36
U6 (U7)	Validate the S1 MAC (Currency Exchange)	38
U8 (U9)	Generate the S2 MAC (Linked load, declined unlinked load, unload)	40
V0 (V1)	Generate the S2 MAC (Currency Exchange)	42
V2 (V3)	Generate the S2 MAC (Approved Unlinked Load)	44
V4 (V5)	Validate the S3 MAC (Currency Exchange transactions)	46
V6 (V7)	Validate the S3 MAC (Load or Unload transactions)	48
V8 (V9)	Validate the H2LSAM	50
W0 (W1)	Validate S6 MAC	56
W2 (W3)	Validate S6' MAC	58
W4 (W5)	Validate S6'' MAC	60
W6 (W7)	Validate S5',DLT MAC	62
W8 (W9)	Validate S5',ISS MAC	64
X0 (X1)	Validate the S4 MAC (Old Terminals)	66
X2 (X3)	Validate the S4 MAC (New Terminals)	68

Chapter 2 – OBKM Commands

Introduction

The commands in this section allow the Card Issuer to set up the appropriate RSA keys required for the MasterCard OBKM Three-level key management hierarchy process. The following step by step description shows how the commands are intended to be used.

i) The Issuer creates his own RSA keyset by using the *Generate Issuer RSA Key Set* command. The key length will have to be defined (typically 512, 640, 768, 896 or 1024 bits) and the public exponent chosen. The Private Key part of the keyset is returned to the host system encrypted under the HSM's Local Master Key. This must be stored on the host database. The Public Key (PK) part of the keyset is also returned to the host system in two formats; a self-signed certificate and the Public Key protected with a MAC. The self-signed certificate is in the format required for transportation to the scheme Certification Authority (CA). It is normally transferred directly to suitable transport media for transport to the Certification Authority. The exact format details of how the self-signed PK certificate is written to the media is to be determined by the scheme provider (MasterCard).

If the PK is to be stored on the local database it is recommended that it is protected from alteration by storing the MAC as well. In this way, the authenticity of the PK can be later verified using the *Validate a Public Key* command.

ii) The MasterCard KMC will read the self-signed PK certificate from the transport media. The Certification Authority PK(s) (in the form of self-signed certificate(s)) will be written to a transport media for transportation back to the Issuer.

iii) The Issuer reads the transport media and places the CA PK(s) on the host database. The certificates are then verified. First it is necessary to verify the CA self-signed certificate(s) using the *Validate Certification Authority Self-Signed Certificate* command. This command returns the CA Public Key and a MAC which should be stored for later use.

iv) During the key transport process it is necessary to have available the appropriate Issuer Private Key (SK) within the HSM. It may be held (in encrypted form) on the host database and sent to the HSM every time it is used. Alternatively, to save on communication time, it may be pre-loaded into each HSM requiring it using the *Load a Private Key* command. It is the responsibility of the host application to keep track of the SK loaded at any time. Different HSM configurations can store a different number of SK(s) simultaneously. In this case the stored SK is referenced by a Key Index number.

v) At infrequent intervals it is normal to change the Local Master Keys (LMKs) of the HSMs. When this happens it is necessary to translate all keys encrypted under the old LMKs to encryption under the new LMKs. The Private Key(s) can be translated using the *Translate a Private Key* host command. The MACs protecting the Public Key(s) can be translated using the *Translate a Public Key* command.

Set KMC Sequence Number

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☒</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☑</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Required</b>
Activity: <b>misc.console</b></td></tr>
</table>

Command: **A6**

Function: To set the value of the KMC sequence number held within the HSM protected memory.

Authorization: The HSM must be in the Offline state to run this command. Additionally, the HSM must be either in the Authorized State, or the activity misc.console must be authorized.

Inputs: New sequence number value.

Outputs: None.

Errors:

`Not Authorized` - The HSM is not in Authorized State

`Not Offline` – The HSM must be offline to run this command

`Invalid Entry` – The value entered is invalid (Counter can have any value between 00000000 and FFFFFFFF).

Example:

```
Offline-AUTH> A6 <Return>

Current KMC sequence number is: 00000000 000000F3

Enter new value or <Enter> for no change: 2BAF <Return>

Current KMC sequence number is: 00000000 00002BAF

Offline-AUTH>
```

Generate an Issuer RSA Key Set

Variant ☑	Key Block ☒
License: **HSM9-LIC002 & HSM9-LIC004**	
Authorization: **Required** Activity: **generate.rsa-sk.host**	

Command: To generate an Issuer RSA Key Set and return the Public Key in the form of a MasterCard-format Self-Signed Issuer Public Key Certificate.

Notes: Depending on key size, this function may take up to a minute or more to execute. This command may be used with either an odd Public Exponent or a Public Exponent = 2. This command uses the “MasterCard” method of generating key pairs.

Field	**Length & Type**	**Details**
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'J0' (J-zero).
Hash Identifier	2 N	Identifier of algorithm used to hash data.
Signature Identifier	2 N	Identifier of signature algorithm.
Key Length	4 N	Modulus length in bits (must be a multiple of 8) Range: '0400' – '2040'.
Data Block	10 B	Data block to be included in the Self-Signed Certificate (comprises Certificate Subject ID (5 bytes), Expiry Date (2 bytes) and Certificate Serial Number (3 bytes)).
Issuer Public Key Index	3 B	Issuer Public Key Index.
Authentication Data	n A	Optional; additional data to be included in the MAC calculation (must not include ';').
Delimiter	1 A	Delimiter to indicate end of Authentication Data field: Value ';'.
Public Exponent Length	4 N	Optional; length in bits of the Public Exponent; must be supplied if Public Exponent present in command message.
Public Exponent	n B	Optional; if supplied then it must be odd or equal to 2; if not supplied then a default exponent of 65537 is assumed.
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 'J1'.
Error Code	2 N	'00': No error '04': Key length error '05': Invalid hash identifier '06': Invalid signature identifier '07': Public exponent length error '08': Invalid public exponent or a standard error code, as listed in Chapter 4 of [2].
MAC	4 B	MAC on Public Key and Authentication Data calculated using LMK 36-37.
Public Key	n B	Public Key, DER encoded in ASN.1 format (sequence of modulus and exponent).
Certificate Length	4 N	Length in bytes of Self-Signed Certificate.
Self-Signed Issuer Public Key Certificate	n B	Self-Signed Issuer Public Key Certificate (the concatenation of the Clear Data and the Self-Signed Certificate).
Hash Length	2 N	Length in hex characters of hash result in next field. This length will depend on the hash algorithm specified in the command message. For SHA-1, this length will be 40.
Hash Value	n H	Hash value of self signed Issuer Public Key data.
Private Key Length	4 N	Length (in bytes) of the Private Key field.
Private Key	n B	Private Key, encrypted using LMK pair 34-35.
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.

Validate a CA Self-Signed Certificate

Variant ☑	Key Block ☒
License: **HSM9-LIC002 & HSM9-LIC004**	
Authorization: **Required** Activity: **import.rsa-sk.host**	

Command: To validate a MasterCard-style Self-Signed Certification Authority (CA) Certificate.

Field	Length & Type	Details
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'JO' (J-Oh).
Certificate Length	4 N	Length (in bytes) of CA Self-Signed Certificate.
CA Self-Signed Certificate	n B	CA Self-Signed Certificate (concatenation of the Clear Data and the Self-Signed Certificate).
Delimiter	1 A	Delimiter, value ';'.
Authentication Data	n A	Optional; additional data to be included in the MAC calculation (must not include ';').
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 'JP'.
Error Code	2 N	'00': No error '02': Hash validation failure '05': Invalid hash algorithm '06': Invalid public key algorithm indicator '08': Invalid public key '80': Certificate length error '81': Invalid certificate header '82': Invalid trailer '83': Invalid certificate format '84': Invalid subject ID '85': Invalid public key data or a standard error code, as listed in Chapter 4 of [2].
MAC	4 B	MAC on Public Key and Authentication Data, calculated using LMK 36-37.
Public Key	n B	Public key, DER encoded in ASN.1 format (sequence of

Field	Length & Type	Details
		modulus, exponent).
Hash Length	2 N	Length in hex characters of hash result in next field. This length will depend on the hash algorithm specified in the command message. For SHA-1, this length will be 40.
Hash Value	n H	Hash value of self signed CA Public Key data.
Expiry Date	2 D	The Certificate Expiry Date (MMYY) recovered from the certificate.
Certificate Serial Number	3 B	The Certificate Serial Number recovered from the certificate.
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.

Import Transport Key Set

Variant ☑	Key Block ☒
License: **HSM9-LIC002 & HSM9-LIC004**	
Authorization: **Not Required**	

Command: To import the transport keys generated by the KMC.

Notes: The output from this function is a double length key used to encrypt keys sent from the MasterCard KMC (BKEM) and a double length key used to MAC keys sent from the MasterCard KMC (BKAM).

Field	**Length & Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'R8'.
KMC Sequence Number	8 B	Sequence number generated by KMC.
Member ID	10 N	The ID of the member this key set is intended for.
Transport Key Set ID	4 N	Identifier of the set BKEM, BKAM, as given by the KMC.
MAC on Public Key	4 B	MAC on the MasterCard Public key.
Public Key	n B	MasterCard Public Key, DER encoded in ASN.1 format (sequence of modulus and exponent).
Delimiter	1 A	Value ‘;’.
Signature Length	4 N	Length of signature block (T). This is a two byte signed integer with Most Significant Byte first.
Signature Block	T B	Signature generated using the MasterCard private key.
Delimiter	1 A	Value ‘;’.
Private Key Length	4 N	Length (in bytes) of the following Private Key field.
Private Key	n B	Member’s Private Key, encrypted using LMK pair 34-35.
Delimiter	1 A	Value ‘;’.
Encrypted Key Length	4 N	Length of encrypted key (S). This is a two byte signed integer with Most Significant Byte first.
Encrypted BKEM	S B	BKEM encrypted with the member’s public key.
Encrypted BKAM	S B	BKAM encrypted with the member’s public key.
Delimiter	1 A	Value ‘;’.
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 'R9'.
Error Code	2 N	'00': No error '51': Invalid message header '52': Invalid MAC algorithm number '53': Invalid Signature '54': Invalid BKAM data format '55': Invalid BKEM data format '56': BKAM parity error '57': BKEM parity error '58': Invalid MAC on Public Key or a standard error code, as listed in Chapter 4 of [2].
BKAM	1 A + 32 H	BKAM encrypted under LMK pair 22-23 variant 6.
BKEM	1 A + 32 H	BKEM encrypted under LMK pair 22-23 variant 5.
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.

Export Magnetic Stripe Card Key Set

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: To export a member's magnetic stripe key set for transport to the KMC.

Notes: The output from this function is a set of double length keys encrypted under the BKEM, together with a MAC over the key set, calculated using the BKAM.

Some of the keys in the key set may be set to 'all zeroes' to indicate they are not used.

The ESP sequence number is created from the date/time in BCD = YYYYMMDDhhmmss00.

Field	**Length & Type**	**Details**
		COMMAND MESSAGE
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'R6'.
Delimiter	1 A	Optional. If present the following field must be present. Value ';'.
OBKM Version	1 A	'0': September 2002 Specification '1': April 2003 Specification (Version = 01 02). Only present if above Delimiter is present.
Member ID	10 N	Identifier for the member, as defined by the KMC.
Key Set Reference	4 N	Reference of the Magnetic Stripe Card Keys provided in this key set, as defined by the member.
Floor Expiry Date for key set	4 N	Expiry Date in format MMYY.
PAN Range for Key Set	38 N	Concatenation of 19 digits formed of PAN-low left padded by 0s and 19 digits formed of PAN-high left padded by 0s.
PVKI	1 N	Index of PVV, '0' to '9'.
PVV Key	1 A + 32 H	Double length PVV key, encrypted under LMK pair 14-15 using Key Encryption Scheme U.
Extra PVV Key Information	12 N	Extra data linked to the key.
CVC1	1 A + 32 H	Double length CVC1 key, encrypted under LMK 14-15 variant 4 using Key Encryption Scheme U.
Extra CVC1 Key Information	11 N	Extra data linked to the key.
CVC2	1 A + 32 H	Double length CVC2 key, encrypted under LMK 14-15 variant 4 using Key Encryption Scheme U.
Extra CVC2 Key Information	7 N	Extra data linked to the key.

Field	Length & Type	Details
COMMAND MESSAGE		
Transport Key ID	4 N	Key ID of the BKAM BKEM pair used.
MAC algorithm	1 N	MAC algorithm parameters to be used with BKAM: '2', '3', '4' or '6': as defined in ISO/IEC 9797-1.
BKAM	1 A + 32 H	BKAM encrypted under LMK pair 22-23 variant 6.
BKEM	1 A + 32 H	BKEM encrypted under LMK pair 22-23 variant 5.
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 'R7'.
Error Code	2 N	'00': No error '08': BKAM parity error '09': BKEM parity error '10': PVV key parity error '11': CVC Key1 parity error '50': CVC Key2 parity error '51': Invalid message header or a standard error code, as listed in Chapter 4 of [2].
ESP Sequence Number	16 H	Sequence Number from the ESP.
Encrypted PVV Key	32 H	BKEM Encrypted PVV Key.
PVV Key CV	3 B	Check Value on PVV.
Encrypted CVC1 Key	32 H	BKEM Encrypted CVC1 Key.
CVC1 Key CV	3 B	Check Value on CVC1.
Encrypted CVC2 Key	32 H	BKEM Encrypted CVC2 Key.
CVC2 Key CV	3 B	Check Value on CVC2.
MAC	16 H	MAC calculated over key set data using BKAM.
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.

Export Chip Card Key Set (2002 & 2003 Version)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: To export a member’s chip card key set for transport to the KMC.

Notes: The output from this function is a set of double length keys encrypted under the BKEM, together with a MAC over the key set, calculated using the BKAM.

Some of the keys in the key set may be set to ‘all zeroes’ to indicate they are not used.

Field	**Length & Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'R4'.
Delimiter	1 A	Optional. If present the following field must be present. Value ';'.
OBKM Version	1 A	'0': September 2002 Specification '1': April 2003 Specification (Version = 02 02) Only present if above Delimiter is present.
Member ID	10 N	Identifier for the member, as defined by the KMC.
Key Set Reference	4 N	Reference of the Magnetic Stripe Card Keys provided in this key set, as defined by the member.
Floor Expiry Date for key set	4 N	Expiry Date in format MMYY.
PAN Range for Key Set	38 N	Concatenation of 19 digits formed of PAN-low left padded by 0s and 19 digits formed of PAN-high left padded by 0s.
Key Derivation Index	3 N	Index for the Key Set.
Cryptogram Version Number	1 B	
IMKac	1 A + 32 H	Double length IMKac, encrypted under LMK pair 28-29 Variant 1, using Key Encryption Scheme U.

Field		Length & Type	Details
Extra IMKac Key Data	Decision Matrix in case of Invalid Cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	ICC Master Key Derivation Algorithm ID	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme.
	Session Key Derivation Algorithm ID (SKD)	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme.
	ARQC/ARPC Algorithm ID	1 N	'1': reserved for future use.
	Issuer Application Data Layout	1 N	'1': M/Chip Lite 2.1 and M/Chip 4 schemes '2': M/Chip Select 2.0.5 scheme.
	H	2 N	Height of the tree. Only present if SKD = '4'.
	B	2 N	Branch of the tree. Only present if SKD = '4'.
IMKsmi		1 A + 32 H	Double length IMKsmi, encrypted under LMK pair 28-29 Variant 2, using Key Encryption Scheme U.
Extra IMKsmi Key Data	ICC Master Key Derivation Algorithm ID	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme.
	Session Key Derivation Algorithm ID (SKD)	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme.
	MAC Algorithm ID	1 N	'1': reserved for future use.
	H	2 N	Height of the tree. Only present if SKD = '4'.
	B	2 N	Branch of the tree. Only present if SKD = '4'.
IMKsmc		1 A + 32 H	Double length IMKsmc encrypted under LMK pair 28-29 Variant 3, using Key Encryption Scheme U.
Extra IMKsmc Key Data	ICC Master Key Derivation Algorithm ID	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme.
	Session Key Derivation Algorithm ID (SKD)	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme.
	Encryption Algorithm ID	1 N	'1': reserved for future use.
	H	2 N	Height of the tree. Only present if SKD = '4'.
	B	2 N	Branch of the tree. Only present if SKD = '4'.

Field		Length & Type	Details
IMKidn		1 A + 32 H	Double length IMKidn, encrypted under LMK pair 28-29 Variant 5, using Key Encryption Scheme U.
Extra IMKIdn Key Data	Decision Matrix in case of invalid cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	ICC Master Key Derivation Algorithm ID	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme.
	IDN Algorithm ID	1 N	'1': reserved for future use.
IMKdac		1 A + 32 H	Double length IMKdac, encrypted under LMK pair 28-29 Variant 4, using Key Encryption Scheme U.
Extra IMKdac Key Data	Decision Matrix in case of invalid cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	DAC Algorithm ID	1 N	'1': reserved for future use.
Transport Key ID		4 N	Key ID of the BKAM, BKEM used.
MAC algorithm		1 N	MAC algorithm to be used with BKAM, '2', '3', '4' or '6': as defined in ISO/IEC 9797-1.
BKAM		1 A + 32 H	BKAM encrypted under LMK pair 22-23, variant 6.
BKEM		1 A + 32 H	BKEM encrypted under LMK pair 22-23, variant 5.
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 'R5'.
Error Code	2 N	'00': No error '08': BKAM parity error '09': BKEM parity error '10': IMKac parity error '11': IMKsmi parity error '50': IMKsmc parity error '51': Invalid message header '52': IMKidn parity error '53': IMKdac parity error or a standard error code, as listed in Chapter 4 of [2].
ESP Sequence Number	16 H	Sequence Number from the ESP.
Encrypted IMKac	32 H	BKEM Encrypted Key.
IMKac Key Check Value	3 B	
Encrypted IMKsmi	32 H	BKEM Encrypted Key.
IMKsmi Key Check Value	3 B	
Encrypted IMKsmc	32 H	BKEM Encrypted Key.
IMKsmc Key Check Value	3 B	
Encrypted IMKidn	32 H	BKEM Encrypted Key.
IMKidn Key Check Value	3 B	
Encrypted IMKdac	32 H	BKEM Encrypted Key
IMKdac Key Check Value	3 B	
MAC	16 H	MAC calculated over key set data using BKAM.
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.

Export Chip Card Key Set (2007 Version)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: To export a member's chip card key set for transport to the KMC.

Notes: The output from this function is a set of double length keys encrypted under the BKEM, together with a MAC over the key set, calculated using the BKAM.

Some of the keys in the key set may be set to 'all zeroes' to indicate they are not used.

Field	**Length & Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'R4'.
Delimiter	1 A	Value ';'.
OBKM Version	1 A	'2': September 2007 Specification (Version = 02 05)
Member ID	10 N	Identifier for the member, as defined by the KMC.
Key Set Reference	4 N	Reference of the Magnetic Stripe Card Keys provided in this key set, as defined by the member.
Floor Expiry Date for key set	4 N	Expiry Date in format MMYY.
PAN Range for Key Set	38 N	Concatenation of 19 digits formed of PAN-low left padded by 0s and 19 digits formed of PAN-high left padded by 0s.
Key Derivation Index	3 N	Index for the Key Set.
Cryptogram Version Number	1 B	
IMKac	1 A + 32 H	Double length IMKac, encrypted under LMK pair 28-29 Variant 1, using Key Encryption Scheme U.

Field		Length & Type	Details
Extra IMKac Key Data	Decision Matrix in case of Invalid Cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '055': Invalid PIN '057': Transaction not permitted to Cardholder '075': Allowable number of PIN tries exceeded '086': PIN Validation not possible.
	Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '055': Invalid PIN '057': Transaction not permitted to Cardholder '075': Allowable number of PIN tries exceeded '086': PIN Validation not possible.
	Decision Matrix in case of invalid TVR/CVR	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '055': Invalid PIN '057': Transaction not permitted to Cardholder '075': Allowable number of PIN tries exceeded '086': PIN Validation not possible. *Supported on Banknet only.*
	Decision Matrix in case cryptogram is not an ARQC	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '055': Invalid PIN '057': Transaction not permitted to Cardholder '075': Allowable number of PIN tries exceeded '086': PIN Validation not possible. *Supported on Banknet only.*
	ICC Master Key Derivation Algorithm ID	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme '5': CCD scheme
	Card Application Identifier (CAI)	1 N	'1': M/Chip 2.x schemes '4': M/Chip 4 scheme '5': CCD scheme
	ARQC/ARPC Algorithm ID	1 N	'1': M/Chip schemes '2': CCD scheme
	CVN Position Indicator	1 N	Indicates the position of CVN (Cryptogram Version Number) sub-element with tag 9F10 (Issuer Application Data): '1': 2nd byte of tag 9F10 – for M/Chip scheme (M/Chip 2.1 Lite and M/Chip 4.0 and CCD) '2': 3rd byte of 9F10 – for VSDC scheme (M/Chip 2.0.5 Select).
	H	2 N	If CAI = '1', this field should be set to '00'. If CAI = '4' or '5': Height factor of the EMV 2000 session key derivation algorithm. Acceptable values: If CAI = '4': '8' or '16' If CAI = '5': '8'.

Field	Length & Type	Details
b	2 M	If CAI = '1', this field should be set to '00'. If CAI = '4' or '5': Branch factory of the EMV 2000 session key derivation algorithm. Acceptable values: If CAI = '4': '2' (if H='16') or '4' (if H='8') If CAI = '5': '4'.
ARC if transaction accepted	8 H	If CAI = '1', this field should be set to '00000000'. If CAI = '4' or '5', this field specifies the ARPC Response Code for an approved transaction.
ARC if transaction rejected	8 H	If CAI = '1', this field should be set to '00000000'. If CAI = '4' or '5', this field specifies the ARPC Response Code for a declined transaction.
TVR/CVR bitmask and expected value	44 H	TVR/CVR bitmask and expected value needed by Mastercard Chip On-behalf Services to check transaction TVR and CVR data elements on behalf of the issuer. Filled with 44 digits '0' if not used.
POS Terminal PAN Entry Mode	2 N	This parameter gives the issuers the flexibility to use, for the same PAN range, floor expiry date and Key Derivation Index, a different chip cryptography type, specified through field 6 (Card Application Identifier) above, depending on the value of DE22 SF1. Allowed values: '05': M/Chip contact '07': M/Chip contactless. *Supported on Banknet only.*
Transport Key ID	4 N	Key ID of the BKAM, BKEM used.
MAC algorithm	1 N	MAC algorithm to be used with BKAM, '2', '3', '4' or '6': as defined in ISO/IEC 9797-1.
BKAM	1 A + 32 H	BKAM encrypted under LMK pair 22-23, variant 6.
BKEM	1 A + 32 H	BKEM encrypted under LMK pair 22-23, variant 5.
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 'R5'.
Error Code	2 N	'00': No error '08': BKAM parity error '09': BKEM parity error '10': IMKac parity error '51': Invalid message header or a standard error code, as listed in Chapter 4 of [2].
ESP Sequence Number	16 H	Sequence Number from the ESP.
Encrypted IMKac	32 H	IMKac encrypted under BKEM.
IMKac Key Check Value	3 B	The check value of the IMKac.
MAC	16 H	MAC calculated over key set data using BKAM.
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.

Export Electronic Purse Card Key Set

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: To export a member's electronic purse card key set for transport to the KMC.

Notes: The output from this function is a set of double length keys encrypted under the BKEM, together with a MAC over the key set, calculated using the BKAM.

Some of the keys in the key set may be set to 'all zeroes' to indicate they are not supplied. The zero value will then be placed in the data block to be protected with a MAC.

The MasterCard documents refer to the KML as KDLiss, KM3X as K3Xiss etc.

All keys are passed in using key scheme U.

Field	**Length & Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'R2'.
Delimiter	1 A	Optional. If present the following field must be present. Value ';'.
ESP Version	1 A	'0': September 2002 Specification '1': April 2003 Specification (Version = 03 02). Only present if above Delimiter is present.
Member ID	10 N	Identifier for the member, as defined by the KMC.
Key Set Reference	4 N	Reference of the Magnetic Stripe Card Keys provided in this key set, as defined by the member.
Floor Expiry Date for key set	4 N	Expiry Date in format MMYY.
PAN Range for Key Set	38 N	Concatenation of 19 digits formed of PAN-low left padded by 0s and 19 digits formed of PAN-high left padded by 0s.
KMLiss	1 A + 32 H	Double length master key, encrypted under LMK pair 20-21 Variant 1, using Key Encryption Scheme U.

Field		Length & Type	Details
Extra KDLIss Key Data	Decision Matrix in case of Invalid Cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	ICC Mater Key Derivation Algorithm ID	1 N	'1': Algorithm 4.
	Session Key Derivation Algorithm ID	1 N	'1': Algorithm 3. '2': Algorithm 5.
	S1 Cryptogram Algorithm ID	1 N	'1': Reserved for future use.
	S2 Cryptogram Algorithm ID	1 N	'1': Reserved for future use.
	H	2 N	If SKD = '1': Filler If SKD = '2': Height of the tree.
	B	2 N	If SKD = '1': Filler If SKD = '2': Branch of the tree.
KM3Liss		1 A + 32 H	Double length master key, encrypted under LMK pair 20-21 Variant 5, using Key Encryption Scheme U.
Extra KD3LIss Key Data	Decision Matrix in case of Invalid Cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	ICC Master Key Derivation Algorithm ID	1 N	'1': Algorithm 4.
	Session Key Derivation Algorithm ID (SKD)	1 N	'1': Algorithm 3 '2': Algorithm 5.
	S3 Cryptogram Algorithm ID	1 N	'1': Reserved for future use.
	H	2 N	If SKD = '1': Filler If SKD = '2': Height of the tree.
	B	2 N	If SKD = '1': Filler If SKD = '2': Branch of the tree.
KMXiss		1 A + 32 H	Double length master key encrypted under LMK pair 20-21 Variant 2, using Key Encryption Scheme U.

Field		**Length & Type**	**Details**
Extra KDXIss Key Data	Decision Matrix in case of Invalid Cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	ICC Master Key Derivation Algorithm ID	1 N	'1': Algorithm 4.
	Session Key Derivation Algorithm ID (SKD)	1 N	'1': Algorithm 3 '2': Algorithm 5.
	S1 Cryptogram Algorithm ID	1 N	'1': Reserved for future use.
	S2 Cryptogram Algorithm ID	1 N	'1': Reserved for future use.
	H	2 N	If SKD = '1': Filler If SKD = '2': Height of the tree.
	B	2 N	If SKD = '1': Filler If SKD = '2': Branch of the tree.
KM3Xiss		1 A + 32 H	Double length master key, encrypted under LMK pair 20-21 Variant 6, using Key Encryption Scheme U.
Extra KD3XIss Key Data	Decision Matrix in case of Invalid Cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	ICC Master Key Derivation Algorithm ID	1 N	'1': Algorithm 4.
	Session Key Derivation Algorithm ID (SKD)	1 N	'1': Algorithm 3 '2': Algorithm 5.
	S3 Cryptogram Algorithm ID	1 N	'1': Reserved for future use.
	H	2 N	If SKD = '1': Filler If SKD = '2': Height of the tree.
	B	2 N	If SKD = '1': Filler If SKD = '2': Branch of the tree.
KMPiss		1 A + 32 H	Double length master key, encrypted under LMK pair 20-21 Variant 3, using Key Encryption Scheme U.

Field		**Length & Type**	**Details**
Extra KDPiss Key Dat a	Decision Matrix in case of Invalid Cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	Decision Matrix in case of Impossible to validate cryptogram	3 N	'000': Approved '001': Refer to Card Issuer '004': Pick-up '005': Do not Honour '008': Honour with Identification '012': Invalid Transaction '057': Transaction not permitted to Cardholder.
	ICC Master Key Derivation Algorithm ID	1 N	'1': Algorithm 4.
	Session Key Derivation Algorithm ID (SKD)	1 N	'1': Algorithm 3 '2': Algorithm 5.
	S6 Cryptogram Algorithm ID	1 N	'1': Reserved for future use.
	H	2 N	If SKD = '1': Filler If SKD = '2': Height of the tree.
	B	2 N	If SKD = '1': Filler If SKD = '2': Branch of the tree.
KMSIiss		1 A + 32 H	Double length master key, encrypted under LMK pair 22-23 Variant 3, using Key Encryption Scheme U.
Extra KDSIiss Key Data	ICC Master Key Derivation Algorithm ID	1 N	'1': Algorithm 4.
	Session Key Derivation Algorithm ID (SKD)	1 N	'1': Algorithm 3 '2': Algorithm 5.
	MAC Algorithm ID	1 N	'1': Reserved for future use.
	H	2 N	If SKD = '1': Filler If SKD = '2': Height of the tree.
	B	2 N	If SKD = '1': Filler If SKD = '2': Branch of the tree.
KMSCiss		1 A + 32 H	Double length master key, encrypted under LMK pair 22-23 Variant 4, using Key Encryption Scheme U.
Extra KDSCiss Key Data	ICC Master Key Derivation Algorithm ID	1 N	'1': Algorithm 4.
	Session Key Derivation Algorithm ID (SKD)	1 N	'1': Algorithm 3 '2': Algorithm 5.
	Encryption Algorithm ID	1 N	'1': Reserved for future use.
	H	2 N	If SKD = '1': Filler If SKD = '2': Height of the tree.
	B	2 N	If SKD = '1': Filler If SKD = '2': Branch of the tree.
Transport Key ID		4 N	Key ID of the BKAM, BKEM used.
IDcep		6 B	Derivation Data.

Field	Length & Type	Details
MAC algorithm	1 N	MAC algorithm to be used with BKAM, '2', '3', '4' or '6': as defined in ISO/IEC 9797-1.
BKAM	1 A + 32 H	BKAM encrypted under LMK pair 22-23, variant 6.
BKEM	1 A + 32 H	BKEM encrypted under LMK pair 22-23, variant 5.
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 'R3'.
Error Code	2 N	'00': No error '08': BKAM parity error '09': BKEM parity error '10': KML parity error '11': KM3L parity error '50': KMX parity error '51': Invalid message header '52': KM3X parity error '53': KMP parity error '54': KMSI parity error '55': KMSC parity error or a standard error code, as listed in Chapter 4 of [2].
ESP Sequence Number	16 H	Sequence Number from the ESP.
Encrypted KDL	32 H	BKEM Encrypted Key.
KDL Key Check Value	3 B	
Encrypted KD3L	32 H	BKEM Encrypted Key.
KD3L Key Check Value	3 B	
Encrypted KDX	32 H	BKEM Encrypted Key.
KDX Key Check Value	3 B	
Encrypted KD3X	32 H	BKEM Encrypted Key.
KD3X Key Check Value	3 B	
Encrypted KDP	32 H	BKEM Encrypted Key.
KDP Key Check Value	3 B	
Encrypted KSI	32 H	BKEM Encrypted Key.
KSI Key Check Value	3 B	
Encrypted KSC	32 H	BKEM Encrypted Key.
KSC Key Check Value	3 B	
MAC	16 H	MAC calculated over key set data using BKAM.
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.

Chapter 3 – CEPS Commands

Decrypt R_1 and validate the MAC_{LSAM}

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: To decrypt R_1 and validate the MAC_{LSAM}.

Notes: This command is complementary to the SA command in the Load Acquirer commands that generates the encrypted R_1.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'U0'.
TPK	16 H or 1 A + 32 H	The Terminal PIN key 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". A single length TPK will be input as 16 hexadecimal characters. A double length TPK will be input as a 'U' character followed by 32 hexadecimal characters.
R_1Length	1 N	The length of the key R_1: '1': single length '2': double length.
R_1	16 / 32 H	The session key encrypted under the TPK.
DD_{CEP}Length	1 B	The length in bytes of the DD_{CEP} field. The length is specified in binary and must be in the range 00H to 20H (equivalent to 0 to 32 decimal).
ID_{ISS}	4 B	The Issuer ID.
ID_{CEP}	6 B	The CEP Card Identifier.
NT_{CEP}	2 B	The transaction number assigned by the card.
$CURR_{LDA}$	3 B	The Currency Indicator.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
M_{LDA}	4 B	The Transaction amount.
S1	8 B	The CEP Card signature produced by the card during 'Card Initialise for Load'.
H_{CEP}	10 B	The SHA-1 Hash generated by the CEP card on the Load Transaction data.
H_{LSAM}	8 B	SHA-1 hash of internally generated R_{LSAM}.
$H2_{LSAM}$	8 B	SHA-1 hash of internally generated $R2_{LSAM}$.
DD_{CEP}	0 - 32 B	Discretionary Data.
MAC_{LSAM}	4 B	EMV MAC of Transactional data.
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.

Field	Length & Type	Details
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 'U1'.
Error Code	2 N	'00': No error (MAC validated successfully) '01': MAC validation failed '11': TPK parity error '70': Invalid R_1Length code '72': R_1 Parity Error or a standard error code, as listed in Chapter 4 of [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.

Compute H_{CEP}

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Create R_{CEP} and use the SHA-1 algorithm to compute H_{CEP}.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'U2'.
*KML	32 H or 1 A + 32 H	Double length KML encrypted under LMK pair 20-21 variant 1.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
ID_{ISS}	4 B	The Issuer ID.
ID_{CEP}	6 B	The CEP Card Identifier.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
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	Will be returned to the Host unchanged
Response Code	2 A	Value 'U3'.
Error Code	2 N	'00': No error '10': KML parity error or a standard error code, as listed in Chapter 4 of [2].
H_{CEP}	10 B	SHA hash of input data and R_{CEP} .
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.

Validate the S_1 MAC (Load and Unload)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Validate the S_1 MAC for load and unload transactions.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'U4'.
*KML	32 H or 1 A + 32 H	Double length KML encrypted under LMK pair 20-21 variant 1.
ID_{CEP}	6 B	The CEP Card Identifier. Used to create the *KDL.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
TI	1 B	Transaction Indicator: ‘0C': load transactions ’0A': unload transactions.
$DTHR_{LDA}$	5 B	Transaction date and time.
$CURR_{LDA}$	3 B	The Currency Code.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
M_{LDA}	4 B	The Transaction amount.
$NT_{LASTLOAD}$	2 B	Transaction number of last load.
$NT_{LASTCANCEL}$	2 B	Transaction number of last cancel.
$CSTAT_{CEP}$	2 B	Card Status.
$TLfail_{CEP}$	1 B	Tag and length of failed update.
$DEXP_{CEP}$	3 B	Expiry date of the card, YYMMDD.
BAL_{CEP}	4 B	Balance of slot prior to completion.
$BALmax_{CEP}$	4 B	Maximum balance of the slot.
PVS_{CEP}	1 B	PIN verification status.
S_1	8 B	Signature for verification.
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 'U5'.
Error Code	2 N	'00': No error (S_1 validated successfully) '01': S_1 validation failed '10': KML parity error '70': Invalid transaction indicator or a standard error code, as listed in Chapter 4 of [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.

Validate the S_1 MAC (Currency Exchange)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Validate the S_1 MAC for currency exchange transactions.

Field	Length & Type	Details
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'U6'.
*KMX	32 H or 1 A + 32 H	Double length KMX encrypted under LMK pair 20-21 variant 2.
ID_{CEP}	6 B	The CEP Card Identifier. Used to create the *KDX.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
TI	1 B	Transaction Indicator: '08' for currency exchange transactions.
$DTHR_{LDA}$	5 B	Transaction date and time.
$CURR_{SOURCE}$	3 B	The Currency Code for the source slot.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
M_{LDA}	4 B	The Transaction amount.
$NT_{LASTLOAD}$	2 B	Transaction number of last load.
$NT_{LASTCANCEL}$	2 B	Transaction number of last cancel.
$CSTAT_{CEP}$	2 B	Card Status.
$TLfail_{CEP}$	1 B	Tag and Length of failed update.
$DEXP_{CEP}$	3 B	Expiry date of the card, YYMMDD.
$CURR_{TARGET}$	3 B	The Currency Code.
BAL_{TARGET}	4 B	Balance of target slot .
$BALmax_{TARGET}$	4 B	Maximum balance of the target slot.
BAL_{SOURCE}	4 B	Balance of source slot.
S_1	8 B	Signature for verification.
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 'U7'.
Error Code	2 N	'00': No error (S_1 validated successfully) '01': S_1 validation failed '10': KDX parity error '70': Invalid transaction indicator or a standard error code, as listed in Chapter 4 of [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 the S_2 MAC (Linked load, declined unlinked load, unload)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Generate the S_2 MAC for Linked Load, Declined Unlinked Load or Unload transactions.

Field	Length & Type	Details
		COMMAND MESSAGE
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'U8'.
*KML	32 H or 1 A + 32 H	Double length KML encrypted under LMK pair 20-21 variant 1.
ID_{CEP}	6 B	The CEP Card Identifier. Used to create the *KDL.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
Updates Length	2 N	Length in bytes of the $UPDATES_{ISS}$ field.
CC_{ISS}	2 B	Completion Code.
TI	1 B	Transaction Indicator: ‘0C': Linked Load or Declined Unlinked Load transactions ’0A': unload transactions.
S_1	8 B	Signature.
BAL_{ISS}	4 B	Balance of card for this currency.
$BALmax_{ISS}$	4 B	Maximum balance of the target slot.
$CALPHA_{ISS}$	3 B	Alphanumeric currency code.
$UPDATES_{ISS}$	0 - 24 B	Updates to CEP card data.
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 'U9'.
Error Code	2 N	'00': No error '10': *KML parity error '70': Invalid transaction indicator '71': Invalid Updates Length or a standard error code, as listed in Chapter 4 of [2].
S_2	8 B	Generated Signature.
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 the S_2 MAC (Currency Exchange)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Generate the S_2 MAC for currency exchange transactions.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'V0'.
*KMX	32 H or 1 A + 32 H	Double length *KMX encrypted under LMK pair 20-21 variant 2.
ID_{CEP}	6 B	The CEP Card Identifier. Used to create the *KDX.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
Updates Length	2 N	Length in bytes of the $\text{UPDATES}_{\text{ISS}}$ field.
CC_{ISS}	2 B	Completion Code.
TI	1 B	Transaction Indicator: ‘08': currency exchange transactions
S_1	8 B	Signature.
$\text{BAL}_{\text{ISS,TARGET}}$	4 B	New Balance of target slot.
$\text{BALmax}_{\text{ISS,TARGET}}$	4 B	Maximum balance of the target slot.
$\text{CALPHA}_{\text{ISS, TARGET}}$	3 B	Alphanumeric representation of the target currency code.
$\text{BAL}_{\text{ISS,SOURCE}}$	4 B	New Balance of the source slot.
$\text{UPDATES}_{\text{ISS}}$	0 - 24 B	Updates to CEP card data.
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 'V1'.
Error Code	2 N	'00': No error '10': KML parity error '70': Invalid transaction indicator '71': Invalid Updates Length or a standard error code, as listed in Chapter 4 of [2].
S_2	8 B	Generated Signature.
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 the S_2 MAC (Approved Unlinked Load)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Generate the S_2 MAC for unlinked load transactions.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'V2'.
*KML	32 H or 1 A + 32 H	Double length KML encrypted under LMK pair 20-21 variant 1.
ID_{CEP}	6 B	The CEP Card Identifier. Used to create the *KDL.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
Updates Length	2 N	Length in bytes of the $UPDATES_{ISS}$ field.
CC_{ISS}	2 B	Completion Code.
TI	1 B	Transaction Indicator: ‘0C': unlinked load transactions.
S_1	8 B	S1 Signature.
BAL_{ISS}	4 B	Balance of CEP card.
$BALmax_{ISS}$	4 B	Maximum balance of the target slot.
$CALPHA_{ISS}$	3 B	Alphanumeric representation of the currency code for this slot.
H_{LSAM}	8 B	Left 8 bytes from SHA-1 hash of: ID_{LACQ},ID_{LDA},ID_{ISS},ID_{CEP},NT_{CEP},R_{LSAM}
$UPDATES_{ISS}$	0 - 24 B	Updates to CEP card data.
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 'V3'.
Error Code	2 N	'00': No error '10': KML parity error '70': Invalid transaction indicator '71': Invalid Updates Length or a standard error code, as listed in Chapter 4 of [2].
S_2	8 B	Generated Signature.
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.

Validate the S_3 MAC (Currency Exchange transactions)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Validate the S_3 MAC for currency exchange transactions.

Notes: After a CEP card completes processing, it generates an S_3 MAC to prove to the issuer that the currency exchange transaction was completed successfully. The load processor uses this function to verify the S_3 MAC.

Field	**Length & Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'V4'.
*KM3X	32 H or 1 A + 32 H	Double length KM3X encrypted under LMK pair 20-21 variant 6.
ID_{CEP}	6 B	The CEP Card Identifier. Used to create the *KDX.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
CC_{TRX}	2 B	Transaction Completion Code.
TI	1 B	Transaction Indicator: ‘08': currency exchanges.
$DTHR_{LDA}$	5 B	Transaction date and time.
$CURR_{LDA,SOURCE}$	3 B	The Currency Code.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
M_{LDA}	4 B	The Transaction amount.
$CURR_{LDA,TARGET}$	3 B	The Currency Code.
$BAL_{CEP,TARGET}$	4 B	Balance of slot prior to completion.
$BAL_{CEP,SOURCE}$	4 B	Balance of slot prior to completion.
S_3	8 B	Signature for verification.
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 'V5'.
Error Code	2 N	'00': No error (S_3 validated successfully) '01': S_3 validation failed '10': KML parity error '70': Invalid transaction indicator or a standard error code, as listed in Chapter 4 of [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.

Validate the S_3 MAC (Load or Unload transactions)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Validate the S_3 MAC for load or unload transactions.

Notes: After a CEP card completes processing, it generates an S_3 MAC to prove to the issuer that the load or unload transaction was completed successfully. This function is used by the load processor to verify the S_3 MAC.

Field	**Length & Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'V6'.
*KM3L	32 H or 1 A + 32 H	Double length *KM3L encrypted under LMK pair 20-21 variant 5.
ID_{CEP}	6 B	The CEP Card Identifier. Used to create the *KD3L.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
CC_{TRX}	2 B	Transaction Completion Code.
TI	1 B	Transaction Indicator: ‘0C': load transactions ’0A': unload transactions.
$DTHR_{LDA}$	5 B	Transaction date and time.
$CURR_{LDA}$	3 B	The Currency Code.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
M_{LDA}	4 B	The Transaction amount.
BAL_{CEP}	4 B	Balance of slot prior to completion.
S_3	8 B	Signature for verification.
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 'V7'.
Error Code	2 N	'00': No error (S_3 validated successfully) '01': S_3 validation failed '10': KMX parity error '70': Invalid transaction indicator or a standard error code, as listed in Chapter 4 of [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.

Validate the $H2_{LSAM}$

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Validate the $H2_{LSAM}$, creating a SHA-1 hash over the transaction data and comparing with the input $H2_{LSAM}$.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'V8'.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
ID_{ISS}	4 B	The Issuer ID.
ID_{CEP}	6 B	The CEP Card Identifier.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
$R2_{LSAM}$	16 B	Random Number .
$H2_{LSAM}$	8 B	Verification code (SHA-1 hash).
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 'V9'.
Error Code	2 N	'00': No error ($H2_{LSAM}$ validated successfully) '01': $H2_{LSAM}$ validation failed '10': KML parity error '70': Invalid transaction indicator or a standard error code, as listed in Chapter 4 of [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.

Unlinked Load Transaction Request

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Unlinked Load Transaction Request.

Field	Length & Type	Details
		COMMAND MESSAGE
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'T0'.
S1	8 B	The CEP Card MAC produced by the card during 'Card Initialise for Load'.
H_{CEP}	10 B	The SHA-1 Hash generated by the CEP card on the Load Transaction data.
TPK	16 H or 1 A + 32 H	The Terminal PIN key 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".
REFNO	3 B	The Transaction Reference Number.
R_1Length	1 N	The required length of the generated key R_1: '1': single length '2': double length.
ID_{ISS}	4 B	The Issuer ID.
ID_{CEP}	6 B	The CEP Card Identifier.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
$CURR_{LDA}$	3 B	The Currency Indicator.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
M_{LDA}	4 B	The Transaction amount.
DD_{CEP}Length	1 B	The length in bytes of the DD_{CEP} field that follows.
DD_{CEP}	0 - 32 B	Discretionary Data.
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 'T1'.
Error Code	2 N	'00': No error '11': TPK Parity Error or a standard error code, as listed in Chapter 4 of [2].
(DES)R_1	16 / 32 H	The generated session key encrypted under the TPK. (Note, if the supplied TPK is double length then this will also be double length.)
(DES)R_{LSAM}	64 H	The generated double length key R_{LSAM} and other data CBC encrypted under LMK pair 10-11.
(DES)$R2_{LSAM}$	64 H	The generated double length key $R2_{LSAM}$ and other data CBC encrypted under LMK pair 10-11.
H_{LSAM}	8 B	SHA-1 hash of internally generated R_{LSAM}.
$H2_{LSAM}$	8 B	SHA-1 hash of internally generated $R2_{LSAM}$.
(DES)HCEP	64 H	The HCEP, concatenated with REFNO and ID_{LACQ} and CBC encrypted under LMK pair 10-11.
MAC_{LSAM}	4 B	EMV MAC of Transactional data.
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.

Release R_{LSAM}

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Release R_{LSAM}.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'T2'.
REFNO	3 B	The Transaction Reference Number.
ID_{LACQ}	4 B	Load Acquirer ID.
(DES)R_{LSAM}	64 H	The generated double length key R_{LSAM} and other data CBC encrypted under LMK pair 10-11.
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 'T3'.
Error Code	2 N	'00': No error '01': Validation Error '10': R_{LSAM} parity error or a standard error code, as listed in Chapter 4 of [2].
R_{LSAM}	32 H	The clear text value of R_{LSAM} returned as 32 HEX characters.
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.

Release $R2_{LSAM}$

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Release $R2_{LSAM}$.

Field	Length & Type	Details
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'T4'.
REFNO	3 B	The Transaction Reference Number.
ID_{LACQ}	4 B	Load Acquirer ID.
(DES)$R2_{LSAM}$	64 H	The generated double length key $R2_{LSAM}$ and other data CBC encrypted under LMK pair 10-11.
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 'T5'.
Error Code	2 N	'00': No error '01': Validation Error '10': $R2_{LSAM}$ parity error or a standard error code, as listed in Chapter 4 of [2].
$R2_{LSAM}$	32 H	The clear text value of $R2_{LSAM}$ returned as 32 HEX characters.
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 R_{CEP}

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Verify R_{CEP}.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'T6'.
REFNO	3 B	The Transaction Reference Number.
(DES)H_{CEP}	64 H	The HCEP, concatenated with REFNO and ID_{LACQ} and CBC encrypted under LMK pair 10-11.
ID_{LACQ}	4 B	Load Acquirer ID.
ID_{LDA}	6 B	The Identifier for the Load Device.
ID_{ISS}	4 B	The Issuer ID.
ID_{CEP}	6 B	The CEP Card Identifier.
NT_{CEP}	2 B	The transaction number assigned by the Load Acquirer.
R_{CEP}	16 B	The 16 Byte value returned by the CEP card following a Credit for Load rejection.
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 'T7'.
Error Code	2 N	'00': No error '01': Verification Failure or a standard error code, as listed in Chapter 4 of [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.

Validate S_6 MAC

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: To validate an S_6 Message Authentication Code (MAC) calculated by a CEP card on a detailed transaction record.

Field	Length & Type	Details
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'W0'.
KMP	32 H	Master Purchase Key, encrypted under variant 3 of LMK pair 20-21.
ALGP2	1 B	Algorithm code for S_6 in purchase transactions: must equal X'10.
ID_{CEP}	6 B	CEP card serial number.
NT_{CEP}	2 B	CEP card transaction number.
$DEXPP_{CEP}$	3 B	CEP card expiration date for offline transactions.
TI_{CEP}	1 B	CEP card transaction indicator.
$DTHR_{PDA}$	5 B	PDA transaction date and time.
$CURR_{PDA}$	3 B	PDA currency.
AM_{CEP}	1 B	CEP card authentication method.
RID_{PSAM}	5 B	Registered identity of the entity assigning PSAM Creator IDs.
$ID_{PSAMCREATOR}$	4 B	Identifier for the creator of a PSAM.
ID_{PSAM}	4 B	Identifier of a PSAM.
NT_{PSAM}	4 B	PSAM transaction number.
$MTOT_{CEP}$	4 B	CEP card total transaction amount.
M_{PDA}	4 B	PDA transaction amount.
BAL_{CEP}	4 B	CEP card slot balance.
S_6	8 B	Transaction MAC, to be validated.
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 'W1'.
Error Code	2 N	'00': No error (S_6 verification successful) '01': S_6 verification failure '10': KMP parity error '70': Invalid ALGP2 or a standard error code, as listed in Chapter 4 of [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.

Validate $S_{6'}$ MAC

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: To validate an $S_{6'}$ Message Authentication Code (MAC) calculated by a CEP card on an aggregated transaction.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'W2'.
KMP	32 H	Master Purchase Key, encrypted under variant 3 of LMK pair 20-21.
ALGP2	1 B	Algorithm code for $S_{6'}$ in purchase transactions: must equal X'10.
ID_{CEP}	6 B	CEP card serial number.
NT_{CEP}	2 B	CEP card transaction number.
MAC Type	1 B	MAC type; must equal X'01.
$CURR_{PDA}$	3 B	PDA currency.
$MTOT_{AGG}$	4 B	Amount of aggregated transactions in the current record.
NT_{AGG}	2 B	Number of aggregated transactions in the current record.
ID_{BATCH}	2 B	Identifier of batch containing the aggregated transactions.
RID_{PSAM}	5 B	Registered identity of the entity assigning PSAM Creator IDs.
$ID_{PSAMCREATOR}$	4 B	Identifier for the creator of a PSAM.
ID_{PSAM}	4 B	Identifier of a PSAM.
NT_{PSAM}	4 B	PSAM transaction number.
$S_{6'}$	8 B	Transaction MAC, to be validated.
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 'W3'.
Error Code	2 N	'00': No error ($S_{6'}$ verification successful) '01': $S_{6'}$ verification failure '10': KMP parity error '70': Invalid ALGP2 '71': Invalid MAC type or a standard error code, as listed in Chapter 4 of [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.

Validate $S_{6''}$ MAC

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: To validate an $S_{6''}$ Message Authentication Code (MAC) calculated by a CEP card on an Issuer backup total.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	m A	Value 'W4'.
KMP	32 H	Master Purchase Key, encrypted under variant 3 of LMK pair 20-21.
ALGP2	1 B	Algorithm code for $S_{6''}$ in purchase transactions: must equal X'10.
ID_{CEP}	6 B	CEP card serial number.
NT_{CEP}	2 B	CEP card transaction number.
MAC Type	1 B	MAC type; must equal X'02.
$CURR_{PDA}$	3 B	PDA currency.
$MTOTold_{IB}$	4 B	Signed amount of transactions in the batch for the Issuer.
$NTold_{IB}$	2 B	Signed number of transactions in the batch for the Issuer.
ID_{BATCH}	2 B	Identifier of batch containing the aggregated transactions.
RID_{PSAM}	5 B	Registered identity of the entity assigning PSAM Creator IDs.
$ID_{PSAMCREATOR}$	4 B	Identifier for the creator of a PSAM.
ID_{PSAM}	4 B	Identifier of a PSAM.
NT_{PSAM}	4 B	PSAM transaction number.
$S_{6''}$	8 B	Transaction MAC, to be validated.
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 'W5'.
Error Code	2 N	'00': No error ($S_{6''}$ verification successful) '01': $S_{6''}$ verification failure '70': Invalid ALGP2 '71': Invalid MAC type '10': KMP parity error or a standard error code, as listed in Chapter 4 of [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.

Validate $S_{5',DLT}$ MAC

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: To validate an $S_{5',DLT}$ Message Authentication Code (MAC), which provides the Issuer with the ability to verify the integrity of a non-CEP transaction.

Field	**Length & Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'W6'.
$KI_{S5'}$	32 H	$S_{5'}$ Issuer Key, encrypted under variant 4 of LMK pair 20-21.
ALG_{KS}	1 B	Algorithm code for $S_{5'}$ transactions; must equal X'01.
NT_{PSAM}	4 B	PSAM transaction number.
TI_{PDA}	1 B	PDA transaction indicator.
$DTHR_{PDA}$	5 B	PDA transaction date and time.
ID_{PSAM}	4 B	Identifier of a PSAM.
M_{PDA}	4 B	PDA transaction amount.
$DEXP_{CARD}$	3 B	Card expiry date.
AM_{CEP}	1 B	CEP card authentication method.
BAL_{CEP}	4 B	CEP card slot balance.
RID_{PSAM}	5 B	Registered identity of the entity assigning PSAM Creator IDs.
$ID_{PSAMCREATOR}$	4 B	Identifier for the creator of a PSAM.
NT_{PSAM}	4 B	PSAM transaction number.
$S_{5',DLT}$	8 B	Transaction MAC, to be validated.
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 'W7'.
Error Code	2 N	'00': No error ($S_{5',DLT}$ verification successful) '01': $S_{5',DLT}$ verification failure '10': $KI_{S5'}$ parity error '70': Invalid ALG_{KS} or a standard error code, as listed in Chapter 4 of [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.

Validate $S_{5',ISS}$ MAC

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: To validate an $S_{5',ISS}$ Message Authentication Code (MAC) which provides the Issuer with the ability to verify the integrity of a non-CEP transaction.

Field	**Length & Type**	**Details**
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'W8'.
$KI_{S5'}$	32 H	$S_{5'}$ Issuer Key, encrypted under variant 4 of LMK pair 20-21.
ALG_{KS}	1 B	Algorithm code for $S_{5'}$ transactions; must equal X’01.
NT_{PSAM}	4 B	PSAM transaction number.
MAC Type	1 B	MAC type; must equal X’01 or X’02.
MTOT	4 B	$MTOTold_{IB}$ or $MTOT_{AGG}$.
$CURR_{PDA}$	3 B	PDA currency.
NT	2 B	$NTold_{IB}$ or NT_{AGG}.
ID_{BATCH}	2 B	Identifier of batch containing the aggregated transactions.
RID_{PSAM}	5 B	Registered identity of the entity assigning PSAM Creator IDs.
$ID_{PSAMCREATOR}$	4 B	Identifier for the creator of a PSAM.
ID_{PSAM}	4 B	Identifier of a PSAM.
$S_{5',ISS}$	8 B	Transaction MAC, to be validated.
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 'W9'.
Error Code	2 N	'00': No error ($S_{5',ISS}$ verification successful) '01': $S_{5',ISS}$ verification failure '02': Invalid ALG_{KS} '03': Invalid MAC type '10': $KI_{S5'}$ parity error or a standard error code, as listed in Chapter 4 of [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.

Validate the S_4 MAC (Old Terminals)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Validate the S_4 MAC (MAC of the PSAM for a Batch) for old terminals.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'X0'.
*KMAC$_{S4}$	32 H	Double length KMAC$_{S4}$ encrypted under LMK pair 20-21 variant 7.
S_4	16 H	Signature for verification.
ID$_{CAD}$	4 B	Identifier for the CAD.
ID$_{MCARD}$	4 B	Identifier for the MCard.
Collection Number	1 B	Collection Number.
MCard Date	1 B	Month number as known by the MCard.
MTOT$_{BATCH}$	4 B	Total of all successful payments in the batch.
CURR$_{MCARD}$	2 B	Currency code for the batch.
NT$_{BATCH}$	2 B	Number of payment records in the batch.
NTENQ$_{BATCH}$	2 B	Number of successful balance enquiries in the batch.
NTREJ$_{BATCH}$	2 B	Total number of invalid records in the batch.
NTFLT$_{BATCH}$	2 B	Number of non-readable ICCs.
NTSFLT$_{BATCH}$	2 B	Number of system faults.
MCard Version	1 B	Firmware version of the MCard.
CEXP$_{MCARD}$	1 B	Currency exponent.
Batch Close Date Time	2 B	Batch close date and time (may be all a zeroes).
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 'X1'.
Error Code	2 N	'00': No error (S_4 validated successfully) '01': S_4 validation failed '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [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.

Validate the S_4 MAC (New Terminals)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Validate the S_4 MAC for new terminals.

Notes: This command does not check the contents of the data block over which the MAC is generated. It is the responsibility of the user of the command to ensure the data format is correct.

Field	Length & Type	Details
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'X2'.
*KMAC$_{S4}$	32 H	Double length KMAC$_{S4}$ encrypted under LMK pair 20-21 variant 7.
S_4	16 H	Signature for verification.
ID$_{PSAM}$	4 B	Identifier for a PSAM.
ID$_{BATCH}$	2 B	Identifier for a POS Transaction Batch.
NT$_{BATCH}$	2 B	The number of payment and cancellation transactions in this batch.
Data Length	3 N	Length in bytes of the following data block.
Data Block D_4	n B	Binary data 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 'X3'.
Error Code	2 N	'00': No error (S_4 validated successfully) '01': S_4 validation failed '10': KMAC parity error '70': Data D_4 length error or a standard error code, as listed in Chapter 4 of [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.

Validate the S_5 MAC (Old Terminals)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Validate the S_5 MAC (MAC of the PSAM for a Batch) for old terminals.

Notes: The MACing process for old terminals has a different pad process than standard.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'X4'.
*KMAC$_{S5}$	32 H	Double length KMAC$_{S5}$ encrypted under LMK pair 20-21 variant 8.
S_5	16 H	Signature for verification.
ID$_{MCARD}$	4 B	MCard Identifier.
Collection Number	1 B	Collection Number.
NT$_{MCARD}$	4 B	MCard Transaction Number.
C.C.	1 B	Proprietary Completion Codes.
Card Balance	4 B	New Card Balance.
MTOT$_{MCARD}$	4 B	Total Transaction Amount.
CURR$_{MCARD}$	2 B	Currency Code.
CEXP$_{MCARD}$	1 B	Currency Exponent.
ID$_{ISS, MCARD}$	3 B	Issuer BIN or zeroes (For reloadable or disposable cards).
ID$_{CARD, MCARD}$	5 B	Card Identifier.
NT$_{IEP}$	2 B	Card Transaction Number.
RFU	1 B	Reserved.
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 'X5'.
Error Code	2 N	'00': No error (S_5 validated successfully) '01': S_5 validation failed '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [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.

Validate the $S_{5'}$ MAC (MAC of the PSAM for a Transaction) (New Terminals)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Validate the $S_{5'}$ MAC for new terminals.

Notes:

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'X6'.
*KMAC$_{S5}$	32 H	Double length KMAC$_{S5}$ encrypted under LMK pair 20-21 variant 8.
$S_{5'}$	16 H	Signature for verification.
Length of DD$_{CEP}$	1 B	Length of DD$_{CEP}$ field: range 0 – 6.
Record Length	2 B	Record Length.
Record Type	1 B	Record Type.
ID$_{RECORD}$	2 B	Record number within batch.
RID$_{PSAM}$	5 B	The RID of the PSAM creator.
ID$_{PSAMCREATOR}$	4 B	The identifier assigned to the PSAM creator by the RID$_{PSAM}$ owner.
ID$_{PSAM}$	4 B	Identifier for a PSAM.
ID$_{BATCH}$	2 B	Identifier for a POS Transaction Batch.
NT$_{PSAM}$	4 B	PSAM Transaction Number.
MTOT$_{PDA}$	4 B	Net value of transaction.
CURR$_{PDA}$	3 B	Currency of transaction.
ID$_{SCHEME}$	1 B	Reference number assigned to AID$_{CEP}$ in AID table.
ID$_{ISS}$	4 B	Issuer Identifier.
ID$_{CEP}$	6 B	ID of CEP or IEP application.
NT$_{CEP}$	2 B	CEP card transaction number.
S_6	8 B	Signature from CEP card.
CC$_{PDA}$	2 B	CEPS completion code.
CC$_{PROP}$	2 B	Proprietary completion code.
Slot Balance	4 B	Slot balance at end of transaction.
TI$_{PDA}$	1 B	Transaction indicator.
M$_{PDA}$	4 B	Value of last successful increment.
DTHR$_{PDA}$	5 B	Date & Time stamp for transaction.
DEXP$_{CARD}$	3 B	Card expiration date.
ALG$_{KS}$	1 B	Algorithm to calculate S_4 & S_5.
AM$_{CEP}$	1 B	Authentication Method.
VKP$_{CA, ISS, CEP}$	1 B	Version number of the issuer CA key.
ID$_{REG, ISS}$	4 B	Issuer region ID.
VKP$_{REG, ISS}$	1 B	Version number of the regional CA key.
CSN$_{ISS, CEP}$	3 B	Issuer certificate serial number.

L_{DDCEP}	1 B	Length of the DD_{CEP} field.
DD_{CEP}	n B	DD_{CEP} response.
NUM_{SEG}	1 B	Number of Segments.
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 'X7'.
Error Code	2 N	'00': No error ($S_{5'}$ validated successfully) '01': $S_{5'}$ validation failed '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [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.

Validate the S5 Variant MAC (MAC of the PSAM for an Issuer Total) (New Terminals)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Validate the S$_5$ Variant MAC for new terminals.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'X8'.
*KMAC$_{S5}$	32 H	Double length KMAC$_{S5}$ encrypted under LMK pair 20-21 variant 8.
S$_5$ Variant	16 H	Signature for verification.
Length of DD$_{CEP}$	1 B	Length of DD$_{CEP}$ field: range 0 to 16.
Record Length	2 B	Record Length.
Record Type	1 B	Record Type.
ID$_{RECORD}$	2 B	Record number within batch.
RID$_{PSAM}$	5 B	The RID of the PSAM creator.
ID$_{PSAMCREATOR}$	4 B	The identifier assigned to the PSAM creator by the RID$_{PSAM}$ owner.
ID$_{PSAM}$	4 B	Identifier for a PSAM.
ID$_{BATCH}$	2 B	Identifier for a POS Transaction Batch.
NT$_{PSAM}$	4 B	PSAM Transaction Number.
MTOT$_{SIGNED}$	4 B	Net value of record.
CURR$_{PDA}$	3 B	Currency of transaction.
ID$_{SCHEME}$	1 B	Reference number assigned to AID$_{CEP}$ in AID table.
ID$_{ISS}$	4 B	Issuer Identifier.
ID$_{CEP}$	6 B	ID of CEP or IEP application.
NT$_{CEP}$	2 B	CEP card transaction number.
S$_{6'}$ or S$_{6''}$	8 B	Signature from CEP card.
NT$_{ISS, SIGNED}$	2 B	Number of transactions accounted for in the signed MTOT in this summary.
MTOT$_{NOSIG}$	4 B	Unsigned net value of record.
NT$_{ISS, NOSIG}$	4 B	Number of transactions included in unsigned net value.
ALG$_{KS}$	1 B	Algorithm used to calculate S$_4$ and S$_5$ MACs.
L$_{DDCEP}$	1 B	Length of the DD$_{CEP}$ field.
DD$_{CEP}$	N B	DD$_{CEP}$ response.
NUM$_{SEG}$	1 B	Number of Segments.
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.

Field	Length & Type	Details
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 'X9'.
Error Code	2 N	'00': No error (S_5 variant validated successfully) '01': S_5 variant validation failed '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [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.

Create the Acknowledgement MAC (Old Terminals)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Create the Acknowledgement MAC for old terminals.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Y0'.
*KMAC$_{ACQ}$	32 H	Double length KMAC$_{ACQ}$ encrypted under LMK pair 20-21 variant 9.
Rec. ID$_{MCARD}$	4 B	ID of the receiving Mcard.
Gen. ID$_{MCARD}$	4 B	ID of the MCard that generated the collection batch.
Coll. No.	1 B	Collection Number.
NT$_{BATCH}$	2 B	The total number of purchase and cancellation transactions included in the batch.
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 'Y1'.
Error Code	2 N	'00': No error '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [2].
S$_{AQC}$	16 H	Acknowledgement MAC.
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.

Create the Acknowledgement MAC (New Terminals)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Create the Acknowledgement MAC for new terminals.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Y2'.
Mode Flag	1 N	Mode Flag: '0': *KMAC$_{ACK}$ supplied '1': No *KMAC$_{ACK}$ supplied.
*KMAC$_{ACK}$	32 H	Double length KMAC$_{ACK}$ encrypted under LMK pair 20-21 variant 9, only supplied if Mode Flag = '0'.
CLA	1 B	CLA.
INS	1 B	INS.
P1P2	2 B	P1P2.
L$_{C}$	1 B	L$_{C}$.
ID$_{THREAD}$	1 B	ID$_{THREAD}$.
Action Requested	1 B	Action Requested.
RID$_{PSAM}$	5 B	The RID of the PSAM Creator.
ID$_{PSAMCREATOR}$	4 B	The identifier assigned to the PSAM creator by the RID$_{PSAM}$ owner.
ID$_{PSAM}$	4 B	Identifier for a PSAM.
DATE$_{PSAM}$	2 B	Current month.
ID$_{BATCH}$	2 B	Identifier for a POS Transaction Batch.
NT$_{RECORD}$	2 B	The number of payment records in a batch.
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 'Y3'.
Error Code	2 N	'00': No error '10': KMAC parity error '70': Invalid Mode Flag or a standard error code, as listed in Chapter 4 of [2].
S_{ACK}	16 H	Acknowledgement MAC
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.

Create the Update MAC

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Create the Update MAC.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Y4'.
*KMAC$_{UPD}$	32 H	Double length KMAC$_{UPD}$ encrypted under LMK pair 22-23 variant 1.
ID$_{BATCH}$	2 B	Identifier for a POS Transaction Batch.
ID$_{PSAM}$	4 B	PSAM Identifier assigned by the PSAM creator.
CLA	1 B	CLA.
INS	1 B	INS.
P1P2	2 B	P1P2.
L$_{C}$	1 B	L$_{C}$.
ID$_{THREAD}$	1 B	ID$_{THREAD}$.
Update Number	1 B	Update Number.
TAG	2 B	Tag identifying data in the update.
LEN	1 B	Length of the following data.
Update data	n B	Update data.
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 'Y5'.
Error Code	2 N	'00': No error '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [2].
S$_{UPD}$	16 H	Update MAC.
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.

Validate the S_{ADMIN} MAC (Administrative MAC of the PSAM)

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Validate the S_{ADMIN} MAC.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Y6'.
S_{ADMIN}	16 H	Signature for verification.
Length	2 B	Length.
Record Type	1 B	Record Type.
RID_{PSAM}	5 B	The RID of the PSAM Creator.
$ID_{PSAMCREATOR}$	4 B	The identifier assigned to the PSAM creator by the RID_{PSAM} owner.
ID_{PSAM}	4 B	PSAM Identifier assigned by the PSAM creator.
Administrative Record ID	1 B	Operating data table content status.
CNT_{TABLE}	1 B	Number of tables whose status is being reported in this record.
Table ID_N	1 B	Identifies the table being reported.
HASH $value_N$	8 B	Hash value of data in the table.
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 'Y7'.
Error Code	2 N	'00': No error (S_{ADMIN} validated successfully) '01': S_{ADMIN} validation failed '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [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.

Create the Merchant Acquirer MAC

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Create the Merchant Acquirer MAC.

Field	Length & Type	Details
	COMMAND MESSAGE	
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Y8'.
*KMAC$_{MA}$	32 H	Double length KMAC$_{MA}$ encrypted under LMK pair 22-23 variant 2.
Date & Time	6 B	Date and Time.
Function Code	2 B	Function Code.
ID$_{SOURCE}$	4 B	ID$_{SOURCE}$.
CURR$_{CPDA}$	2 B	CURR$_{CPDA}$, can be all zeroes.
Block 1	9 B	Block 1 containing CNT$_{BATCH}$, CNT$_{ACCEPT}$, ID$_{BATCH}$, NT$_{BATCH}$ and RESEND.
Block 2	9 B	Block 2 containing Amount and Net Reconciliation.
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 'Y9'.
Error Code	2 N	'00': No error '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [2].
S$_{MA}$	16 H	Merchant Acquirer MAC.
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.

Validate the Card Issuer MAC

Variant ☑	Key Block ☒
License: **HSM9-LIC004**	
Authorization: **Not required**	

Command: Validate the Card Issuer MAC.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	Subsequently returned to the Host unchanged.
Command Code	2 A	Value 'Z0'.
*KMAC$_{CI}$	32 H	Double length KMAC$_{CI}$ encrypted under LMK pair 22-23 variant 3.
S$_{CI}$	16 H	Signature for Verification.
Date & Time	6 B	Date and Time.
Function Code	2 B	Function Code.
ID$_{DEST}$	4 B	ID$_{DEST}$.
Block 1	2 B	Block 1, fixed to all zeroes.
Block 2	9 B	Block 2 containing CNT$_{BATCH}$, CNT$_{ACCEPT}$, ID$_{BATCH}$, NT$_{BATCH}$ and RESEND.
Block 3	9 B	Block 3 containing Amount and Net Reconciliation.
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 'Z1'.
Error Code	2 N	'00': No error (S$_{CI}$ validated successfully) '01': S$_{CI}$ validation failed '10': KMAC parity error or a standard error code, as listed in Chapter 4 of [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.

THALES

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 <