

**Host Security Module
RG7000**

Programmer's Manual

1270A514 Issue 5

HOST SECURITY MODULE RG7000

PROGRAMMERS MANUAL, REVISION STATUS

Revision	Release Date	HSM Functional Revision
1270A514 Issue 1	January 1999	1.04 / 5.04
1270A514 Issue 2	May 2000	1.05 / 5.05 / Pre-release
1270A514 Issue 3	May 2000	1.05 / 5.05
1270A514 Issue 4	November 2001	1.05 / 5.05
1270A514 Issue 5	July 2002	2.0 / 6.0

This manual describes the functionality within the 2.0/6.0 base release of HSM firmware. For all other versions please refer to the appropriate manuals and associated HSM firmware specifications.

THALES e-SECURITY

Europe, Middle East, Africa

Meadow View House
 Crendon Ind. Estate
 Long Crendon
 Aylesbury
 Buckinghamshire HP18 9EQ
 UK

Telephone: +44 1844 201800
 Fax: +44 1844 208550

Support

Telephone: +44 1844 202566
 Fax: +44 1844 208356
 emea.support@thales-esecurity.com

Americas

Suite 200
 2200 North Commerce Parkway
 Weston, FL 33326
 USA

Telephone: 1-888-744-4976 (in U.S.)
 +1 954-888-6200 (outside U.S.)
 Fax: +1 954-888-6211

Support

Telephone: 800-521-6261 (in U.S.)
 +1 954-888-6277 (outside U.S.)
 Fax: +1 954-888-6233

americas.support@thales-esecurity.com

Asia Pacific

Units 2205-06, 22/F
 Vicwood Plaza
 199 Des Voeux Road, Central
 Hong Kong

Telephone: +852 2815 8633
 Fax: +852 2815 8141

Support

Telephone: +852 2815 8633
 Fax: +852 2815 8141
 asia.support@thales-esecurity.com

www.thales-esecurity.com

© Copyright 1987 - 2002 THALES e-SECURITY LTD

This document is issued by Thales e-Security Limited (hereinafter referred to as Thales) in confidence and is not to be reproduced in whole or in part without the prior written approval of Thales. The information contained herein is the property of Thales and is to be used only for the purpose for which it is submitted and is not to be released in whole or in part without the prior written permission of Thales.

Host Security Module RG7000

THALES e-SECURITY LTD. ("THALES") COMPUTER PROGRAM LICENSE AGREEMENT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT (the "AGREEMENT"). FOR PURPOSES OF THIS AGREEMENT, "SOFTWARE" IS DEFINED TO INCLUDE COMPUTER PROGRAMS INTENDED TO BE RUN ON A WORK STATION, PC, OR SIMILAR MACHINE, AND INCLUDES THE CD-ROM OR OTHER MEDIA ON WHICH THE SOFTWARE IS CONTAINED. "FIRMWARE" IS DEFINED TO INCLUDE COMPUTER PROGRAMS WHICH ARE INTENDED TO BE RUN SOLELY ON OR WITHIN A HARDWARE MACHINE ("MACHINE") PROVIDED BY THALES, INCLUDING, WITHOUT LIMITATION, FPGA BITSTREAMS. THE SOFTWARE AND FIRMWARE AND THE ACCOMPANYING USER DOCUMENTATION (THE "DOCUMENTATION") ARE LICENSED (NOT SOLD) TO YOU BY THALES DIRECTLY OR THROUGH AUTHORIZED RESELLERS OF THALES. OPENING OR INSTALLING ANY OF THE CONTENTS OF THIS CD-ROM OR OTHER PROVIDED MEDIA PACKAGE INDICATES YOUR ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT AGREE WITH THE TERMS AND CONDITIONS, PROMPTLY RETURN THE PACKAGE, THE MACHINE WHICH CONTAINS A COPY OF THE LICENSED FIRMWARE, AND ALL OTHER ENCLOSED ITEMS, IF ANY, TO THE PLACE WHERE YOU OBTAINED THEM, AND YOU WILL RECEIVE A REFUND.

LICENSE GRANT

A. In consideration of the license fee paid to THALES or to an authorized THALES reseller, THALES hereby grants you, and you accept a nonexclusive license to use the Software on a single machine (if a "single license" is purchased) or multiple machines (if an "organizational license" is purchased) owned, leased, or otherwise controlled by you, and to use the Firmware solely on the Machine sold to you by THALES or its dealers, if any, but only to operate or engage those features and/or applications for which a charge appears on your order and invoice under the terms stated in this Agreement. If a software or Firmware enabling key or other similar access device (the "Key") is provided, you agree to use same solely for accessing the Software on a single PC or Firmware on a single Machine. Title and ownership of the Software, Firmware, Documentation and/or Key remain in THALES or its suppliers. If an organizational license is purchased, then you may use the Software or Firmware on multiple Machines in your organization regardless of quantity, provided all Machines are located within a single country. A separate single or organizational license will be required in each country.

B. You may not decompile, reverse engineer, modify, or copy the Software, Firmware, or Documentation for any purpose, except you may copy the Software into machine-readable or printed form for backup purposes in the event the CD-ROM or other provided media is damaged or destroyed. You may combine the Software with other programs. Any portion of the Software merged into or used in conjunction with another program will continue to be the property of THALES and is subject to the terms and conditions of this Agreement.

C. The Software, Firmware, and the Documentation are copyrighted by THALES and/or its suppliers. You agree to respect and not to remove or conceal from view any copyright or trademark notice appearing on the Software, Firmware, or Documentation, and to reproduce any such copyright or trademark notice on all copies of the Software, Firmware, and Documentation or any portion thereof made by you as permitted hereunder and on all portions contained in or merged into other programs and documentation.

D. You may transfer the Software, Firmware, and this license to another party if the other party agrees to accept the terms and conditions of this Agreement. If you transfer the Software and/or Firmware, you must at the same time either transfer all copies whether in printed or machine-readable form, and the Machine, if any, on which the Firmware is licensed for use, to the same party or destroy any copies not transferred; this includes all modifications and portions of the Software and/or contained or merged into other programs.

YOU MAY NOT USE, COPY, MODIFY, OR TRANSFER THE SOFTWARE, FIRMWARE, DOCUMENTATION OR KEY, OR ANY COPY, MODIFICATION OR MERGED PORTION, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED FOR IN THIS LICENSE.

IF YOU TRANSFER POSSESSION OF ANY COPY, MODIFICATION OR MERGED PORTION OF THE SOFTWARE, FIRMWARE, OR DOCUMENTATION OR KEY TO ANOTHER PARTY, EXCEPT AS PROVIDED IN THIS SECTION D, YOUR LICENSE IS AUTOMATICALLY TERMINATED.

TERM

This Agreement is effective upon your acceptance (as set forth above) and shall continue until terminated. You may terminate this license at any time by destroying the Software, Key, and Documentation along with all copies, modifications and merged portions in any form, and return the Machine (including Firmware) to THALES or its authorized resellers. It will also terminate upon conditions set forth elsewhere in this Agreement if you fail to comply with any term or condition of this Agreement. You agree upon such termination to destroy the Software, Documentation, and Key together with all copies, modifications and merged portions in any form, and to return the Machine (including Firmware) to THALES or its authorized resellers.

LIMITED WARRANTY

The following limited warranty applies only to the Software and/or Firmware licensed hereunder. The hardware Machine is warranted pursuant to a separate Warranty set forth in the Machine documentation. The Machine documentation is contained on the CD-ROM, if any.

During the first 90 days after receipt of the Software and/or Firmware by you, as evidenced by a copy of your receipt, invoice or other proof of purchase (the "Warranty Period"), THALES warrants, for your benefit alone, that the Software and Firmware when properly installed, will perform substantially in conformance with the Documentation provided by THALES at the time you obtained the Software and/or Firmware from THALES or its authorized resellers, and that the media on which the Software and/or Firmware is furnished will be free from defects in materials and workmanship under normal use.

EXCEPT AS SPECIFICALLY PROVIDED ABOVE, THE WARRANTIES PROVIDED HEREIN ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. WHEREVER SUCH EXCLUSION IS NOT PERMITTED BY LAW, ALL IMPLIED WARRANTIES, INCLUDING THOSE OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE, SHALL BE LIMITED TO THE WARRANTY PERIOD. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH MAY VARY FROM JURISDICTION TO JURISDICTION.

THALES does not warrant that the functions contained in the Software or Firmware will meet your requirements or that their operation will be uninterrupted or error free.

LIMITATIONS OF REMEDIES

THALES, its authorized resellers', and/or its suppliers' entire liability and your exclusive remedies under this Agreement are as follows:

- (1) THALES shall use commercially reasonable efforts to correct any defect in the Software or Firmware which is reported by you during the Warranty Period in writing to THALES, provided such defect can be recreated by THALES in an unmodified version of the Software or Firmware. However, if THALES is unable to correct such defect within a reasonable amount of time, you may terminate this Agreement by returning the Software, Machine including Firmware, Documentation, and Key to the place where you obtained them either for replacement or, if so elected by THALES, a refund of the amount paid by you for the subject item.
- (2) THALES shall replace any media not meeting THALES' "Limited Warranty" and which is returned to THALES with a copy of your receipt, invoice or other proof of purchase or, if THALES is unable to deliver replacement media which is free from defects in materials or workmanship, you may terminate this Agreement by returning the Software, Firmware, Documentation, and Key to the place where you obtained them for a refund of the amount paid by you for the subject item.

IN NO EVENT WILL THALES, ITS AUTHORIZED RESELLERS, OR ITS SUPPLIERS BE LIABLE FOR INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES OF ANY KIND OR TYPE, INCLUDING, BUT NOT LIMITED TO LOSS OF PROFITS OR REVENUE, LOSS OF USE OF THE PRODUCT(S) OR ANY ASSOCIATED PRODUCT(S), OR COST OF SUBSTITUTED FACILITIES, PRODUCTS OR SERVICES WHICH ARISE OUT OF THALES' PERFORMANCE OR FAILURE TO PERFORM ANY OBLIGATION CONTAINED WITHIN THIS AGREEMENT OR WITH USE, OR INABILITY TO USE, SOFTWARE AND/OR FIRMWARE, WHETHER THE CLAIM FOR DAMAGES IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE. EXCEPT FOR CLAIMS FOR PERSONAL INJURY OR FOR DAMAGE TO REAL OR TANGIBLE PROPERTY TO THE EXTENT CAUSED BY THALES' FAULT OR NEGLIGENCE, THALES' MAXIMUM LIABILITY FOR ANY CLAIM FOR DAMAGES RELATING TO THALES' PERFORMANCE OR NON-PERFORMANCE UNDER THIS AGREEMENT SHALL BE LIMITED TO THE LESSER OF (a) YOUR ACTUAL DAMAGES OR (b) THE COST OF THE PRODUCT GIVING RISE TO THE LIABILITY.

SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

U.S. GOVERNMENT RESTRICTED RIGHTS

If the Software or Firmware and Documentation are acquired on behalf of a unit or agency of the United States Government, this provision applies. The Software, Firmware and Documentation: (a) were developed at private expense, and no part of it was developed with government funds; (b) are "commercial computer software" subject to limited utilization as provided in the contract between the vendor and the governmental entity; and (c) in all respects are proprietary data belonging solely to THALES. For units of the Department of Defense (DOD), the Software, Firmware and Documentation are supplied only with "Restricted Rights" as that term is defined in the DOD Supplement to the Federal Acquisition Regulations, 252.227-7013(c)(1)(ii) and:

Use, duplication or disclosure by the Government is subject to restrictions as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013. Contractor: THALES, e-SECURITY INC., 1601 N. Harrison Parkway, Building A, Suite 100, Sunrise, Florida 33323-2899.

Governmental personnel using this Software, Firmware and Documentation other than under a DOD contract or GSA Schedule, are hereby on notice that use of this Software, Firmware and Documentation is subject to restricted rights which are the same as or similar to those specified above.

EXPORT AUTHORIZATIONS

You shall assume all responsibility for obtaining any required export authorizations necessary to export any Software and/or Firmware and Documentation purchased hereunder. You shall not re-export Software and/or Documentation directly or through others, or the product of such data, to the prescribed countries for which such prohibition exists pursuant to the U.S. or U.K. export regulations unless properly authorized by the appropriate government.

GENERAL

You may not sublicense, assign or transfer this license, Software, Firmware, Documentation or Key, except as expressly provided in this Agreement. Any attempt otherwise to sublicense, assign or transfer any of the rights, duties or obligations hereunder is void.

This Agreement will be governed by the laws of the United Kingdom or the event that the Product was delivered in the United States, Latin America or Canada, the laws of the State of Virginia.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT IT IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN YOU AND THALES WHICH SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING (ORAL OR WRITTEN) BETWEEN US RELATING TO THE SOFTWARE OR FIRMWARE.

NOTWITHSTANDING THE ABOVE, IF YOU PREVIOUSLY SIGNED A SEPARATE AGREEMENT HAVING A SOFTWARE LICENSE PROVISION APPLICABLE TO THIS PROGRAM, WHICH HAS NOT EXPIRED OR BEEN TERMINATED, THE TERMS AND CONDITIONS OF SUCH SEPARATE AGREEMENT AND THE SOFTWARE LICENSE CONTAINED THEREIN SHALL TAKE PRECEDENCE OVER ALL CONFLICTING TERMS AND CONDITIONS, IF ANY, CONTAINED IN THIS LICENSE AGREEMENT. OTHERWISE, ANY ADDITIONAL TERMS AND CONDITIONS SET FORTH IN THIS LICENSE AGREEMENT SHALL SUPPLEMENT AND BE READ IN CONJUNCTION WITH THE SOFTWARE LICENSE CONTAINED IN ANY SUCH SEPARATE AGREEMENT.

**HOST SECURITY MODULE RG7000
PROGRAMMER'S MANUAL**

CONTENTS

CHAPTER 1	Programming Guide
CHAPTER 2	Host Commands
CHAPTER 3	PIN Block Formats
CHAPTER 4	Error Codes

REFERENCES

The following documents are referenced in this document:

1	Host Security Module RG7000, Operation and Installation Manual, Document Number 1270A513-5
2	PKCS#1: RSA Encryption Standard - Version 1.5 – Revised November 1993 (www.rsalabs.com)
3	PKCS#1: RSA Cryptography Standard – Version 2.0 – October 1998 (www.rsalabs.com)
4	Visa Integrated Circuit Card Specification, Version 1.3.2 – July 1999 (www.visa.com)

CHAPTER 1

PROGRAMMING GUIDE

1	INTRODUCTION	1-1
2	GENERAL	1-2
3	TRIPLE DES	1-3
3.1	KEY USAGE	1-3
3.2	KEY ENCRYPTION SCHEMES	1-3
3.3	KEY GENERATE, IMPORT AND EXPORT	1-4
4	COMMAND MESSAGE FORMAT	1-5
4.1	START OF TEXT CHARACTER	1-5
4.2	MESSAGE HEADER	1-5
4.3	COMMAND CODE	1-5
4.4	DATA	1-5
4.5	MESSAGE TRAILER	1-6
4.6	END OF TEXT CHARACTER	1-6
5	RESPONSE MESSAGE FORMAT	1-7
5.1	START OF TEXT CHARACTER	1-7
5.2	MESSAGE HEADER	1-7
5.3	RESPONSE CODE	1-8
5.4	ERROR CODE	1-8
5.5	DATA	1-8
5.6	MESSAGE TRAILER	1-8
5.7	END OF TEXT CHARACTERS	1-8
6	DATA REPRESENTATION	1-9
6.1	ASCII CHARACTER CODES	1-10
6.2	EBCDIC CHARACTER CODES	1-11
7	TRANSPARENT ASYNCHRONOUS COMMUNICATIONS	1-13
7.1	MESSAGE FORMAT	1-13
7.2	HSM PROCESSING OF PACKETS	1-13
7.3	PARITY ERRORS	1-14
8	INPUT/OUTPUT FLOW CONTROL	1-15
9	ERROR HANDLING	1-16
10	USE OF MULTIPLE HSMS	1-17
11	USER STORAGE	1-18
11.1	ASSIGNING AND USING INDICES	1-18
11.2	SPECIFYING STORED DATA	1-19
12	PRINTING TO AN HSM-ATTACHED PRINTER	1-21
13	REJECTION OF WEAK AND SEMI-WEAK KEYS	1-22
14	LOCAL MASTER KEYS	1-23
15	LOCAL MASTER KEY VARIANTS	1-25
16	LOCAL MASTER KEY TRIPLE DES VARIANT SCHEME	1-27

1 INTRODUCTION

The Host Security Module (HSM) acts as a peripheral to the Host computer. It performs cryptographic processing in a physically secure environment on behalf of the Host. The processing is performed by the HSM in response to commands which it receives via a serial data link.

Typically the HSM is used in a realtime, online environment performing key management, PIN and MAC related functions as required by the system.

This manual contains programming notes to assist the application programmer and a complete command reference section detailing each of the Host commands available. A glossary of terms is included at the end of the Operation and Installation Manual.

For commands that are entered manually at a Console terminal attached to the HSM, see the associated Operation and Installation Manual.

2 GENERAL

The application program sends commands to the HSM, and receives responses from the HSM. Each command and response consists of a variable number of fields.

In order that the data can be sent via a serial data link, it is encoded as either ASCII or EBCDIC characters (the choice is made during the HSM configuration).

Versions of the HSM can be configured to support asynchronous, bisynchronous, SNA, SDLC, TCP/IP and IBM channel communications protocols. The HSM has no flow control support so the programmer must ensure that the HSM input buffer is not exceeded. SNA/SDLC units do not support RSA key functions.

The HSM returns an error code to the Host as part of the response message. The programmer must ensure that a suitable response is made to each type of error.

In a typical system, a minimum of two HSMs are connected to the Host via separate Host ports. The HSMs are independent, and the programmer should make maximum use of all the HSMs to increase throughput, using one HSM if another is already processing data or is faulty. Also, it is useful to ensure that the program allows for additional HSMs to be subsequently added as throughput requirements increase.

Each HSM has a user storage area reserved for use by the programmer to store data required by the HSM during processing. Typically it is used to store keys and tables. Instructing the HSM to access data from user storage reduces the amount of data necessary in each command, and thus reduces the communications time. The user storage area does not have battery backup, so must be reloaded whenever the HSM is powered up and when coming on-line from an off-line state.

There is a facility to print data (e.g., account holder PINs) at a printer connected to an RG7X00 series HSM. The HSM must have format information for the data before sending it to the printer. The program must send a print format command to the HSM before print commands can be issued.

Normally the HSM responds to all data that it receives. However, in some environments, the Host computer sends system messages to all attached devices. The HSM has support for two IBM environments where this occurs; these are CICS and IMS. If using the SRM in an IBM environment, see the SRM manual for the appropriate HSM configuration settings.

The RG7X10 High-Speed HSM does not support printing functions in its standard command set. The printing facilities can be made available to special order. It is recommended that an RG7X00 series HSM is chosen to implement secure printing facilities.

3 TRIPLE DES

The HSM host commands support single, double and triple length DES keys. The command set is completely backward compatible with earlier versions of firmware. The commands support extensions to enable the specification of key length and key encryption scheme to use.

3.1 Key Usage

If the first character of the key is a hexadecimal character (0 – 9 or A - F) or “K” or “S” the commands will operate as previously specified. In most circumstances the key is single length except for ZMKs when the ZMK length is configured for double length or for specific keys that are double length by definition. This is the 16H or 32H length and types.

To support double and triple length keys throughout the command set key scheme tags have been defined these enable the HSM to determine the key length and encryption mechanism used for a key. The key scheme tag prefixes the key. This is the 1A+32H or 1A+48H length and types.

3.2 Key Encryption Schemes

There are currently two key encryption schemes supported by the HSM.

ANSI X9.17 method

Each key of a double or triple length key is encrypted separately using the ECB mode of encryption. This scheme is only available for import and export of keys and must be enabled via the Configure Security (CS) command.

The tags for this scheme are:

- X – Double length DES keys.
- Y – Triple length DES keys.

Variant method

Each key of a double or triple length key is encrypted separately using the ECB mode of encryption. For the second or third key, depending on whether it is a double or triple length key, a variant is applied to the encryption key. There are five variants to enable the encryption of each key distinctly. This application of variants enforces the key use as a double or triple length key and the key order. This scheme is available for encryption of keys under the Local Master Key and for import and export of keys.

Local Master Keys by definition are double length keys consisting of a left and right half. Each half consists of 16 hexadecimal characters. Other keys, such as ZMKs may be of double or triple lengths. Triple length keys are comprised of three parts; left, middle and right. Each part, like double length keys, consists of 16 hexadecimal characters. The variant is applied to the right half of double length encrypting keys, and to the middle part of triple length encrypting keys.

The tags for this scheme are as follows:

- U – Double length DES keys.
- T – Triple length DES keys.

Double length key variants	Key 1 of 2 – A6 Key 2 of 2 – 5A
Triple length key variants	Key 1 of 2 – 6A Key 2 of 3 – DE Key 3 of 3 – 2B

Example:

Given a double length encrypting key of: XXXX XXXX XXXX XXXX YYYYY YYYYY YYYYY YYYYY
 And a double length key of: AAAA AAAA AAAA BBBB BBBB BBBB BBBB

- The variant A6 is applied to the first two hex characters of Y to encrypt A.
- The variant 5A is applied to the first two hex characters of Y to encrypt B

Given a double length encrypting key of: XXXX XXXX XXXX XXXX YYYYY YYYYY YYYYY YYYYY
 And a triple length key of: AAAA AAAA AAAA AAAA BBBB BBBB BBBB BBBB BBBB
 CCCC CCCC CCCC CCCC

- The variant 6A is applied to the first two hex characters of Y to encrypt A.
- The variant DE is applied to the first two hex characters of Y to encrypt B
- The variant 2B is applied to the first two hex characters of Y to encrypt C

Variants are applied by “Exclusive Oring” (XOR) the first two characters of Y with the Variant.

3.3 Key Generate, Import and Export

All the key management commands have extensions to enable the specification of key scheme to use when encrypting a key. This also defines the key length to generate within key generation commands. For import and export of keys the key schemes must be consistent as far as length is concerned i.e. if a double length key is input the key scheme flag defining the output must also be for a double length key.

The extension consists of a delimiter ";" and three single character option fields. If the extension is used all fields must be provided. If the command does not use an option "0" or any valid value can be entered in that field. The option will be ignored during processing.

The option fields are:

Key scheme for encrypting the output key under ZMK.
 Key scheme for encrypting the output key under LMK.
 Key check value type.

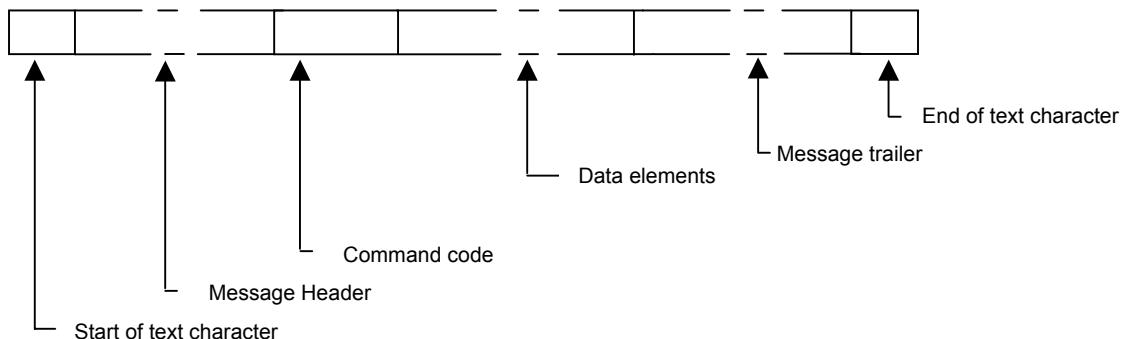
The valid values for these options are:

Key under ZMK	- Z, U, T - X, Y	Z – Single Length, U – Double Length, T – Triple Length. Encryption under Transport Key: X – ANSI X9.17 Double Length Y – ANSI X9.17 Triple Length These follow key encryption schemes defined previously.
Key under LMK	- Z, U, T	Z – Single length, U – Double Length, T – Triple Length.
Key check value	- 0 - 1 - 2	Is backwards compatible and produces a 16 hex KCV (except for DW & DY where an 8 hex KCV is returned). Produces a 6 hexadecimal character KCV. Is for special cases and is defined where used.

4 COMMAND MESSAGE FORMAT

To give the HSM an instruction, the Host application must assemble a message containing all the necessary information and send it to the HSM as a sequence of characters on the communications link. In general, each command consists of the following fields:

- Start of text character.
- Message header.
- Command code.
- Data elements.
- Message trailer.
- End of text character.



4.1 Start of Text Character

The Start of Text (STX) character indicates the start of a valid message. The ASCII and EBCDIC value is X'02. The STX character is not used in SNA-SDLC, IBM channel or TCP/IP environments.

4.2 Message Header

The message header field can be any length from 1 to 255 characters (1 to 100 for SNA/SDLC), and it is configured at HSM installation. It can contain any printable characters and the HSM returns them unmodified in the response message.

It can be used to label commands and their responses for systems that implement batch queues or which multi-thread commands.

4.3 Command Code

Every command has a unique two-character command code. The command codes are detailed in Chapter 2, Host Commands.

4.4 Data

Most HSM commands require data, often including cryptographic keys. Details of the data are shown for each command in Chapter 3, PIN Block Formats.

4.5 Message Trailer

The message trailer (EM) is an additional variable-length field (to a maximum of 32 characters), which can be used to pass additional details required by the Host for further processing. The field should always be preceded by the EM control character; ASCII and EBCDIC value is X'19.

The data in this field can be any printable character, and it is returned in the response message unchanged.

4.6 End of Text Character

The End of Text (ETX) character indicates the end of command data. The HSM ignores any data received after the ETX and before the next STX. The ETX character is not used in SNA-SDLC, IBM channel or TCP/IP environments.

The ASCII and EBCDIC value is X'03.

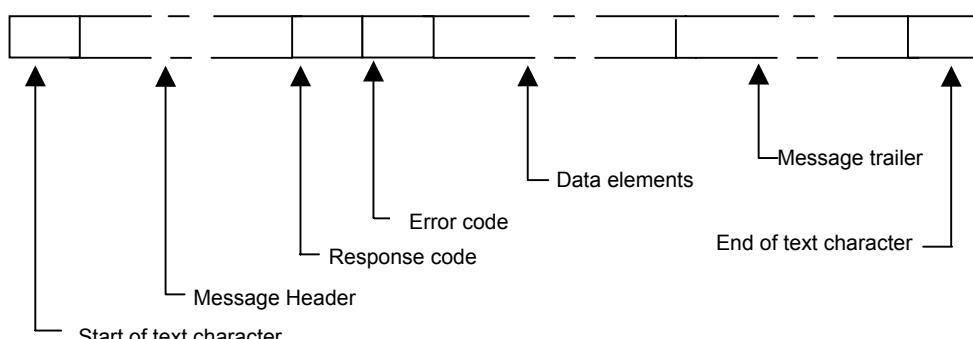
5 RESPONSE MESSAGE FORMAT

To inform the Host of the results of processing, the HSM sends a message containing all the necessary information as a sequence of characters on the communications link. A response message is generated for each of the following:

- In response to a command.
- As a second response to a print command after the HSM has finished sending the print data to the printer.
- In response to the entry of PIN solicitation data at the Console (but only after the Host has enabled this function).

Each response from the HSM consists of the following:

- Start of text character (if applicable).
- Message header.
- Response code.
- Error code.
- Data elements.
- Message trailer.
- End of text character (if applicable).



5.1 Start of Text Character

The Start of Text (STX) character indicates the start of a valid message. The ASCII and EBCDIC value is X'02. The STX character is not used in SNA-SDLC, IBM channel or TCP/IP environments.

5.2 Message Header

The message header field is a copy of the field received in the command message from the Host. The data is returned to the Host unchanged. It can be used to label commands and their responses for systems that implement batch queues or which multi-thread commands.

5.3 Response Code

Every response has a unique two-character code. Normally this code has the same first character as the command to which it is a response, and the second character is one greater than the second character of the command (e.g., if the command code is AA, the response code is AB). The value of each code is detailed in Chapter 2.

5.4 Error Code

The two-character error code field is used by the HSM to report errors detected during processing. The values are always numeric and the value 00 indicates that no errors have been found. If an error (other than 00) is returned, subsequent fields, with the exception of the end of text character, are not returned by the HSM. Error codes specific to a command or frequently returned with a command are listed with the command code in Chapter 2. A list of global errors is included in Chapter 4.

5.5 Data

Many HSM commands return data as a result of the processing. Details of the contents of the returned data are given in Chapter 2. Generally, data is not returned for error codes other than 00. There are some exceptions to this rule, for example the Key Import command (A6) returns error code 01 to advise that the key being imported is not odd parity.

5.6 Message Trailer

The message trailer (EM) field is present only if it was present in the command message, and it is returned unchanged. It is not returned for error codes other than 00.

5.7 End of Text Characters

The End of Text (ETX) field indicates the end of the response message from the HSM. In a bisynchronous system its ASCII and EBCDIC value is X'03. The End of Text field is not used in SNA-SDLC, IBM channel or TCP/IP environments.

In an asynchronous system it can be configured to be one or two characters in length, and the value of each of the characters is configurable (normally at installation time).

6 DATA REPRESENTATION

With the exception of the STX (X'02), ETX (X'03) and EM (X'19) control characters, the HSM expects all data to be encoded as either ASCII or EBCDIC characters. Where the HSM does not try and interpret the data (e.g., in the message header and message trailer fields), it is possible to include other control characters, but this is not good practice.

When sending data to the HSM, other than data that is already in character format, encode each digit (0-9, A-F) as a character (e.g., to send the hexadecimal value 1234ABCD to the HSM requires 8 characters).

6.1 ASCII Character Codes

The table shows the ASCII characters and their hexadecimal values.

ASCII	HEX	ASCII	HEX	ASCII	HEX	ASCII	HEX
NUL	00	SP	20	@	40	.	60
SOH	01	!	21	A	41	a	61
STX	02	"	22	B	42	b	62
ETX	03	#	23	C	43	c	63
EOT	04	\$	24	D	44	d	64
ENQ	05	%	25	E	45	e	65
ACK	06	&	26	F	46	f	66
BEL	07	'	27	G	47	g	67
BS	08	(28	H	48	h	68
HT	09)	29	I	49	i	69
LF	0A	*	2A	J	4A	j	6A
VT	0B	+	2B	K	4B	k	6B
FF	0C	,	2C	L	4C	l	6C
CR	0D	-	2D	M	4D	m	6D
SO	0E	.	2E	N	4E	n	6E
SI	0F	/	2F	O	4F	o	6F
DLE	10	0	30	P	50	p	70
DC1	11	1	31	Q	51	q	71
DC2	12	2	32	R	52	r	72
DC3	13	3	33	S	53	s	73
DC4	14	4	34	T	54	t	74
NAK	15	5	35	U	55	u	75
SYN	16	6	36	V	56	v	76
ETB	17	7	37	W	57	w	77
CAN	18	8	38	X	58	x	78
EM	19	9	39	Y	59	y	79
SUB	1A	:	3A	Z	5A	z	7A
ESC	1B	;	3B	[5B	{	7B
FS	1C	<	3C	\	5C		7C
GS	1D	=	3D]	5D	}	7D
RS	1E	>	3E	^	5E	~	7E
US	1F	?	3F	=	5F	DEL	7F

6.2 EBCDIC Character Codes

The table shows the EBCDIC characters and their hexadecimal values.

EBCDIC	HEX	EBCDIC	HEX	EBCDIC	HEX	EBCDIC	HEX
NUL	00	SP	40		80		C0
SOH	01		41	a	81	A	C1
STX	02		42	b	82	B	C2
ETX	03		43	c	83	C	C3
	04		44	d	84	D	C4
HT	05		45	e	85	E	C5
	06		46	f	86	F	C6
DEL	07		47	g	87	G	C7
	08		48	h	88	H	C8
	09		49	i	89	I	C9
	0A		4A		8A		CA
VT	0B	.(period)	4B	{	8B		CB
FF	0C	<	4C		8C		CC
CR	0D	(4D		8D		CD
SO	0E	+	4E		8E		CE
SI	0F		4F		8F		CF
DLE	10	&	50		90		D0
DC1	11		51	j	91	J	D1
DC2	12		52	k	92	K	D2
DC3	13		53	l	93	L	D3
	14		54	m	94	M	D4
	15		55	n	95	N	D5
BS	16		56	o	96	O	D6
	17		57	p	97	P	D7
CAN	18		58	q	98	Q	D8
EM	19		59	r	99	R	D9
	1A	!	5A		9A		DA
	1B	\$	5B	}	9B		DB
	1C	*	5C		9C		DC
	1D)	5D		9D		DD
	1E	;	5E		9E		DE
	1F		5F		9F		DF

EBCDIC	HEX	EBCDIC	HEX	EBCDIC	HEX	EBCDIC	HEX
FS	20	- (minus)	60	~ (tilde)	A0	\	E0
	21	/	61		A1		E1
	22		62		A2	S	E2
	23		63		A3	T	E3
LF	24		64	u	A4	U	E4
	25		65	v	A5	V	E5
	26		66	w	A6	W	E6
	27		67	x	A7	X	E7
	28		68	y	A8	Y	E8
	29		69	z	A9	Z	E9
	2A		6A		AA		EA
	2B	,(comma)	6B		AB		EB
ENQ	2C	%	6C	[AC		EC
	2D	_(underscore)	6D		AD		ED
	2E	>	6E		AE		EE
	2F	?	6F		AF		EF
SYN	30		70		B0	0	F0
	31		71		B1	1	F1
	32		72		B2	2	F2
	33		73		B3	3	F3
EOT	34		74		B4	4	F4
	35		75		B5	5	F5
	36		76		B6	6	F6
	37		77		B7	7	F7
	38		78		B8	8	F8
	39	`(grave)	79		B9	9	F9
	3A	:	7A		BA		FA
	3B	#	7B		BB		FB
DC4	3C	@	7C]	BC		FC
	3D	'	7D		BD		FD
	3E	=	7E		BE		FE
	3F	"	7F		BF		FF

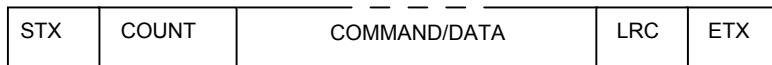
7 TRANSPARENT ASYNCHRONOUS COMMUNICATIONS

In the standard asynchronous mode of communication, codes like STX (X'02) and ETX (X'03) have a special meaning, but they can sometimes occur in a stream of binary data, where that special meaning does not apply.

To avoid ambiguity, Transparent Asynchronous Communications mode is used.

7.1 Message Format

The Host port of the HSM must be configured for Transparent Async Communications and 8-bit data transfers. The message format for Transparent Async Communications is:



Where:

- STX is the Start of Text character (X'02).
- COUNT is a two-byte hexadecimal value in the range X'0003 to X'03FB inclusive, representing the number of bytes in the COMMAND/DATA field. The count excludes the STX, COUNT, LRC and the ETX.
- LRC is a single-byte Longitudinal Redundancy Check character. It is calculated by performing an exclusive-OR on each byte of the data sent over the communications link excluding the STX, COUNT, LRC and the ETX.
- ETX is the End of Text character (X'03).

7.2 HSM Processing of Packets

When the HSM receives a Transparent Async packet it:

- Checks the LRC value with that computed over the input data and returns a response message with Error 91 if a match is not obtained.
- Checks that the Count value is between limits. If this check fails, the HSM responds in one of two ways:

If Count > X'03FB,

it returns a response message with Error 92;

otherwise it responds with the following error message:

Message Header : 0000
Response Code : ZZ
Error Code : 92

e.g., for Message Header length 4, the response is 0000ZZ92.

- Checks that the number of characters received between the Count characters and the LRC matches the value in Count. If this check fails, it returns a response message with Error 92.
- If no errors are discovered in the Transparent Async packet, the HSM processes the command and responds accordingly.

If the HSM discovers both errors (Error 91 and Error 92), it reports Error 92.

7.3 Parity Errors

If the HSM reports Error 90 there is a Data Parity Error. Check the HSM Host port settings using the QH Console command and ensure that the correct parity is in use.

8 INPUT/OUTPUT FLOW CONTROL

There is no flow control provided by the HSM. It is the responsibility of the application to ensure that the input buffer in the HSM, which is 2048 bytes long, is not exceeded. The buffer in the HSM used in an SNA-SDLC environment is 1024 bytes long.

No single command contains more than 2048 bytes (1024 for SNA-SDLC), including any STX and ETX characters. The Async connected HSM operates in half duplex the response to a command must be received before a new command request is sent.

9 ERROR HANDLING

There are four types of errors generated by the HSM:

- Fatal errors.
- Non-recoverable errors.
- Recoverable errors.
- Programming errors.

Fatal errors indicate a hardware fault in the equipment. Such an error should be logged and reported for user action to be taken (e.g., report to supervisor). Fatal errors are usually reported on the console and are not seen by the host application. The host application usually times out if a fatal error occurs.

Non-recoverable errors cannot be rectified by the program and need user intervention (e.g., with the HSM set into the Authorised state). Such errors should also be logged and reported for user action to be taken (e.g., report to supervisor). This type of error does not mean that the HSM cannot action other types of commands.

Recoverable errors may be the result of data corruption or indicate that the HSM cannot process a command because some other action is required first. The application should attempt to recover by re-issuing the command, attempting to clear the corruption or by implementing the missing action (e.g., the HSM reports that the print format definition is not loaded, so the program should load it and re-issue the failed command).

Programming errors are normally found during testing, but if they occur at other times, they are probably non-recoverable.

Additionally the application should monitor the HSM for timeouts on the interface.

In any of the above events, the application should try to continue processing by using another HSM to action the command. Continued failure may indicate a catastrophic failure of all HSMs (unlikely), a power failure or a program error.

The application should monitor usage of all HSMs and mark any unit as "out of service" if it has given a fatal error, or where a unit repeatedly reports non-recoverable errors.

10 USE OF MULTIPLE HSMS

A typical system has two or more HSMs connected as 'live' units. This provides increased capability where the processing requires more than one HSM, and provision for backup in the event of an HSM failure.

Each HSM is normally connected to the Host via a separate Host port, although a port-sharing unit can be used if the number of Host ports available is limited. The sharing configuration is not capable of providing backup if the port or the port-sharing unit becomes faulty.

Optionally it is possible to have a backup unit not connected to the Host but ready for connection in place of a faulty unit. This is not the preferred practice because the unit may remain idle for a long time and may itself have developed a fault.

In addition to the 'live' units, a typical system contains at least one HSM connected to a test or development computer system. This allows changes in the environment to be tested, without disturbing the live system.

11 USER STORAGE

The HSM areas of memory allocated to store data for use during processing. This facility allows commonly-used data to be held within the HSM, and not transmitted with each command that requires it. This reduces communications time and thus increases throughput.

User storage is erased when:

- The HSM is opened.
- It (the storage) is used for processing PIN solicitation data.
- The HSM diagnostics function is issued from the Console.
- Power is turned off.
- The HSM is reset by the use of the RESET button.

The application should reload user storage if the HSM reports that the user storage has been erased, or there is a key parity error.

User data is stored in 8-byte blocks, each block containing 16 hexadecimal digits. The size of key to store in the user storage area is configured using the Configure Security (CS) command. The user storage is indexed with reference to the key size. If keys of shorter lengths or decimalization tables are to be loaded they should be padded with F to the key length configured, i.e. filling the index location.

The memory available is shown in the following table:

	Standard speed HSM	High speed HSM
Memory	8192	98304
Maximum index		
Single length keys	1024 (3FF)	4096 (FFF)
Double length keys	512 (1FF)	4096 (FFF)
Triple length keys	341 (154)	4096 (FFF)

The amount of available user storage defined is for the standard HSM base firmware, currently at release 6.0/2.0, and may not be representative of a unit using customised firmware. User storage must be reloaded on power up or when coming on-line from an off-line state.

11.1 Assigning and Using Indices

To load user data, provide an index which points to a particular memory location. A valid index is expressed as 3 hexadecimal digits, and must be within the range X'000 to X'FFF.

An index points to a key block this varies in length depending on the key length specified in the Configure Security command. For example, if loading two encrypted working keys and specifying X'000 as the base index, the first encrypted key is stored in bytes 0-7; the second encrypted key is stored in bytes 8-15.

	Single Length			Double Length			Triple Length	
	Byte 0	Byte 7	Byte 8	Byte 15	Byte 16	Byte 23		
Location 000								
Location 001								
Location 154								
Location 155							Byte 8184	Byte 8191
Location 1FE								
Location 1FF				Byte 8184	Byte 8191			
Location 3FE								
Location 3FF	Byte 8184		Byte 8191					
Location FFE								
Location FFF								Byte 98303

Data can be stored in continuous bytes, or in discrete areas of memory. The only requirement for index assignment applies to storage of the Diebold table. This table must be stored as 256 contiguous bytes. Thus, X'3E0 is the highest possible base index that can be specified when the Diebold table is loaded or accessed.

It is the programmer's responsibility to assign and keep track of the indices. When an index is provided to load new data, the HSM does not check the memory location to determine if it already contains data. If the wrong index is provided, the data overwrites the previous contents. For example, if X'000 is specified as the base index when loading the Diebold table, and the same index is then used to load an encrypted key, the table is invalidated.

11.2 Specifying Stored Data

To use the keys or other data in user memory, the HSM must have the index that points to the appropriate storage location. The Host provides this index in place of the encrypted key (or other data element) that would otherwise be required.

To indicate the substitution of an index for a data element, the data element in the transaction must begin with the index flag K, followed by the 3-digit index value. These four characters replace the key (or other data elements). A key of appropriate length will be extracted based upon the key scheme and the key length expected by the command. The exception is if the HSM is configured for single length keys and the command expects a double length key (32H) for backwards compatibility the command will require two indices to be specified.

If the triple DES key schemes are used a number of scenarios exist:

1. All key lengths used – configure for either single or triple length keys.
2. Single and double length keys used - configure for either single or double length keys.
3. Single and triple length keys used - configure for either single or triple length keys.
4. Double length keys used - configure for either single or double length keys.
5. Triple length keys used - configure for either single or triple length keys.

Example 1:

To supply a single length key to a command there is no key scheme and a single index. - K000

To supply a double length key to a command using the U scheme, the key scheme and a single index must be provided. - UK000

To supply a triple length key to a command using the T scheme, the key scheme and the index must be provided. - TK000

If the HSM is configured for single length keys an index will return a single length key if no key scheme is specified or an appropriate key if a key scheme is supplied.

Example 2:

To supply a single length key to a command there is no key scheme and a single index. - K000

To supply a double length key (32H) to a command there is no key scheme and two indices must be provided. - UK000

To supply a triple length key to a command the key scheme and a single index must be provided. - TK000

12 PRINTING TO AN HSM-ATTACHED PRINTER

A printer is connected to the HSM, then the Host instructs the HSM to print (when required, e.g. to print PINs to be sent to customers of a bank). The stationery should be of the multicopy type which allows information to be read only after the stationery has been opened.

The HSM must also be in the Authorised state; if it is not, an error is returned. To enable the HSM to format the data before sending it to the printer, the HSM must be given formatting details by the Host. The HSM retains this information until new details are provided or until:

- The HSM is opened (when armed).
- The HSM diagnostics function is issued from the Console.
- Power is turned off.
- The HSM is reset by the use of the RESET button.

When the printer is connected, the HSM is in the Authorised state, and the formatting data has been provided, the following sequence occurs:

- The Host sends a print command with encrypted data to the HSM.
- The HSM verifies the data and sends a response message to the Host. If there is an error in the data, the next step does not occur.
- The HSM formats the data and outputs it to the printer. On completion, the HSM sends a second response message to the Host indicating that the printing is complete and the next print command can be sent.

13 REJECTION OF WEAK AND SEMI-WEAK KEYS

All HSM commands that generate keys ensure that the standard DES weak or semi-weak keys can not be used. If the new key matches one of the listed weak or semi-weak keys it is rejected and the key generation process is repeated.

DES Weak Keys

0101	0101	0101	0101
FEFE	FEFE	FEFE	FEFE
1F1F	1F1F	0E0E	0E0E
E0E0	E0E0	F1F1	F1F1

DES Semi-Weak Keys

01FE	01FE	01FE	01FE
FE01	FE01	FE01	FE01
1FE0	1FE0	0EF1	0EF1
E01F	E01F	F10E	F10E
01E0	01E0	01F1	01F1
E001	E001	F101	F101
1FFE	1FFE	0EFE	0EFE
FE1F	FE1F	FE0E	FE0E
011F	011F	010E	010E
1F01	1F01	0E01	0E01
E0FE	E0FE	F1FE	F1FE
FEE0	FEE0	FEF1	FEF1

14 LOCAL MASTER KEYS

The HSM Local Master Keys (LMKs) are numbered from key 00 to key 99. They are used in pairs and each pair has a function, as shown in the table.

LMK Pair	Function
00 - 01	Contains the two Smart Card "keys" (Passwords if the HSM is configured for Password mode) required for setting the HSM into the Authorized state.
02 - 03	Encrypts the PINs for Host storage.
04 - 05	Encrypts Zone Master Keys and double-length ZMKs. Encrypts Zone Master Key components under a Variant.
06 - 07	Encrypts the Zone PIN keys for interchange transactions.
08 - 09	Used for random number generation.
10 - 11	Used for encrypting keys in HSM buffer areas.
12 - 13	The initial set of Secret Values created by the user; used for generating all other Master Key pairs.
14 - 15	Encrypts Terminal Master Keys, Terminal PIN Keys, and PIN Verification Keys. Encrypts Card Verification Keys under a Variant.
16 - 17	Encrypts Terminal Authentication Keys.
18 - 19	Encrypts reference numbers for solicitation mailers.
20 - 21	Encrypts 'not on us' PIN Verification Keys and Card Verification Keys under a Variant.
22 - 23	Encrypts Watchword Keys.
24 - 25	Encrypts Zone Transport Keys.
26 - 27	Encrypts Zone Authentication Keys.
28 - 29	Encrypts Terminal Derivation Keys.
30 - 31	Encrypts Zone Encryption Keys.
32 - 33	Encrypts Terminal Encryption Keys.
34 - 35	Encrypts RSA Keys.
36 - 99	Reserved for future use.
There are Variants of some keys to suit particular requirements.	

LMK Pair	Standard Test LMK Set							
00-01	0101	0101	0101	0101	7902	CD1F	D36E	F8BA
02-03	2020	2020	2020	2020	3131	3131	3131	3131
04-05	4040	4040	4040	4040	5151	5151	5151	5151
06-07	6161	6161	6161	6161	7070	7070	7070	7070
08-09	8080	8080	8080	8080	9191	9191	9191	9191
10-11	A1A1	A1A1	A1A1	A1A1	B0B0	B0B0	B0B0	B0B0
12-13	C1C1	0101	0101	0101	D0D0	0101	0101	0101
14-15	E0E0	0101	0101	0101	F1F1	0101	0101	0101
16-17	1C58	7F1C	1392	4FEF	0101	0101	0101	0101
18-19	0101	0101	0101	0101	0101	0101	0101	0101
20-21	0202	0202	0202	0202	0404	0404	0404	0404
22-23	0707	0707	0707	0707	1010	1010	1010	1010
24-25	1313	1313	1313	1313	1515	1515	1515	1515
26-27	1616	1616	1616	1616	1919	1919	1919	1919
28-29	1A1A	1A1A	1A1A	1A1A	1C1C	1C1C	1C1C	1C1C
30-31	2323	2323	2323	2323	2525	2525	2525	2525
32-33	2626	2626	2626	2626	2929	2929	2929	2929
34-35	2A2A	2A2A	2A2A	2A2A	2C2C	2C2C	2C2C	2C2C
36-37	2F2F	2F2F	2F2F	2F2F	3131	3131	3131	3131
38-39	0101	0101	0101	0101	0101	0101	0101	0101
Password 1 = 0101 0101 0101 0101 Password 2 = NOW IS THE TIME FOR A								

The check value is 2686 0474 4491 2422.

15 LOCAL MASTER KEY VARIANTS

Variants of the Local Master Key in the HSM are used for encryption of defined keys or key components. These variants are calculated as follows:

1. Select the appropriate LMK pair, for example:

0123 4567 89AB CDEF 3131 3131 3131 3131.

2. Identify which Variant of the LMK is required and select the appropriate offset value:

Variant 2: 5A.

3. Exclusive-OR add the selected offset to the first byte of the LMK pair (01 in the example above).

4. Replace the left-most byte of the LMK pair with the result of Step 3 and use the resulting key as the specified Variant:

Variant 2 = 5B23 4567 89AB CDEF 3131 3131 3131 3131.

The variants are:

Variant 1 : A6
Variant 2 : 5A
Variant 3 : 6A
Variant 4 : DE
Variant 5 : 2B
Variant 6 : 50
Variant 7 : 74
Variant 8 : 9C

When the Variants are applied to the standard test LMK set, the left-most bytes of the sets are as follows:

LMK Pair	First byte of LMK							
	1	2	3	4	5	6	7	8
00-01	A7	5B	6B	DF	2A	51	75	9D
02-03	86	7A	4A	FE	0B	70	54	BC
04-05	E6	1A	2A	9E	6B	10	34	DC
06-07	C7	3B	0B	BF	4A	31	15	FD
08-09	26	DA	EA	5E	AB	D0	F4	1C
10-11	07	FB	CB	7F	8A	F1	D5	3D
12-13	67	9B	AB	1F	EA	91	B5	5D
14-15	46	BA	8A	3E	CB	B0	94	7C
16-17	BA	46	76	C2	37	4C	68	80
18-19	A7	5B	6B	DF	2A	51	75	9D
20-21	A4	58	68	DC	29	52	76	9E
22-23	A1	5D	6D	D9	2C	57	73	9B
24-25	B5	49	79	CD	38	43	67	8F
26-27	B0	4C	7C	C8	3D	46	62	8A
28-29	BC	40	70	C4	31	4A	6E	86
30-31	85	79	49	FD	08	73	57	BF
32-33	80	7C	4C	F8	0D	76	52	BA
34-35	8C	70	40	F4	01	7A	5E	B6
36-37	89	75	45	F1	04	7F	5B	B3
38-39	A7	5B	6B	DF	2A	51	75	9D

16 LOCAL MASTER KEY TRIPLE DES VARIANT SCHEME

Variants are applied to the Local Master Key in the HSM for encryption of double and triple length keys. These variants are calculated as follows:

1. Select the appropriate LMK pair, for example:

0123 4567 89AB CDEF 3131 3131 3131 3131.

2. Identify which Variant of the LMK is required and select the appropriate offset value:

Variant 2: A6.

3. Exclusive-OR add the selected offset to the first byte of the second key within the LMK pair (31 in the example above).

4. Replace the left-most byte of the LMK pair with the result of Step 3 and use the resulting key as the specified Variant:

Variant 2 = 0123 4567 89AB CDEF 9731 3131 3131 3131.

The variants applied are as follows:

Double length key	Key 1 of 2 – A6
	Key 2 of 2 – 5A
Triple length key	Key 1 of 3 – 6A
	Key 2 of 3 – DE
	Key 3 of 3 – 2B

When the Variants are applied to the standard test LMK set, the first bytes of the second key are as follows:

LMK Pair	First byte of second key of the LMK					
	Double length Key		Triple Length Key			
	Scheme Tag “U”		Scheme Tag “T”			
	1 of 2	2 of 2	1 of 3	2 of 3	3 of 3	
04 - 05	F7	0B	3B	8F	7A	
06 - 07	D6	2A	1A	AE	5B	
14 - 15	57	AB	9B	2F	DA	
16 - 17	A7	5B	6B	DF	2A	
18 - 19	A7	5B	6B	DF	2A	
20 - 21	A2	5E	6E	DA	2F	
22 - 23	B6	4A	7A	CE	3B	
24 - 25	B3	4F	7F	CB	3E	
26 - 27	BF	43	73	C7	32	
28 - 29	BA	46	76	C2	37	
30 - 31	83	7F	4C	FB	0E	
32 - 33	8F	73	43	F7	02	
34 - 35	8A	76	46	F2	07	
35 - 37	97	6B	5B	EF	1A	
38 - 39	A7	5B	6B	DF	2A	

CHAPTER 2

HOST COMMANDS

CONTENTS

Page

1	GENERAL	2-1
2	HOST COMMANDS	2-2
2.1	LIST OF HOST COMMANDS (ALPHABETICAL)	2-2
2.2	LIST OF HOST COMMANDS (FUNCTIONAL)	2-6
3	GENERIC KEY MANAGEMENT COMMANDS	2-12
3.1	KEY TYPE TABLE	2-12
3.2	KEY SCHEME TABLE	2-13
3.3	GENERATE A KEY	2-14
3.4	GENERATE AND PRINT A COMPONENT	2-15
3.5	GENERATE AND PRINT A KEY AS SPLIT COMPONENTS	2-17
3.6	FORM A KEY FROM ENCRYPTED COMPONENTS	2-19
3.7	IMPORT A KEY	2-20
3.8	EXPORT A KEY	2-21
3.9	TRANSLATE KEY SCHEME	2-22
4	ZONE MASTER KEY MANAGEMENT	2-23
4.1	GENERATE AND PRINT A ZMK COMPONENT	2-23
4.2	FORM A ZMK FROM THREE ZMK COMPONENTS	2-25
4.3	FORM A ZMK FROM 2 TO 9 ZMK COMPONENTS	2-26
4.4	TRANSLATE ZMK FROM ZMK TO LMK ENCRYPTION	2-28
5	ZONE PIN KEY MANAGEMENT	2-30
5.1	GENERATE A ZPK	2-31
5.2	TRANSLATE A ZPK FROM ZMK TO LMK ENCRYPTION	2-32
5.3	TRANSLATE A ZPK FROM LMK TO ZMK ENCRYPTION	2-34
6	ZONE ENCRYPTION, ZONE AUTHENTICATION KEY MANAGEMENT	2-35
6.1	GENERATE ZEK/ZAK	2-36
6.2	TRANSLATE A ZEK/ZAK FROM ZMK TO LMK ENCRYPTION	2-37
6.3	TRANSLATE A ZEK/ZAK FROM LMK TO ZMK ENCRYPTION	2-38
7	TERMINAL MASTER, TERMINAL PIN AND PIN VERIFICATION KEY MANAGEMENT	2-39
7.1	GENERATE AND PRINT A TMK, TPK OR PVK	2-40
7.2	GENERATE A TMK, TPK OR PVK	2-42
7.3	TRANSLATE A TMK, TPK OR PVK FROM LMK TO ANOTHER TMK, TPK OR PVK	2-43
7.4	TRANSLATE A TMK, TPK OR PVK FROM ZMK TO LMK ENCRYPTION	2-44
7.5	TRANSLATE A TMK, TPK OR PVK FROM LMK TO ZMK ENCRYPTION	2-45
7.6	GENERATE A PAIR OF PVKS	2-47
8	TERMINAL AUTHENTICATION KEY MANAGEMENT	2-49
8.1	GENERATE A TAK	2-50
8.2	TRANSLATE A TAK FROM ZMK TO LMK ENCRYPTION	2-51
8.3	TRANSLATE A TAK FROM LMK TO ZMK ENCRYPTION	2-52

8.4	TRANSLATE A TAK FROM LMK TO TMK ENCRYPTION	2-53
9	PIN AND OFFSET GENERATION	2-54
9.1	DERIVE A PIN USING THE IBM METHOD	2-55
9.2	DERIVE A PIN USING THE DIEBOLD METHOD	2-57
9.3	GENERATE A RANDOM PIN	2-58
9.4	GENERATE AN IBM PIN OFFSET	2-59
9.5	GENERATE A DIEBOLD PIN OFFSET	2-60
9.6	GENERATE A VISA PIN VERIFICATION VALUE	2-61
10	PIN VERIFICATION	2-62
10.1	VERIFY A TERMINAL PIN USING THE IBM METHOD	2-62
10.2	VERIFY AN INTERCHANGE PIN USING THE IBM METHOD	2-64
10.3	VERIFY A TERMINAL PIN USING THE DIEBOLD METHOD	2-66
10.4	VERIFY AN INTERCHANGE PIN USING THE DIEBOLD METHOD	2-67
10.5	VERIFY A TERMINAL PIN USING THE VISA METHOD	2-68
10.6	VERIFY AN INTERCHANGE PIN USING THE VISA METHOD	2-69
10.7	VERIFY A TERMINAL PIN USING THE COMPARISON METHOD	2-70
10.8	VERIFY AN INTERCHANGE PIN USING THE COMPARISON METHOD	2-71
11	PIN TRANSLATION	2-72
11.1	TRANSLATE A PIN FROM ONE ZPK TO ANOTHER	2-73
11.2	TRANSLATE A PIN FROM TPK TO ZPK ENCRYPTION	2-75
11.3	TRANSLATE A PIN FROM ZPK TO LMK ENCRYPTION	2-76
11.4	TRANSLATE A PIN FROM TPK TO LMK ENCRYPTION	2-77
11.5	TRANSLATE A PIN FROM LMK TO ZPK ENCRYPTION	2-78
11.6	TRANSLATE PIN ALGORITHM	2-79
12	PIN MAILER PRINTING	2-80
12.1	PRINT PIN/PIN AND SOLICITATION DATA	2-81
12.2	PRINT A PIN SOLICITATION MAILER	2-83
12.3	VERIFY PIN/PIN AND SOLICITATION MAILER CRYPTOGRAPHY	2-85
12.4	VERIFY SOLICITATION MAILER CRYPTOGRAPHY	2-86
13	PIN SOLICITATION DATA PROCESSING	2-87
13.1	LOAD SOLICITATION DATA TO USER STORAGE	2-90
13.2	FINAL LOAD OF SOLICITATION DATA TO USER STORAGE	2-91
14	CLEAR PIN SUPPORT	2-93
14.1	ENCRYPT A CLEAR PIN	2-93
14.2	DECRYPT AN ENCRYPTED PIN	2-94
15	HOST WATCHWORD SUPPORT	2-95
15.1	GENERATE A WATCHWORD KEY	2-95
15.2	TRANSLATE A WATCHWORD KEY FROM LMK TO ZMK ENCRYPTION	2-96
15.3	TRANSLATE A WATCHWORD KEY FROM ZMK TO LMK ENCRYPTION	2-97
15.4	VERIFY A WATCHWORD RESPONSE	2-98
15.5	GENERATE A DECIMAL MAC	2-99
15.6	VERIFY A DECIMAL MAC	2-100
16	MESSAGE AUTHENTICATION CODE SUPPORT	2-101
16.1	GENERATE A MAC	2-103
16.2	VERIFY A MAC	2-104
16.3	VERIFY AND TRANSLATE A MAC	2-105
16.4	GENERATE MAC (MAB) FOR LARGE MESSAGE	2-106

16.5	GENERATE MAC (MAB) USING ANSI X9.19 METHOD FOR A LARGE MESSAGE	2-108
17	BASE24 BINARY MAC COMMANDS	2-110
17.1	GENERATE A BINARY MAC (BASE24)	2-110
17.2	VERIFY A BINARY MAC (BASE24)	2-112
17.3	VERIFY AND TRANSLATE A BINARY MAC (BASE24)	2-113
18	USER STORAGE SUPPORT	2-114
18.1	LOAD DATA TO USER STORAGE	2-114
18.2	READ DATA FROM USER STORAGE	2-115
18.3	VERIFY THE DIEBOLD TABLE IN USER STORAGE	2-116
19	PRINT OUTPUT FORMATTING	2-117
19.1	PRINTING PINS IN WORD FORMAT	2-120
19.2	PRINTING PINS IN COLUMNS	2-121
19.3	LOAD FORMATTING DATA TO HSM	2-122
19.4	LOAD ADDITIONAL FORMATTING DATA TO HSM	2-123
19.5	LOAD A PIN TEXT STRING	2-124
20	TRANSLATE DATA AFTER CHANGE OF LOCAL MASTER KEYS	2-125
20.1	TRANSLATE A ZMK	2-125
20.2	TRANSLATE A ZPK	2-126
20.3	TRANSLATE A TMK, TPK OR PVK	2-127
20.4	TRANSLATE A TAK	2-128
20.5	TRANSLATE A PIN AND PIN LENGTH	2-129
20.6	TRANSLATE KEYS FROM OLD LMK TO NEW LMK	2-130
20.7	ERASE THE KEY CHANGE STORAGE	2-132
21	MISCELLANEOUS COMMANDS	2-133
21.1	CANCEL THE AUTHORISED STATE	2-133
21.2	GENERATE A KEY CHECK VALUE (NOT DOUBLE-LENGTH ZMK)	2-134
21.3	GENERATE A KEY CHECK VALUE	2-135
21.4	SET HSM RESPONSE DELAY	2-137
21.5	PERFORM DIAGNOSTICS	2-138
21.6	HSM STATUS	2-139
22	VISA CARD VERIFICATION VALUES	2-140
22.1	GENERATE A CVK PAIR	2-140
22.2	TRANSLATE A CVK PAIR FROM LMK TO ZMK ENCRYPTION	2-141
22.3	TRANSLATE A CVK PAIR FROM ZMK TO LMK ENCRYPTION	2-142
22.4	TRANSLATE A CVK PAIR FROM OLD LMK TO NEW LMK ENCRYPTION	2-143
22.5	GENERATE A VISA CVV	2-144
22.6	VERIFY A VISA CVV	2-145
23	VISA CASH SYSTEM	2-146
23.1	GENERATE AND EXPORT A *KML	2-147
23.2	IMPORT A *KML	2-148
23.3	VERIFY LOAD SIGNATURE S ₁ AND GENERATE LOAD SIGNATURE S ₂	2-149
23.4	VERIFY LOAD COMPLETION SIGNATURE S ₃	2-150
23.5	VERIFY UNLOAD SIGNATURE S ₁ AND GENERATE UNLOAD SIGNATURE S ₂	2-151
23.6	VERIFY UNLOAD COMPLETION SIGNATURE S ₃	2-152
24	CHIP CARD	2-153
24.1	ARQC (OR TC/AAC) VERIFICATION AND/OR ARPC GENERATION	2-154
24.2	DATA AUTHENTICATION CODE AND DYNAMIC NUMBER VERIFICATION	2-156

24.3 GENERATE SECURE MESSAGE WITH INTEGRITY AND OPTIONAL CONFIDENTIALITY AND PIN CHANGE	2-157
25 AMERICAN EXPRESS CARD SECURITY CODE	2-160
25.1 GENERATE A *CSCK	2-160
25.2 EXPORT A *CSCK	2-161
25.3 IMPORT A *CSCK	2-162
25.4 CALCULATE CARD SECURITY CODES	2-164
25.5 VERIFY CARD SECURITY CODES	2-165
26 RACAL TRANSACTION KEY SCHEME (RTKS)	2-166
26.1 TRANSACTION REQUEST WITH A PIN (T/AQ KEY)	2-168
26.2 TRANSACTION REQUEST WITHOUT A PIN	2-170
26.3 TRANSACTION REQUEST WITH A PIN (T/CI KEY)	2-172
26.4 TRANSLATE KEYVAL	2-174
26.5 ADMINISTRATION REQUEST MESSAGE	2-175
26.6 TRANSACTION RESPONSE WITH AUTH PARA FROM CARD ISSUER	2-177
26.7 GENERATE AUTH PARA AND TRANSACTION RESPONSE	2-179
26.8 CONFIRMATION	2-181
27 DERIVED UNIQUE KEY PER TRANSACTION (DUKPT) SYSTEM	2-183
27.1 GENERATE AN BASE DERIVATION KEY (*BDK)	2-184
27.2 TRANSLATE A PIN FROM *BDK ENCRYPTION TO INTERCHANGE KEY ENCRYPTION	2-185
27.3 VERIFY A PIN USING THE IBM METHOD	2-186
27.4 VERIFY A PIN USING THE VISA PVV METHOD	2-187
27.5 VERIFY A PIN USING THE DIEBOLD METHOD	2-188
27.6 VERIFY A PIN USING THE ENCRYPTED PIN METHOD	2-189
27.7 TRANSLATE A BASE DERIVATION KEY FROM *ZMK TO LMK ENCRYPTION	2-190
27.8 TRANSLATE A BASE DERIVATION KEY FROM LMK TO *ZMK ENCRYPTION	2-191
28 AUSTRALIAN TRANSACTION KEY SCHEME (ATKS)	2-192
28.1 TRANSACTION REQUEST WITHOUT A PIN	2-193
28.2 TRANSACTION REQUEST WITH A PIN (T/AQ KEY)	2-195
28.3 TRANSACTION REQUEST WITH A PIN (T/CI KEY)	2-197
28.4 TRANSACTION RESPONSE WITH AUTH PARA GENERATED BY THE ACQUIRER	2-199
28.5 TRANSACTION RESPONSE WITH AUTH PARA GENERATED BY THE CARD ISSUER	2-201
28.6 TRANSLATE A PIN FROM PEK TO ZPK ENCRYPTION	2-203
28.7 VERIFY A TRANSACTION COMPLETION CONFIRMATION REQUEST	2-204
28.8 GENERATE A TRANSACTION COMPLETION RESPONSE	2-206
28.9 VERIFY A PIN AT THE CARD ISSUER USING THE IBM METHOD	2-208
28.10 VERIFY A PIN AT THE CARD ISSUER USING THE DIEBOLD METHOD	2-210
28.11 VERIFY A PIN AT THE CARD ISSUER USING THE VISA METHOD	2-212
28.12 VERIFY A PIN AT THE CARD ISSUER BY COMPARISON	2-214
28.13 GENERATE AUTH PARA AT THE CARD ISSUER	2-216
28.14 MESSAGE AUTHENTICATION MODE NUMBERS	2-217
28.15 GENERATE A MAC ON A BINARY MESSAGE	2-218
28.16 VERIFY A MAC ON A BINARY MESSAGE	2-220
29 USING THE OPTIONAL RSA CRYPTOSYSTEM	2-222
29.1 GENERATE AN RSA KEY SET	2-229
29.2 LOAD A SECRET KEY	2-231
29.3 TRANSLATE A SECRET KEY FROM THE OLD LMK TO A NEW LMK	2-232
29.4 GENERATE A MAC ON A PUBLIC KEY	2-233

29.5	VERIFY A MAC ON A PUBLIC KEY	2-234
29.6	VALIDATE A CERTIFICATE AND GENERATE A MAC ON ITS PUBLIC KEY	2-235
29.7	TRANSLATE A MAC ON A PUBLIC KEY	2-238
29.8	GENERATE A SIGNATURE	2-239
29.9	VALIDATE A SIGNATURE	2-241
29.10	IMPORT A DES KEY	2-243
29.11	EXPORT A DES KEY	2-246
29.12	HASH A BLOCK OF DATA	2-249

1 GENERAL

The HSM provides a variety of functions to implement key management, PIN management (including PIN verification) and Message Authentication Code (MAC) processing.

This Chapter details all the commands available with their responses and possible error codes. A number of abbreviations are used throughout. They are:

L	:	Encrypted PIN length. Set at installation.
m	:	Message header length. Set at installation.
n	:	Variable length field.
A	:	Alphanumeric (can include any non-control type) characters.
H	:	Hexadecimal character.
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 that the Host must send the number of alphanumeric characters that has been set for the message header length.

For convenience, the STX and ETX control characters, which bracket every command and response, are not shown in the details that follow.

In a command to the HSM, any key can be replaced by a reference to internal user storage. In the details that follow, a key is always shown as if it is to be sent with each command; in every case the key can be replaced by the index flag K and a three-digit pointer value.

The HSM 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 HSM can support 1 or 2 digit Atalla variants.

2 HOST COMMANDS

2.1 LIST OF HOST COMMANDS (ALPHABETICAL)

Host Command (Response)	Function	Paragraph	Page
A0 (A1)	Generate a Key	3.3	14
A2 (A3)	Generate and Print a Component	3.4	15
A4 (A5)	Form a Key from Encrypted Components	3.6	19
A6 (A7)	Import a Key	3.7	20
A8 (A9)	Export a Key	3.8	21
AA (AB)	Translate a TMK, TPK or PVK	20.3	127
AC (AD)	Translate a TAK	20.4	128
AE (AF)	Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK	7.3	43
AG (AH)	Translate a TAK from LMK to ZMK Encryption	8.4	53
AS (AT)	Generate a CVK Pair	22.1	140
AU (AV)	Translate a CVK Pair from LMK to ZMK Encryption	22.2	141
AW (AX)	Translate a CVK Pair from ZMK to LMK Encryption	22.3	142
AY (AZ)	Translate a CVK Pair from Old LMK to New LMK Encryption	22.4	143
B0 (B1)	Translate Key Scheme	3.9	22
BA (BB)	Encrypt a Clear PIN	14.1	93
BC (BD)	Verify a Terminal PIN Using the Comparison Method	10.7	70
BE (BF)	Verify an Interchange PIN Using the Comparison Method	10.8	71
BG (BH)	Translate a PIN and PIN Length	20.5	129
BI (BJ)	Generate an Base Derivation Key (*BDK)	27.1	184
BQ (BR)	Translate PIN Algorithm	11.6	79
BS (BT)	Erase the Key Change Storage	20.7	132
BU (BV)	Generate a Key Check Value	21.3	135
BW (BX)	Translate Keys from Old LMK to New LMK	20.6	130
BY (BZ)	Translate ZMK from ZMK to LMK encryption	4.4	28
CA (CB)	Translate a PIN from TPK to ZPK Encryption	11.2	75
CC (CD)	Translate a PIN from One ZPK to Another	11.1	73
CE (CF)	Generate a Diebold PIN Offset	9.5	60
CG (CH)	Verify a Terminal PIN Using the Diebold Method	10.3	66
CI (CJ)	Translate a PIN from *BDK Encryption to Interchange Key Encryption	27.2	185
CK (CL)	Verify a PIN Using the IBM Method	27.3	186
CM (CN)	Verify a PIN Using the VISA PVV Method	27.4	187
CO (CP)	Verify a PIN Using the Diebold Method	27.5	188
CQ (CR)	Verify a PIN Using the Encrypted PIN Method	27.6	189
CW (CX)	Generate a VISA CVV	22.5	144
CY (CZ)	Verify a VISA CVV	22.6	145
DA (DB)	Verify a Terminal PIN Using the IBM Method	10.1	62
DC (DD)	Verify a Terminal PIN Using the VISA Method	10.5	68

Host Command (Response)	Function	Paragraph	Page
DE (DF)	Generate an IBM PIN Offset	9.4	59
DG (DH)	Generate a VISA PIN Verification Value	9.6	61
DI (DJ)	Generate and Export a *KML	23.1	147
DK (DL)	Import a *KML	23.2	148
DM (DN)	Verify Load Signature S1 and Generate Load Signature S2	23.3	149
DO (DP)	Verify Load Completion Signature S3	23.4	150
DQ (DR)	Verify Unload Signature S1 and Generate Unload Signature S2	23.5	151
DS (DT)	Verify Unload Completion Signature S3	23.6	152
DW (DX)	Translate a Base Derivation Key from *ZMK to LMK Encryption	27.7	190
DY (DZ)	Translate a Base Derivation Key from LMK to *ZMK Encryption	27.8	191
EA (EB)	Verify an Interchange PIN Using the IBM Method	10.2	64
EC (ED)	Verify an Interchange PIN Using the VISA Method	10.6	69
EE (EF)	Derive a PIN Using the IBM Method	9.1	55
EG (EH)	Verify an Interchange PIN Using the Diebold Method	10.4	67
EI (EJ)	Generate an RSA Key Set	29.1	229
EK (EL)	Load a Secret Key	29.2	231
EM (EN)	Translate a Secret Key from the Old LMK to a New LMK	29.3	232
EO (EP)	Generate a MAC on a Public Key	29.4	233
EQ (ER)	Verify a MAC on a Public Key	29.5	234
ES (ET)	Validate a Certificate and Generate a MAC on its Public Key	29.6	235
EU (EV)	Translate a MAC on a Public Key	29.7	238
EW (EX)	Generate a Signature	29.8	239
EY (EZ)	Validate a Signature	29.9	241
FA (FB)	Translate a ZPK from ZMK to LMK Encryption	5.2	32
FC (FD)	Translate a TMK, TPK or PVK from ZMK to LMK Encryption	7.4	44
FE (FF)	Translate a TMK, TPK or PVK from LMK to ZMK Encryption	7.5	45
FG (FH)	Generate a Pair of PVKs	7.6	47
FI (FJ)	Generate ZEK/ZAK	6.1	36
FK (FL)	Translate a ZEK/ZAK from ZMK to LMK Encryption	6.2	37
FM (FN)	Translate a ZEK/ZAK from LMK to ZMK Encryption	6.3	38
FO (FP)	Generate a Watchword Key	15.1	95
FQ (FR)	Translate a Watchword Key from LMK to ZMK Encryption	15.2	96
FS (FT)	Translate a Watchword Key from ZMK to LMK Encryption	15.3	97
FU (FV)	Verify a Watchword Response	15.4	98
GA (GB)	Derive a PIN Using the Diebold Method	9.2	57
GC (GD)	Translate a ZPK from LMK to ZMK Encryption	5.3	34
GE (GF)	Translate a ZMK	20.1	125
GG (GH)	Form a ZMK from Three ZMK Components	4.2	25
GI (GJ)	Import a DES Key	29.10	243
GK (GL)	Export a DES Key	29.11	246
GM (GN)	Hash a Block of Data	29.12	249

Host Command (Response)	Function	Paragraph	Page
GY (GZ)	Form a ZMK from 2 to 9 ZMK Components	4.3	26
HA (HB)	Generate a TAK	8.1	50
HC (HD)	Generate a TMK, TPK or PVK	7.2	42
IA (IB)	Generate a ZPK	5.1	31
JA (JB)	Generate a Random PIN	9.3	58
JC (JD)	Translate a PIN from TPK to LMK Encryption	11.4	77
JE (JF)	Translate a PIN from ZPK to LMK Encryption	11.3	76
JG (JH)	Translate a PIN from LMK to ZPK Encryption	11.5	78
KA (KB)	Generate a Key Check Value (Not Double-Length ZMK)	21.2	134
KC (KD)	Translate a ZPK	20.2	126
KQ (KR)	ARQC (or TC/AAC) Verification and/or ARPC Generation	24.1	154
KS (KT)	Data Authentication Code and Dynamic Number Verification	24.2	156
KU (KV)	Generate Secure Message with Integrity and optional Confidentiality	24.3	157
LA (LB)	Load Data to User Storage	18.1	114
LC (LD)	Verify the Diebold Table in User Storage	18.3	116
LE (LF)	Read Data from User Storage	18.2	115
LG (LH)	Set HSM Response Delay	21.4	137
LI (LJ)	Load a PIN Text String	19.5	124
LK (LL)	Generate a Decimal MAC	15.5	99
LM (LN)	Verify a Decimal MAC	15.6	100
MA (MB)	Generate a MAC	16.1	103
MC (MD)	Verify a MAC	16.2	104
ME (MF)	Verify and Translate a MAC	16.3	105
MG (MH)	Translate a TAK from LMK to ZMK Encryption	8.3	52
MI (MJ)	Translate a TAK from ZMK to LMK Encryption	8.2	51
MK (ML)	Generate a Binary MAC (Base24)	17.1	110
MM (MN)	Verify a Binary MAC (Base24)	17.2	112
MO (MP)	Verify and Translate a Binary MAC (Base24)	17.3	113
MQ (MR)	Generate MAC (MAB) for Large Message	16.4	106
MS (MT)	Generate MAC (MAB) using ANSI X9.19 Method for a Large Message	16.5	108
MU (MV)	Message Authentication Mode Numbers	28.14	217
MW (MX)	Generate a MAC on a Binary Message	28.15	218
NC (ND)	Perform Diagnostics	21.5	138
NE (NF)	Generate and Print a Key as Split Components	3.5	17
NG (NH)	Decrypt an Encrypted PIN	14.2	94
NO (NP)	HSM Status	21.6	139
OA (OB) (OZ)	Print a PIN Solicitation Mailer	12.2	83
OC (OD) (OZ)	Generate and Print a ZMK Component	4.1	23
OE (OF) (OZ)	Generate and Print a TMK, TPK or PVK	7.1	40
PA (PB)	Load Formatting Data to HSM	19.3	122
PC (PD)	Load Additional Formatting Data to HSM	19.4	123

Host Command (Response)	Function	Paragraph	Page
PE (PF) (PZ)	Print PIN/PIN and Solicitation Data	12.1	81
PG (PH)	Verify PIN/PIN and Solicitation Mailer Cryptography	12.3	85
QA (QB)	Load Solicitation Data to User Storage	13.1	90
QC (QD)	Final Load of Solicitation Data to User Storage	13.2	91
QQ (QR)	Verify a PIN at the Card Issuer Using the IBM Method	28.9	208
QS (QT)	Verify a PIN at the Card Issuer Using the Diebold Method	28.10	210
QU (QV)	Verify a PIN at the Card Issuer Using the Visa Method	28.11	212
QW (QX)	Verify a PIN at the Card Issuer by Comparison	28.12	214
RA (RB)	Cancel the Authorised State	21.1	133
RC (RD)	Verify Solicitation Mailer Cryptography	12.4	86
RI (RJ)	Transaction Request With a PIN (T/AQ Key) (RTKS)	26.1	168
RK (RL)	Transaction Request Without a PIN (RTKS)	26.2	170
RM (RN)	Administration Request Message (RTKS)	26.5	175
RO (RP)	Transaction Response with Auth Para from Card Issuer (RTKS)	26.6	177
RQ (RR)	Generate Auth Para and Transaction Response (RTKS)	26.7	179
RS (RT)	Confirmation (RTKS)	26.8	181
RU (RV)	Transaction Request With a PIN (T/CI Key) (RTKS)	26.3	172
RW (RX)	Translate KEYVAL (RTKS)	26.4	174
RE (RF)	Transaction Request Without a PIN (ATKS)	28.1	193
RG (RH)	Transaction Request With a PIN (T/AQ Key) (ATKS)	28.2	195
RI (RJ)	Transaction Request With a PIN (T/CI Key) (ATKS)	28.3	197
RK (RL)	Transaction Response With Auth Para Generated by the Acquirer (ATKS)	28.4	199
RM (RN)	Transaction Response With Auth Para Generated by the Card Issuer (ATKS)	28.5	201
RO (RP)	Translate a PIN from PEK to ZPK Encryption (ATKS)	28.6	203
RQ (RR)	Verify a Transaction Completion Confirmation Request (ATKS)	28.7	204
RS (RT)	Generate a Transaction Completion Response (ATKS)	28.8	206
RU (RV)	Generate Auth Para at the Card Issuer (ATKS)	28.13	216
RY (RZ)	Generate a *CSCK	25.1	160
RY (RZ)	Export a *CSCK	25.2	161
RY (RZ)	Import a *CSCK	25.3	162
RY (RZ)	Calculate Card Security Codes	25.4	164
RY (RZ)	Verify Card Security Codes	25.5	165

2.2 LIST OF HOST COMMANDS (FUNCTIONAL)

Function	Command	Paragraph	Page
GENERATING A KEY			
Generate a Key	A0 (A1)	3.3	14
Generate and Print a Component	A2 (A3)	3.4	15
Generate and Print a Key as Split Components	NE (NF)	3.5	17
Form a Key from Encrypted Components	A4 (A5)	3.6	19
Generate a CVK Pair	AS (AT)	22.1	140
Generate a TMK, TPK or PVK	HC (HD)	7.2	42
Generate and Print a TMK, TPK or PVK	OE (OF) (OZ)	7.1 40	
Generate a Pair of PVKs	FG (FH)	7.6	47
Generate a TAK	HA (HB)	8.1	50
Generate a Watchword Key	FO (FP)	15.1	95
Generate ZEK/ZAK	FI (FJ)	6.1	36
Generate a ZPK	IA (IB)	5.1	31
Form a ZMK from Three ZMK Components	GG (GH)	4.2	25
Form a ZMK from 2 to 9 ZMK Components	GY (GZ)	4.3	26
Generate and Print a ZMK Component	OC (OD) (OZ)	4.1 23	
TRANSLATING A KEY (FROM ONE ENCRYPTION TO ANOTHER)			
Import a Key	A6 (A7)	3.7	20
Export a Key	A8 (A9)	3.8	21
Translate Key Scheme	B0 (B1)	3.9	22
CVK PAIR			
Translate a CVK Pair from Old LMK to New LMK Encryption	AY (AZ)	22.4	143
Translate a CVK Pair from LMK to ZMK Encryption	AU (AV)	22.2	141
Translate a CVK Pair from ZMK to LMK Encryption	AW (AX)	22.3	142
TMK / TPK / PVK			
Translate a TMK, TPK or PVK	AA (AB)	20.3	127
Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK	AE (AF)	7.3	43
Translate a TMK, TPK or PVK from LMK to ZMK Encryption	FE (FF)	7.5	45
Translate a TMK, TPK or PVK from ZMK to LMK Encryption	FC (FD)	7.4	44
TAK			
Translate a TAK	AC (AD)	20.4	128
Translate a TAK from LMK to TMK Encryption	AG (AH)	8.4	53
Translate a TAK from LMK to ZMK Encryption	MG (MH)	8.3	52
Translate a TAK from ZMK to LMK Encryption	MI (MJ)	8.2	51

Function	Command	Paragraph	Page
WWK			
Translate a Watchword Key from LMK to ZMK Encryption	FQ (FR)	15.2	96
Translate a Watchword Key from ZMK to LMK Encryption	FS (FT)	15.3	97
ZEK / ZAK			
Translate a ZEK/ZAK from LMK to ZMK Encryption	FM (FN)	6.3	38
Translate a ZEK/ZAK from ZMK to LMK Encryption	FK (FL)	6.2	37
ZPK			
Translate a ZPK	KC (KD)	20.2	126
Translate a ZPK from LMK to ZMK Encryption	GC (GD)	5.3	34
Translate a ZPK from ZMK to LMK Encryption	FA (FB)	5.2	32
ZMK			
Translate a ZMK	GE (GF)	20.1	125
Translate ZMK from ZMK to LMK encryption	BY (BZ)	4.4	28
General			
Translate Keys from Old LMK to New LMK	BW (BX)	20.6	130
Erase the Key Change Storage	BS (BT)	20.7	132
PIN SOLICITATION			
Load Solicitation Data to User Storage	QA (QB)	13.1	90
Final Load of Solicitation Data to User Storage	QC (QD)	13.2	91
CLEAR PIN			
Encrypt a Clear PIN	BA (BB)	14.1	93
Decrypt an Encrypted PIN	NG (NH)	14.2	94
GENERATING A PIN, PIN OFFSET, PVV			
Derive a PIN Using the Diebold Method	GA (GB)	9.2	57
Derive a PIN Using the IBM Method	EE (EF)	9.1	55
Generate a Random PIN	JA (JB)	9.3	58
Generate a Diebold PIN Offset	CE (CF)	9.5	60
Generate an IBM PIN Offset	DE (DF)	9.4	59
Generate a VISA PIN Verification Value	DG (DH)	9.6	61
VERIFY AN INTERCHANGE PIN			
Verify an Interchange PIN Using the Comparison Method	BE (BF)	10.8	71
Verify an Interchange PIN Using the Diebold Method	EG (EH)	10.4	67
Verify an Interchange PIN Using the IBM Method	EA (EB)	10.2	64
Verify an Interchange PIN Using the VISA Method	EC (ED)	10.6	69

Function	Command	Paragraph	Page
VERIFY A TERMINAL PIN			
Verify a Terminal PIN Using the Comparison Method	BC (BD)	10.7	70
Verify a Terminal PIN Using the Diebold Method	CG (CH)	10.3	66
Verify a Terminal PIN Using the IBM Method	DA (DB)	10.1	62
Verify a Terminal PIN Using the VISA Method	DC (DD)	10.5	68
TRANSLATING A PIN			
Translate a PIN and PIN Length	BG (BH)	20.5	129
Translate a PIN from LMK to ZPK Encryption	JG (JH)	11.5	78
Translate a PIN from TPK to LMK Encryption	JC (JD)	11.4	77
Translate a PIN from TPK to ZPK Encryption	CA (CB)	11.2	75
Translate a PIN from One ZPK to Another	CC (CD)	11.1	73
Translate a PIN from ZPK to LMK Encryption	JE (JF)	11.3	76
Translate PIN Algorithm	BQ (BR)	11.6	79
PIN MAILER			
Print PIN/PIN and Solicitation Data	PE (PF) (PZ)	12.1	81
Print a PIN Solicitation Mailer	OA (OB) (OZ)	12.2	83
Verify PIN/PIN and Solicitation Mailer Cryptography	PG (PH)	12.3	85
Verify Solicitation Mailer Cryptography	RC (RD)	12.4	86
MESSAGE AUTHENTICATION			
Generate a MAC	MA (MB)	16.1	103
Generate MAC (MAB) for Large Message	MQ (MR)	16.4	106
Verify a MAC	MC (MD)	16.2	104
Verify and Translate a MAC	ME (MF)	16.3	105
Generate MAC (MAB) using ANSI X9.19 Method for a Large Message	MS (MT)	16.5	108
Generate a Binary MAC (Base24)	MK (ML)	17.1	110
Verify a Binary MAC (Base24)	MM (MN)	17.2	112
Verify and Translate a Binary MAC (Base24)	MO (MP)	17.3	113
PRINT FORMATTING			
Load a PIN Text String	LI (LJ)	19.5	124
Load Formatting Data to HSM	PA (PB)	19.3	122
Load Additional Formatting Data to HSM	PC (PD)	19.4	123

Function	Command	Paragraph	Page
USER STORAGE			
Load Data to User Storage	LA (LB)	18.1	114
Verify the Diebold Table in User Storage	LC (LD)	18.3	116
Read Data from User Storage	LE (LF)	18.2	115
WATCHWORD SUPPORT			
Verify a Watchword Response	FU (FV)	15.4	98
Generate a Decimal MAC	LK (LL)	15.5	99
Verify a Decimal MAC	LM (LN)	15.6	100
MISCELLANEOUS			
Generate a VISA CVV	CW (CX)	22.5	144
Verify a VISA CVV	CY (CZ)	22.6	145
Cancel the Authorised State	RA (RB)	21.1	133
Set HSM Response Delay	LG (LH)	21.4	137
Generate a Key Check Value	BU (BV)	21.3	135
Generate a Key Check Value (Not Double-Length ZMK)	KA (KB)	21.2	134
Perform Diagnostics	NC (ND)	21.5	138
HSM Status	NO (NP)	21.6	139
VISA CASH SYSTEM			
Generate and Export a *KML	DI (DJ)	23.1	147
Import a *KML	DK (DL)	23.2	148
Verify Load Signature S1 and Generate Load Signature S2	DM (DN)	23.3	149
Verify Load Completion Signature S3	DO (DP)	23.4	150
Verify Unload Signature S1 and Generate Unload Signature S2	DQ (DR)	23.5	151
Verify Unload Completion Signature S3	DS (DT)	23.6	152
CHIP CARD			
ARQC (or TC/AAC) Verification and/or ARPC Generation	KQ (KR)	24.1	154
Data Authentication Code and Dynamic Number Verification	KS (KT)	24.2	156
Generate Secure Message with Integrity and optional Confidentiality	KU (KV)	24.3	157
AMERICAN EXPRESS SECURITY CODE			
Generate a *CSCK	RY (RZ)	25.1	160
Export a *CSCK	RY (RZ)	25.2	161
Import a *CSCK	RY (RZ)	25.3	162
Calculate Card Security Codes	RY (RZ)	25.4	164
Verify Card Security Codes	RY (RZ)	25.5	165

Function	Command	Paragraph	Page
RACAL TRANSACTION KEY SCHEME			
Transaction Request With a PIN (T/AQ Key)	RI (RJ)	26.1	168
Transaction Request With a PIN (T/CI Key)	RU (RV)	26.3	172
Transaction Request Without a PIN	RK (RL)	26.2	170
Administration Request Message	RM (RN)	26.5	175
Transaction Response with Auth Para from Card Issuer	RO (RP)	26.6	177
Generate Auth Para and Transaction Response	RQ (RR)	26.7	179
Translate KEYVAL	RW (RX)	26.4	174
Confirmation	RS (RT)	26.8	181
DERIVED UNIQUE KEY PER TRANSACTION			
Generate an Base Derivation Key (*BDK)	BI (BJ)	27.1	184
Translate a PIN from *BDK Encryption to Interchange Key Encryption	CI (CJ)	27.2	185
Verify a PIN Using the IBM Method	CK (CL)	27.3	186
Verify a PIN Using the VISA PVV Method	CM (CN)	27.4	187
Verify a PIN Using the Diebold Method	CO (CP)	27.5	188
Verify a PIN Using the Encrypted PIN Method	CQ (CR)	27.6	189
Translate a Base Derivation Key from *ZMK to LMK Encryption	DW (DX)	27.7	190
Translate a Base Derivation Key from LMK to *ZMK Encryption	DY (DZ)	27.8	191
AUSTRALIAN TRANSACTION KEY SCHEME			
Transaction Request Without a PIN	RE (RF)	28.1	193
Transaction Request With a PIN (T/AQ Key)	RG (RH)	28.2	195
Transaction Request With a PIN (T/CI Key)	RI (RJ)	28.3	197
Transaction Response With Auth Para Generated by the Acquirer	RK (RL)	28.4	199
Transaction Response With Auth Para Generated by the Card Issuer	RM (RN)	28.5	201
Translate a PIN from PEK to ZPK Encryption	RO (RP)	28.6	203
Verify a Transaction Completion Confirmation Request	RQ (RR)	28.7	204
Generate a Transaction Completion Response	RS (RT)	28.8	206
Verify a PIN at the Card Issuer Using the IBM Method	QQ (QR)	28.9	208
Verify a PIN at the Card Issuer Using the Diebold Method	QS (QT)	28.10	210
Verify a PIN at the Card Issuer Using the Visa Method	QU (QV)	28.11	212
Verify a PIN at the Card Issuer by Comparison	QW (QX)	28.12	214
Generate Auth Para at the Card Issuer	RU (RV)	28.13	216
Message Authentication Mode Numbers	MU (MV)	28.14	217
Generate a MAC on a Binary Message	MW (MX)	28.15	218

Function	Command	Paragraph	Page
USING THE OPTIONAL RSA CRYPTOSYSTEM			
Generate an RSA Key Set	EI (EJ)	29.1	229
Load a Secret Key	EK (EL)	29.2	231
Translate a Secret Key from the Old LMK to a New LMK	EM (EN)	29.3	232
Generate a MAC on a Public Key	EO (EP)	29.4	233
Verify a MAC on a Public Key	EQ (ER)	29.5	234
Validate a Certificate and Generate a MAC on its Public Key	ES (ET)	29.6	235
Translate a MAC on a Public Key	EU (EV)	29.7	238
Generate a Signature	EW (EX)	29.8	239
Validate a Signature	EY (EZ)	29.9	241
Import a DES Key	GI (GJ)	29.10	243
Export a DES Key	GK (GL)	29.11	246
Hash a Block of Data	GM (GN)	29.12	249

3 GENERIC KEY MANAGEMENT COMMANDS

The HSM provides facilities to:

- Generate keys.
- Print key components.
- Form keys from encrypted components.
- Translate keys.

3.1 Key Type Table

Variant ⇒		0			1			2			3			4			5			6			7			8			9							
↓ LMK ↓		G	E	I	G	E	I	G	E	I	G	E	I	G	E	I	G	E	I	G	E	I	G	E	I	G	E	I	G	E	I					
Pair	Code																																			
04 - 05	00	ZMK			ZMK (Comp)			KML																												
		A			U	A	U	U	A	U																										
06 - 07	01	ZPK																																		
		U	A	U																																
14 - 15	02	PVK TPK TMK															CSCK CVK																			
		U	A	U													U	A	U																	
16 - 17	03	TAK																																		
		U	A	U																																
18 - 19	04																																			
20 - 21	05																																			
22 - 23	06	WWK																																		
		U	A	U																																
24 - 25	07																																			
26 - 27	08																																			
28 - 29	09	BDK			MK-AC			MK-SMI			MK-SMC			MK-DAK			MK-DN																			
		U	A	U	U	A	U	U	A	U	U	A	U	U	A	U	U	A	U	U	A	U														
30 - 31	0A	ZEK																																		
		U	A	U																																
32 - 33	0B																																			
34 - 35	0C	RSA-SK																																		
36 - 37	0D	RSA-MAC																																		
38 - 39	0E																																			

Table of actions applied to each specific LMK pair and variant in generic HSM commands

G = Generate. E = Export. I = Import.
 blank = Not allowed.
 A = allowed in Authorised state.
 U = allowed Unconditionally, i.e. without Authorised state.

The HSM provides a set of commands for key generation, key export and key import. An export command is one that translates a key from LMK encryption to encryption under a ZMK, for sending to another party. Import is the reverse, for receiving keys and translating to local storage. The Key Type Table controls 'permitted actions' for the console and host commands used to generate, import and export keys.

Errors are reported when an action breaks the rules imposed by the table. For example:

29 : Key function not permitted

The table above shows the actions that can be applied to each specific LMK pair.

Not all key type codes are available in all commands for security reasons.

The Key type code used within commands is formed by using the Variant code as the first character then the LMK pair code as the second character. For example the code for a ZPK is 001.

3.2 Key Scheme Table

Key Scheme Tag	Notes
Z	Single length DES key encrypted using ANSI X9.17 methods
U	Encryption of a double length key using variant method. Used for encryption of keys under LMK and can be used for import and export of keys.
T	Encryption of a triple length key using variant method. Used for encryption of keys under LMK and can be used for import and export of keys.
X	Encryption of a double length key using ANSI X9.17 methods only available for import and export of keys. This mode is enabled within configure security command
Y	Encryption of a triple length key using ANSI X9.17 methods only available for import and export of keys. This mode is enabled within configure security command

3.3 Generate a Key

Command: To generate a key and optionally encrypt key under ZMK for transmission.

Notes: See Key Type Table to find key type code.

See Key Scheme Table for schemes available to encrypt keys.

Authorised state is enforced as per Key Type Table.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value A0.
Mode	1 H	0 – Generate Key. 1 – Generate key and encrypt under ZMK.
Key type	3 H	Key type.
Key Scheme (LMK)	1 A	Key length / scheme for encrypting key under LMK. See section 3.2 “Key Scheme Table”.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK only present if mode = 1.
Key scheme (ZMK)	1 A	Key scheme for encrypting key for export. Only present if mode = 1.
Atalla Variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment. Only present if mode = 1.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value A1.
Error code	2 N	00 : No errors 10 : ZMK Parity error 12 : No keys loaded in user storage 13 : LMK error : report to supervisor 15 : Error in input data 21 : Invalid user storage index
Key (LMK)	16H or 1A+32H or 1A+48H	The key encrypted under LMK.
Key (ZMK)	16H or 1A+32H or 1A+48H	The key encrypted under ZMK only present if mode =1.
Key check value	6 H	The key check value.
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.

3.4 Generate and Print a Component

Command: Generate a random component, print it at the HSM attached printer and return the encrypted value to the host.

Notes: The HSM must be in the Authorised state.

A printer must be attached to the HSM Auxiliary port.

The HSM must have a print format already defined.

The Channel Attach option does not return the second response message and its first response message is delayed until after printing has been completed. This is because the channel protocol allows only one response per request.

Not available as part of the standard command set in the RG7X10 series of High-Speed HSMs.

See Key Type Table to find key type code.

See Key Scheme Table for schemes available to encrypt keys.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value A2.
Key type	3 H	Key type.
Key Scheme (LMK)	1 A	Key length / scheme for encrypting key under LMK. See section 3.2 "Key Scheme Table".
Print Field 0	n A	The print field defined as Print Field 0 in the print format definition (must not contain a ";" character).
Delimiter	1 A	Value ";"
Print Field 1	n A	The print field defined as Print Field 1 in the print format definition (must not contain a ";" character).
.	.	.
.	.	.
.	.	.
Last print field	n A	The last print field defined in the print format definition must not contain a ";" character).
End message delimiter	1 C	Optional. 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 (before printing)		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value A3.
Error code	2 N	00 : No Error 13 : LMK error; report to supervisor 15 : Error in input data 16 : Printer not ready/not connected 17 : Not in the Authorized state 18 : Format definition not loaded
Component	16H or 1A+32H or 1A+48H	ZMK component encrypted under component variant of LMK.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.
RESPONSE MESSAGE (after printing)		
Message header	N A	Returned to the Host unchanged
Response code	2 A	Value AZ
Error code	2 N	00 : No errors 13 : LMK error, report to supervisor 16 : Printer not ready/disconnected
End message delimiter	1 C	Present only if present in the command message. Maximum length 32 characters

3.5 Generate and Print a Key as Split Components

Command: Generate a random key, encrypt it under appropriate LMK, print it as two half components or three third components at the HSM attached printer.

Notes: The HSM must be in the Authorised state.

A printer must be attached to the HSM Auxiliary port.

The HSM must have a print format already defined.

The Channel Attach option does not return the second response message and its first response message is delayed until after printing has been completed. This is because the channel protocol allows only one response per request.

Not available as part of the standard command set in the RG7X10 series of High-Speed HSMs.

See Key Type Table to find key type code.

See Key Scheme Table for schemes available to encrypt keys.

For a single length key the key is split into two 8 character values ^P and ^Q in the print format denote the left and right halves respectively.

For a double length key ^P and ^Q in the print format denote the first and second key respectively.

For a triple length key ^P ,^Q and ^R in the print format denote the first, second and third key respectively.

^T in the print format denotes a key check value.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value NE.
Key type	3 H	Key type.
Key Scheme (LMK)	1 A	Key length / scheme for encrypting key under LMK. See section 3.2 "Key Scheme Table".
Print Field 0	n A	The print field defined as Print Field 0 in the print format definition (must not contain a ";" character).
Delimiter	1 A	Value ";"
Print Field 1	n A	The print field defined as Print Field 1 in the print format definition (must not contain a ";" character).
.	.	.
.	.	.
.	.	.
Last print field	n A	The last print field defined in the print format definition must not contain a ";" character).
End message delimiter	1 C	Optional. 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 (before printing)		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value NF.
Error code	2 N	00 : No Error 13 : LMK error; report to supervisor 15 : Error in input data 16 : Printer not ready/not connected 17 : Not in the Authorized state 18 : Format definition not loaded
Key	16H or 1A+32H or 1A+48H	Key encrypted under appropriate LMK.
Key check value	6 H	The key check value
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.
RESPONSE MESSAGE (after printing)		
Message header	N A	Returned to the Host unchanged
Response code	2 A	Value NZ
Error code	2 N	00 : No errors 13 : LMK error, report to supervisor 16 : Printer not ready/disconnected
End message delimiter	1 C	Present only if present in the command message. Maximum length 32 characters

3.6 Form a Key from Encrypted Components

Command: To form a key from encrypted components.

Notes: See Key Type Table to find key type code.

The HSM must be in Authorised state.

See Key Scheme Table for schemes available to encrypt keys.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value A4.
Number of components	1 N	Number of components (2-9).
Key type	3 H	See Key Type Table
Key Scheme (LMK)	1 A	Key scheme for encrypting key under LMK. See section 3.2 "Key Scheme Table".
Key component 1	16H or 1A+32H or 1A+48H	Encrypted key component 1.
Key component 2	16H or 1A+32H or 1A+48H	Encrypted key component 2.
Key component n	16H or 1A+32H or 1A+48H	Encrypted key component n.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value A5.
Error code	2 N	00 : No errors 03 : Invalid number of components 10 : Component parity error 12 : No keys loaded in user storage 13 : LMK error : report to supervisor 15 : Error in input data 17 : Not in authorised state 21 : Invalid user storage index
Key (LMK)	16H or 1A+32H or 1A+48H	The key encrypted under LMK
Key check value	6 H	The key check value
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.

3.7 Import a Key

Command: To import a key encrypted under a ZMK.

Notes: See Key Type Table to find key type code.

Authorised state is enforced as per Key Type Table.

The command does not require the imported key to have odd parity, but odd parity is forced on the encrypted output. Error 01 is returned and subsequent fields are not inhibited.

See Key Scheme Table for schemes available to encrypt keys.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value A6.
Key type	3 H	See Key Type Table.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK.
Key(ZMK)	16H or 1A+32H or 1A+48H	Key encrypted under ZMK.
Key Scheme (LMK)	1 A	Key scheme for encrypting key under LMK. See section 3.2 "Key Scheme Table".
Atalla Variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value A7.
Error code	2 N	00 : No errors 01 : Key parity error, advice only 10 : ZMK Parity error 12 : No keys loaded in user storage 13 : LMK error : report to supervisor 15 : Error in input data 17 : Not in authorised state 21 : Invalid user storage index
Key (LMK)	16H or 1A+32H or 1A+48H	The key encrypted under LMK.
Key check value	6 H	The key check value.
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.

3.8 Export a Key

Command: To encrypt a key under a ZMK for export.

Notes: See Key Type Table to find key type code.

Authorised state is enforced as per Key Type Table.

See Key Scheme Table for schemes available to encrypt keys.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value A8.
Key type	3 H	See Key Type Table.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK.
Key	16H or 1A+32H or 1A+48H	Key encrypted under LMK.
Key Scheme (ZMK)	1 A	Key scheme for encrypting key under ZMK. See section 3.2 "Key Scheme Table".
Atalla Variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value A9.
Error code	2 N	00 : No errors 10 : ZMK Parity error 11 : Key parity error 12 : No keys loaded in user storage 13 : LMK error : report to supervisor 15 : Error in input data 17 : Not in authorised state 21 : Invalid user storage index
Key (ZMK)	16H or 1A+32H or 1A+48H	The key encrypted under ZMK.
Key check value	6 H	The key check value.
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.

3.9 Translate Key Scheme

Command: Translate an existing key to a new key scheme. This command supports the translation from 32H, X and Y formats.

Notes: The HSM must be in Authorised state.

See Key Scheme Table for schemes available to encrypt keys

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value B0.
Key type	3 H	See Key Type Table.
Key	32H or 1A+32H or 1A+48H	The key encrypted under appropriate LMK
Key scheme (LMK)	1 A	Key scheme for encrypting key under LMK. See section 3.2 "Key Scheme Table".
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value B1.
Error code	2 N	00 : No errors 10 : Key Parity error 12 : No keys loaded in user storage 13 : LMK error : report to supervisor 15 : Error in input data 17 : Not in authorised state 21 : Invalid user storage index
Key	1A+32H or 1A+48H	The key encrypted under LMK.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

4 ZONE MASTER KEY MANAGEMENT

The HSM provides facilities to:

- Generate and print a random ZMK component.
- Form a ZMK from three encrypted components.
- Form a ZMK from 2 to 9 encrypted components.
- Translate a ZMK from ZMK to LMK encryption.

4.1 Generate and Print a ZMK Component

Command: Generate a random ZMK component, print it at the HSM attached printer and return the encrypted value to the host.

Notes: The HSM must be in the Authorised state.

A printer must be attached to the HSM Auxiliary port.

The HSM must have a print format already defined.

The Channel Attach option does not return the second response message and its first response message is delayed until after printing has been completed. This is because the channel protocol allows only one response per request.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Not available as part of the standard command set in the RG7X10 series of High-Speed HSMs.

The delimiter to separate optional fields is changed from ";" to "|".

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value OC.
Print Field 0	n A	The print field defined as Print Field 0 in the print format definition (must not contain a ";" character).
Delimiter	1 A	Value ";"
Print Field 1	n A	The print field defined as Print Field 1 in the print format definition (must not contain a ";" character).
.	.	.
Last print field	n A	The last print field defined in the print format definition must not contain a ";" character).
Delimiter	1 A	Optional. If present the following three fields must be present. Value " ". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. 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 (before printing)		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value OZ.
Error code	2 N	00 : No Error 13 : LMK error; report to supervisor 15 : Error in input data 16 : Printer not ready/not connected 17 : Not in the Authorized state 18 : Format definition not loaded
ZMK component	16H or 32H or 1A+32H	ZMK component encrypted under a variant of LMK pair 04-05.
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.
RESPONSE MESSAGE (after printing)		
Message header	N A	Returned to the Host unchanged
Response code	2 A	Value OZ
Error code	2 N	00 : No errors 13 : LMK error, report to supervisor 16 : Printer not ready or disconnected
End message delimiter	1 C	Present only if present in the command message. Maximum length 32 characters

4.2 Form a ZMK from Three ZMK Components

Command: Form a ZMK from three encrypted components and return the ZMK encrypted under LMK pair 04-05, and the check value.

Notes: The HSM must be in the Authorised state.

If a 32-character ZMK is required, the HSM must be configured for double-lengthZMKs using the CS (Configure Security) console command. The encrypted components must be generated using the F or Z console commands.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value GG.
First ZMK component	16H or 32H	The first ZMK component encrypted under a variant of LMK 04-05.
Second ZMK component	16H or 32H	The second ZMK component encrypted under a variant of LMK 04-05.
Third ZMK component	16H or 32H	The third ZMK component encrypted under a variant of LMK 04-05.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. If present must be 0.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value GH.
Error code	2 N	00 : No errors 10 : Parity error in first component 11 : Parity error in second / third component 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 17 : Not in the Authorized state 21 : Invalid user storage index
ZMK	16H or 32H or 1A+32H	The ZMK encrypted under LMK pair 04-05.
Key check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the ZMK. 16H or 6H depends upon KVC type option.
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.

4.3 Form a ZMK from 2 to 9 ZMK Components

Command: Form a ZMK from 2 to 9 encrypted components and return the ZMK encrypted under a variant of LMK pair 04-05, and the check value.

Notes: The HSM must be in the Authorised state.

Use this command to provide inter-operation with non-Thales e-Security security equipment.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command. The encrypted components must be generated using the F or Z console commands.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value GY.
Number of components	1 N	Number of components between 2 and 9 (inclusive).
First ZMK component	16H or 32H	The first ZMK component encrypted under a variant of LMK 04-05.
Second ZMK component	16H or 32H	The second ZMK component encrypted under a variant of LMK 04-05.
.	.	.
Last ZMK component	16H or 32H	The last ZMK component encrypted under a variant of LMK 04-05.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. If present must be 0.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value GZ.
Error code	2 N	00 : No errors 10 : Parity error in first component 11 : Parity error second to ninth components 13 : LMK error; report to supervisor 15 : Error in input data 17 : Not in the Authorized state
ZMK	16H or 32H or 1A+32H	The ZMK encrypted under LMK pair 04-05.
Key check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the ZMK. 16H or 6H depends upon KVC type option.
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.

4.4 Translate ZMK from ZMK to LMK encryption

Command: To translate a ZMK from encryption under a ZMK to encryption under the LMK

Notes: This command is enabled using the CS (Configure Security) console command and also disabled by running the CS command.

The command does not require the imported ZMK to have odd parity, but odd parity is forced on the encrypted output. Error 01 is returned and subsequent fields are not inhibited.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

The HSM must be in Authorised State.

See Key Scheme Table for schemes available to encrypt keys.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value BY.
ZMKi	16H or 32H or 1A+32H or 1A+48H	The ZMKi encrypted under LMK pair 04-05.
ZMK	16H or 32H or 1A+32H or 1A+48H	The ZMK encrypted under ZMKi.
Atalla Variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value “,”. If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value BZ.
Error code	2 N	00 : No errors 01 : ZMK parity error, advice only 10 : ZMKi Parity error 12 : No keys loaded in user storage 13 : LMK error : report to supervisor 15 : Error in input data 17 : Not in authorised state 21 : Invalid user storage index
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK encrypted under LMK pair 04-05.
Key check value	6 H	The key check value.
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.

5 ZONE PIN KEY MANAGEMENT

The HSM provides Host commands to generate and translate a ZPK.

The generate facility encrypts the ZPK under the ZMK for transmission to another party and under the LMK for storage on the Host database.

The two translate commands allow a ZPK to be translated from encryption under a ZMK to encryption under the LMK and vice versa.

5.1 Generate a ZPK

Command: Generate a random PIN key and return it to the Host encrypted under a ZMK for transmission to another party and under the LMK for storage on the Host database.

Notes: If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value IA.
ZMK	16H or 32H or 1A+32H or 1A+48H	The ZMK encrypted under LMK pair 04-05.
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value IB.
Error code	2 N	00 : No errors 10 : ZMK does not have odd parity 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
ZPK under ZMK	16H or 1A+32H or 1A+48H	The ZPK encrypted under the ZMK.
ZPK under LMK	16H or 1A+32H or 1A+48H	The ZPK encrypted under LMK pair 06-07.
Check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the ZPK. 16H or 6H depends upon KCV type option.
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.

5.2 Translate a ZPK from ZMK to LMK Encryption

Command: Translate a ZPK from encryption under a ZMK to encryption under the LMK.

Used to receive a ZPK from another party.

Notes: The command does not require the ZPK to have odd parity, but odd parity is forced on the encrypted output. Unlike other commands, if error 01 is returned, it does not inhibit the return of subsequent fields.

The command tests the ZPK, after decrypting it from under the ZMK, to ensure the key (including the parity bits) is not zero (i.e., X'0000 0000 0000 0000). If the key is zero, the HSM returns error code 11 (all zero ZPK with even parity) and terminates processing.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value FA.
ZMK	16H or 32H or 1A+32H or 1A+48H	The ZMK encrypted under LMK pair 04-05.
ZPK	16H or 1A+32H or 1A+48H	ZPK encrypted under the ZMK.
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. 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
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value FB.
Error code	2 N	00 : No errors 01 : ZPK parity error; advice only 10 : ZMK parity error 11 : All zero ZPK with even parity. Processing is terminated. 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
ZPK	16H or 1A+32H or 1A+48H	Translated ZPK; encrypted under LMK pair 06-07.
Check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the ZPK. 16H or 6H depends upon KCV type option.
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.

5.3 Translate a ZPK from LMK to ZMK Encryption

Command: Translate a ZPK from encryption under the LMK to encryption under a ZMK.
Used to transmit a ZPK to another party.

Notes: If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value GC.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK encrypted under LMK pair 04-05.
ZPK	16H or 1A+32H or 1A+48H	ZPK encrypted under LMK pair 06-07.
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value “;”. If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value GD.
Error code	2 N	00 : No errors 10 : ZMK parity error 11 : ZPK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
ZPK	16H or 1A+32H or 1A+48H	Translated ZPK; encrypted under the ZMK.
Key check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the ZPK. 16H or 6H depends upon KCV type option.
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.

6 ZONE ENCRYPTION, ZONE AUTHENTICATION KEY MANAGEMENT

The HSM provides facilities to generate and translate ZEKs and ZAKs.

For security reasons, encryption and decryption commands using ZEKs are not available in the standard release; if required, refer to Thales e-Security for details.

6.1 Generate ZEK/ZAK

Command: Generate a ZEK or ZAK.

Notes: If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value F1.
Flag	1 N	0 for ZEK, 1 for ZAK.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK encrypted under LMK pair 04-05.
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value FJ.
Error code	2 N	00 : No errors 10 : ZMK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
ZEK or ZAK for transmission	16H or 1A+32H or 1A+48H	ZEK or ZAK encrypted under ZMK (ZEK when Flag is 0, ZAK when Flag is 1).
ZEK for storage	16H or 1A+32H or 1A+48H	ZEK encrypted under LMK pair 30-31 (present only when Flag is 0).
ZAK for storage	16H or 1A+32H or 1A+48H	ZAK encrypted under LMK pair 26-27 (present only when Flag is 1).
Check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the ZEK/ZAK. 16H or 6H depends upon KCV type option.
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.

6.2 Translate a ZEK/ZAK from ZMK to LMK Encryption

Command: Translate a ZEK or ZAK from ZMK to LMK.

Notes: If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value FK.
Flag	1 N	0 for ZEK, 1 for ZAK.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK encrypted under LMK pair 04-05.
ZEK/ZAK	16H or 1A+32H or 1A+48H	ZEK or ZAK encrypted under ZMK (ZEK when Flag is 0, ZAK when Flag is 1).
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value FL.
Error code	2 N	00 : No errors 10 : ZMK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
ZEK	16H or 1A+32H or 1A+48H	ZEK encrypted under LMK pair 30-31 (present only when Flag is 0).
ZAK	16H or 1A+32H or 1A+48H	ZAK encrypted under LMK pair 26-27 (present only when Flag is 1).
Check value	16 H or 6H	Result of encrypting 64 binary zeroes with the ZEK/ZAK. 16H or 6 depends upon KCV type option.
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.

6.3 Translate a ZEK/ZAK from LMK to ZMK Encryption

Command: Translate a ZEK or ZAK.

Notes: If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value FM.
Flag	1 N	0 for ZEK, 1 for ZAK.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK encrypted under LMK pair 04-05.
ZEK	16H or 1A+32H or 1A+48H	ZEK encrypted under LMK pair 30-31 (present only when Flag is 0).
ZAK	16H or 1A+32H or 1A+48H	ZAK encrypted under LMK pair 26-27 (present only when Flag is 1).
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value “,”. If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method: 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value FN.
Error code	2 N	00 : No errors 10 : ZMK parity error 11 : ZEK/ZAK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
ZEK/ZAK	16H or 1A+32H or 1A+48H	ZEK or ZAK encrypted under ZMK (ZEK when Flag is 0, ZAK when Flag is 1).
Check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the ZEK/ZAK. 16H or 6H depends upon KCV type option.
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.

7 TERMINAL MASTER, TERMINAL PIN AND PIN VERIFICATION KEY MANAGEMENT

The TMK, TPK and PVKs are all encrypted under LMK pair 14-15. Therefore the following commands can be used with any of those keys:

- Generate a key and print it in plain text on a mailer.
- Generate a key and encrypt it under a previous version of that key (or any combination of the keys).
- Translate a key from encryption under the LMK to encryption under a similar key.
- Translate a key from ZMK to LMK encryption.
- Translate a key from LMK to ZMK encryption.
- Generate a pair of keys (for VISA PVV keys).

7.1 Generate and Print a TMK, TPK or PVK

Command: Generate a random key, return it encrypted under LMK pair 14-15 and print it on the device attached to the HSM Auxiliary port.

Notes: The HSM must be in the Authorised state.

A printer must be attached to the HSM Auxiliary port.

The HSM must have a print format already defined.

The Channel Attach option does not return the second response message and its first response message is delayed until after printing has been completed. This is because the channel protocol allows only one response per request.

Not available as part of the standard command set in the RG7X10 series of High-Speed HSMs.

The delimiter to separate optional fields is changed from ";" to "|".

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value OE.
Print Field 0	n A	The print field defined as Print Field 0 in the print format definition (must not contain a ";" character).
Delimiter	1 A	Value ;
Print Field 1	n A	The print field defined as Print Field 1 in the print format definition (must not contain a ";" character).
.	.	.
.	.	.
Last print field	n A	The last print field defined in the print format definition (must not contain a ";" character).
Delimiter	1 A	Optional. If present the following three fields must be present. Value " ". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. 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 (before printing)		
Message header	m A	(Subsequently returned to the Host unchanged).
Response code	2 A	Value OF.
Error code	2 N	00 : No errors 13 : LMK error; report to supervisor 15 : Error in input data 16 : Printer not ready/not connected 17 : Not in the Authorized state 18 : Format definition not loaded
TMK, TPK or PVK	16H or 1A+32H or 1A+48H	TMK, TPK or PVK encrypted under LMK pair 14-15.
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.
RESPONSE MESSAGE (after printing)		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value OZ.
Error code	2 N	00 : No errors 13 : LMK error; report to supervisor 16 : Printer not ready/disconnected
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.

7.2 Generate a TMK, TPK or PVK

Command: Generate a random key, and encrypt it under a TMK (TPK or PVK) and under LMK pair 14-15.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value HC.
Current TMK, TPK or PVK	16H or 1A+32H or 1A+48H	The current TMK, TPK or PVK encrypted under LMK pair 14-15.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme TMK	1 A	Optional. Key scheme for encrypting key under TMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value HD.
Error code	2 N	00 : No errors 10 : TMK, TPK or PVK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
New key under the current key	16H or 1A+32H or 1A+48H	The new key encrypted under the current key.
New key under LMK	16H or 1A+32H or 1A+48H	The new key under LMK pair 14-15.
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.

7.3 Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK

Command: Translate a TMK, TPK or PVK from encryption under LMK pair 14-15 to encryption under another TMK (TPK or PVK).

Notes: The command is used to replace an existing key with another key from the database.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value AE.
Current TMK, TPK or PVK	16H or 1A+32H or 1A+48H	The current TMK, TPK or PVK encrypted under LMK pair 14-15.
Stored TMK, TPK or PVK	16H or 1A+32H or 1A+48H	The stored TMK, TPK or PVK under LMK pair 14-15.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme TMK	1 A	Optional. Key scheme for encrypting key under TMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value AF.
Error code	2 N	00 : No errors 10 : Current TMK, TPK or PVK parity error 11 : Stored TMK, TPK or PVK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
Stored key under the current key	16H or 1A+32H or 1A+48H	The stored key encrypted under the current key.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

7.4 Translate a TMK, TPK or PVK from ZMK to LMK Encryption

Command: Translate a TMK, TPK or PVK from encryption under a ZMK to encryption under the LMK.

Notes: The command is used to receive a key from another party.

The HSM must be in the Authorised State.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value FC.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK encrypted under LMK pair 04-05.
TMK, TPK or PVK	16H or 1A+32H or 1A+48H	TMK, TPK or PVK encrypted under the ZMK.
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value “;”. If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value FD.
Error code	2 N	00 : No errors 10 : ZMK parity error 11 : TMK, TPK or PVK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 17: Not in the Authorized state 21 : Invalid user storage index
TMK, TPK or PVK	16H or 1A+32H or 1A+48H	Translated TMK, TPK or PVK; encrypted under LMK pair 14-15.
Key check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the key. 16H or 6H depends upon KCV type option.
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.

7.5 Translate a TMK, TPK or PVK from LMK to ZMK Encryption

Command: Translate a TMK, TPK or PVK from encryption under the LMK to encryption under a ZMK.

Notes: The command is used to send a key to another party.

The HSM must be in the Authorised state.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value FE.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK encrypted under LMK pair 04-05.
TMK, TPK or PVK	16H or 1A+32H or 1A+48H	TMK, TPK or PVK encrypted under LMK pair 14-15.
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value “,”. If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value FF.
Error code	2 N	00 : No errors 10 : ZMK parity error 11 : TMK, TPK or PVK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 17 : Not in the Authorized state 21 : Invalid user storage index
TMK, TPK or PVK	16H or 1A+32H or 1A+48H	Translated TMK, TPK or PVK encrypted under the ZMK.
Key check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the key. 16H or 6H depends upon KCV type option.
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.

7.6 Generate a Pair of PVKs

Command: Generate two random keys and return them each encrypted under LMK pair 14-15 and under a ZMK.

Notes: The command is used to send the keys to another party.

The HSM must be in the Authorised state.

If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value FG.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK encrypted under LMK pair 04-05.
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. Not available for keys generated using new schemes 1 - KCV 6H. Only available for keys generated under new key schemes 2 – KCV 6H for each key. Only available for keys generated in backwards compatible mode.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value FH.
Error code	2 N	00 : No errors 10 : ZMK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 17 : Not in the Authorized state 21 : Invalid user storage index
First TMK, TPK or PVK under LMK	32H or 1A+32H or 1A+48H	New TMK, TPK or PVK; encrypted under LMK pair 14-15.
First TMK, TPK or PVK under ZMK	32H or 1A+32H or 1A+48H	New TMK, TPK or PVK; encrypted under the ZMK.
KCV Type = 0 or 2		
First key check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the first half of TMK, TPK or PVK. 6H if KCV Type = 2.
Second key check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the second half of TMK, TPK or PVK. 6H if KCV Type = 2.
KCV Type = 1		
Key check value	6 H	Result of encrypting 64 binary zeros with the key
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

8 TERMINAL AUTHENTICATION KEY MANAGEMENT

A TAK is used in the generation and verification of MACs. Commands are provided to:

- Generate a TAK for down line loading to an ATM or other terminal.
- Translate a TAK from encryption under a ZMK to encryption under the LMK.
- Translate a TAK from encryption under the LMK to encryption under a ZMK.
- Translate a TAK from encryption under the LMK to encryption under a TMK.

The facilities allow for the use of a TAK in either an interchange or a local network.

8.1 Generate a TAK

Command: Generate a random key, and encrypt it under a TMK (TPK or PVK) and under LMK pair 16-17.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value HA.
TMK	16H or 1A+32H or 1A+48H	The TMK encrypted under LMK pair 14-15.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme TMK	1 A	Optional. Key scheme for encrypting key under TMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value HB.
Error code	2 N	00 : No errors 10 : TMK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
TAK under TMK	16H or 1A+32H or 1A+48H	The random TAK encrypted under the TMK.
TAK under LMK	16H or 1A+32H or 1A+48H	The random TAK under LMK pair 16-17.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

8.2 Translate a TAK from ZMK to LMK Encryption

Command: Translate a TAK from encryption under a ZMK to encryption under the LMK.

Used to receive a key from another party.

Notes: If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value MI.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK encrypted under LMK pair 04-05.
TAK	16H or 1A+32H or 1A+48H	TAK encrypted under ZMK.
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value MJ.
Error code	2 N	00 : No errors 10 : ZMK parity error 11 : TAK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
TAK	16H or 1A+32H or 1A+48H	TAK encrypted under LMK pair 16-17.
Key check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the TAK. 16H or 6H depends upon KCV type option.
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.

8.3 Translate a TAK from LMK to ZMK Encryption

Command: Translate a TAK from encryption under the LMK to encryption under a ZMK.
Used to send a key to another party.

Notes: If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value MG.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK encrypted under LMK pair 04-05.
TAK	16H or 1A+32H or 1A+48H	TAK encrypted under LMK pair 16-17.
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value MH.
Error code	2 N	00 : No errors 10 : ZMK parity error 11 : TAK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
TAK	16H or 1A+32H or 1A+48H	TAK encrypted under the ZMK.
Key check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the TAK. 16H or 6H depends upon KCV type option.
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.

8.4 Translate a TAK from LMK to TMK Encryption

Command: Translate a TAK from encryption under the LMK to encryption under a TMK.
Used to send a key to a terminal.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value AG.
TMK	16H or 1A+32H or 1A+48H	TMK encrypted under the LMK pair 14-15.
TAK	16H or 1A+32H or 1A+48H	TAK encrypted under LMK pair 16-17.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme TMK	1 A	Optional. Key scheme for encrypting key under TMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method: 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value AH.
Error code	2 N	00 : No errors 10 : TMK parity error 11 : TAK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
TAK	16H or 1A+32H or 1A+48H	Translated TAK; encrypted under the TMK.
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.

9 PIN AND OFFSET GENERATION

The HSM provides support for many PIN verification techniques. The techniques often involve the generation of a PIN using a given algorithm, or an algorithm that requires a value known as an offset. The HSM provides support for PIN generation as follows:

- Derive a PIN using the IBM 3624 method.
- Derive a PIN using the Diebold Proprietary Algorithm.
- Generate a random 4-digit PIN.

Offset generation support is provided as follows:

- Generate an IBM PIN offset using the 3624 method.
- Generate a Diebold PIN offset.
- Generate a VISA PIN Verification Value (offset).

9.1 Derive a PIN Using the IBM Method

Command: Generate a 4 to 12-digit PIN using the IBM method.

Notes: If an offset is included, the PIN is derived from the offset in addition to the other data.

If no offset is included, it can be generated by the IBM PIN offset generation command as detailed in Generate an IBM PIN offset.

The decimalization table can be stored in user storage and referenced in the same way as keys.

The decimalization table of 16 digits must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, Error Code 25 is returned.

The HSM can be configured to disallow the use of known weak values in the decimalization tables. This table checking is enabled by default but can be disabled using the Configure Security (CS) console command.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues, deriving the PIN using TDES in place of DES.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value EE.
PVK	16H or 1A+32H or 1A+48H	PVK encrypted under LMK pair 14-15; used to generate the derived PIN.
Offset	12 H	Value OOOOFFFFFF. This field contains the offset (if there is one), left-justified and padded with F.
Check length	2 N	The minimum PIN length.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
Decimalization table	16 N	The table for converting hexadecimal characters to decimal.
PIN validation data	12 A	User-defined data consisting of hexadecimal characters and the character N, which indicates to the HSM where to insert the last 5 digits of the account number.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value EF.
Error code	2 N	00 : No errors 02 : Warning PVK not single length 10 : PVK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 25: Decimalisation table error
PIN	L N or LH	The derived PIN encrypted under LMK pair 02-03.
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.

9.2 Derive a PIN Using the Diebold Method

Command: Generate a PIN using the Diebold method.

Notes: Requires the Diebold table to be in user storage.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value GA.
Index flag	1 A	Value K.
Table pointer	3 H	The value of the base location of the Diebold table.
Algorithm number	2 H	The number of the Diebold algorithm required.
Offset	4 N	For a derived PIN, this is 0000. Otherwise, an offset can be used.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
Validation data	16 A	User-defined data consisting of hexadecimal characters and the character N, which indicates to the HSM where to insert the last 5 digits of the account number. The data must be right-justified and padded with F.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value GB.
Error code	2 N	00 : No errors 12 : No table loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
PIN	L N or LH	The derived PIN encrypted under LMK pair 02-03.
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.

9.3 Generate a Random PIN

Command: Generate a random PIN of 4 to 12 digits.

Notes: If the PIN length is not defined, a PIN of four digits is generated.

The PIN length selected must not exceed the value selected in the Configure Security (CS) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value JA.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN length	2 N	Optional. In the range 04 to 12. If not present, a PIN of 4 digits is generated.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value JB.
Error code	2 N	00 : No errors 13 : LMK error; report to supervisor 15 : Error in input data 24 : PIN length = or > encrypted PIN length
PIN	L N or LH	The derived PIN encrypted under LMK pair 02-03.
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.

9.4 Generate an IBM PIN Offset

Command: Generate a PIN offset using the IBM method.

Notes: The decimalisation table can be stored in user storage and referenced in the same way as keys.

The decimalisation table of 16 digits must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, Error Code 25 is returned.

The HSM can be configured to disallow the use of known weak values in the decimalization tables. This table checking is enabled by default but can be disabled using the Configure Security (CS) console command.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues generating the offset using TDES in place of DES.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value DE.
PVK	16H or 1A+32H or 1A+48H	PVK encrypted under LMK pair 14-15; used to generate the offset.
PIN	L N or LH	The PIN for which an offset is required; encrypted under LMK pair 02-03.
Check length	2 N	The minimum PIN length.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
Decimalization table	16 N	The table for converting hexadecimal values to decimal.
PIN validation data	12 A	User-defined data consisting of hexadecimal characters and the character N, which indicates to the HSM where to insert the last 5 digits of the account number.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value DF.
Error code	2 N	00 : No errors 02 : Warning PVK not single length 10 : PVK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 14: Error in encrypted PIN 15 : Error in input data 21 : Invalid user storage index 25: Decimalization table error
Offset	12 N	The resulting offset value; left-justified and padded with F.
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.

9.5 Generate a Diebold PIN Offset

Command: Generate a PIN using the Diebold method.

Notes: Requires the Diebold table to be in user storage.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value CE.
Index flag	1 A	Value K.
Table pointer	3 H	The value of the base location of the Diebold table in user storage.
Algorithm number	2 H	The number of the Diebold algorithm required.
PIN	L N or LH	The derived PIN encrypted under LMK pair 02-03.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
Validation data	16 A	User-defined data consisting of hexadecimal characters and the character N, which indicates to the HSM where to insert the last 5 digits of the account number. The data must be right-justified and padded with F.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value CF.
Error code	2 N	00 : No errors 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 14 : Encrypted PIN error 15 : Error in input data 21 : Invalid user storage index
Offset	4 N	The resulting Diebold offset.
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.

9.6 Generate a VISA PIN Verification Value

Command: Generate a 4-digit VISA PVV.

Notes: VISA defines the PIN Verification Key Indicator (PVKI) to be between 0 and 6. The HSM does not enforce this restriction.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value DG.
PVK pair	32H or 1A+32H	The two PVKs each encrypted under LMK pair 14-15.
PIN	L N or LH	The PIN for which a PVV is required; encrypted under LMK pair 02-03.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PVKI	1 N	The PVKI (should be between 0 and 6).
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value DH.
Error code	2 N	00 : No errors 10 : PVK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 14 : Error in encrypted PIN 21 : Invalid user storage index 27 : PVK not double length
PVV	4 N	The resulting PVV.
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.

10 PIN VERIFICATION

The HSM supports four methods of PIN verification:

- IBM 3624.
- Diebold Proprietary Algorithm.
- VISA PVV.
- PIN comparison.

For each type, the PIN block is encrypted under a TPK or a ZPK depending on whether it has come from a local ATM (or PIN pad etc.) or from an acquirer. Therefore support is provided for verifying a PIN from a “terminal” or from “interchange”.

10.1 Verify a Terminal PIN Using the IBM Method

Command: Verify a PIN from a local ATM (or PIN pad etc.) using the IBM 3624 method.

Notes: The decimalisation table can be stored in user storage and referenced in the same way as keys.

The decimalisation table of 16 digits must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, Error Code 25 is returned.

The HSM can be configured to disallow the use of known weak values in the decimalization tables. This table checking is enabled by default but can be disabled using the Configure Security (CS) console command.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues verifying the PIN using TDES in place of DES.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value DA.
TPK	16H or 1A+32H or 1A+48H	The TPK under which the PIN block is encrypted; encrypted under LMK pair 14-15.
PVK	16H or 1A+32H or 1A+48H	PVK encrypted under LMK pair 14-15
Maximum PIN length	2 N	Value 12. Mandatory.
PIN block	16 H	The PIN block encrypted under the TPK.
PIN block format code	2 N	One of the valid format codes.
Check length	2 N	The minimum PIN length.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
Decimalization table	16 N	The table for converting hexadecimal values to decimal.
PIN validation data	12 A	User-defined data consisting of hexadecimal characters and the character N, which indicates to the HSM where to insert the last 5 digits of the account number.
Offset	12 H	IBM offset value, left-justified and padded with F.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value DB.
Error code	2 N	00 : No errors 01 : Verification failure 02 : Warning PVK not single length 10 : TPK parity error 11 : PVK parity error 12 : No keys or table loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block error 21 : Invalid user storage index 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits 25 : Decimalization table error
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.

10.2 Verify an Interchange PIN Using the IBM Method

Command: Verify a PIN from interchange using the IBM 3624 method.

Notes: The decimalisation table can be stored in user storage and referenced in the same way as keys.

The decimalisation table of 16 digits must contain at least 8 different digits, with no digit occurring more than 4 times. If this condition is not met, Error Code 25 is returned.

The HSM can be configured to disallow the use of known weak values in the decimalization tables. This table checking is enabled by default but can be disabled using the Configure Security (CS) console command.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues verifying the PIN using TDES in place of DES.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value EA.
ZPK	16H or 1A+32H or 1A+48H	The ZPK under which the PIN block is encrypted; encrypted under LMK pair 06-07.
PVK	16H or 1A+32H or 1A+48H	The PVK encrypted under LMK pair 14-15.
Maximum PIN length	2 N	Value 12.
PIN block	16 H	The PIN block encrypted under the ZPK.
PIN block format code	2 N	One of the valid format codes.
Check length	2 N	The minimum PIN length.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
Decimalization table	16 N	The table for converting hexadecimal values to decimal.
PIN validation data	12 A	User-defined data consisting of hexadecimal characters and the character N, which indicates to the HSM where to insert the last 5 digits of the account number.
Offset	12 H	IBM offset value, left-justified and padded with F.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value EB.
Error code	2 N	00 : No errors 01 : Verification failure 02 : Warning PVK not single length 10 : ZPK parity error 11 : PVK parity error 12 : No keys or table loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block error 21 : Invalid user storage index 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits 25 : Decimalization table error
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.

10.3 Verify a Terminal PIN Using the Diebold Method

Command: Verify a PIN from a local ATM (or PIN pad etc.) using the Diebold method.

Notes: The Diebold table must be stored in user storage before using this command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value CG.
TPK	16H or 1A+32H or 1A+48H	The TPK under which the PIN block is encrypted; encrypted under LMK pair 14-15
Index flag	1 A	Value K.
Table pointer	3 H	The value of the base location of the Diebold table in user storage.
Algorithm number	2 H	The number of the Diebold algorithm required.
PIN block	16 H	The PIN block encrypted under the TPK.
PIN block format code	2 N	One of the valid format codes.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
Validation data	16 A	User-defined data consisting of hexadecimal characters and the character N, which indicates to the HSM where to insert the last 5 digits of the account number. The data must be right-justified and padded with F.
Offset	4 N	For a derived PIN this is 0000. Otherwise, an offset can be used.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value CH.
Error code	2 N	00 : No errors 01 : Verification failure 10 : TPK parity error 12 : No keys loaded or no table in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block error 21 : Invalid user storage index 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits
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.

10.4 Verify an Interchange PIN Using the Diebold Method

Command: Verify a PIN from interchange using the Diebold method.

Notes: The Diebold table must be stored in user storage before using this command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value EG.
ZPK	16H or 1A+32H or 1A+48H	The ZPK under which the PIN block is encrypted; encrypted under LMK pair 06-07.
Index flag	1 A	Value K.
Table pointer	3 H	The value of the base location of the Diebold table in user storage.
Algorithm number	2 H	The number of the Diebold algorithm required.
PIN block	16 H	The PIN block encrypted under the ZPK.
PIN block format code	2 N	One of the valid format codes.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
Validation data	16 A	User-defined data consisting of hexadecimal characters and the character N, which indicates to the HSM where to insert the last 5 digits of the account number. The data must be right-justified and padded with F.
Offset	4 N	For a derived PIN this is 0000. Otherwise, an offset can be used.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value EH.
Error code	2 N	00 : No errors 01 : Verification failure 10 : ZPK parity error 12 : No keys loaded or no table in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block error 21 : Invalid user storage index 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits
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.

10.5 Verify a Terminal PIN Using the VISA Method

Command: Verify a PIN from a local ATM (or PIN pad etc.) using the VISA PVV method.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value DC.
TPK	16H or 1A+32H or 1A+48H	The TPK under which the PIN block is encrypted; encrypted under LMK pair 14-15.
PVK pair	32H or 1A+32H	The two PVKs each encrypted under LMK pair 14-15.
PIN block	16 H	The PIN block encrypted under the TPK.
PIN block format code	2 N	One of the valid format codes.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PVKI	1 N	The PVKI (should be between 0 and 6).
PVV	4 N	The PVV for the PIN.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value DD.
Error code	2 N	00 : No errors 01 : Verification failure 10 : TPK parity error 11 : PVK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block does not contain valid values 21 : Invalid user storage index 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits 27 : PVK not double length
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.

10.6 Verify an Interchange PIN Using the VISA Method

Command: Verify a PIN from interchange using the VISA PVV method.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value EC.
ZPK	16H or 1A+32H or 1A+48H	The ZPK under which the PIN block is encrypted; encrypted under LMK pair 06-07.
PVK pair	32H or 1A+32H	The two PVKs each encrypted under LMK pair 14-15.
PIN block	16 H	The PIN block encrypted under the ZPK.
PIN block format code	2 N	One of the valid format codes.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PVKI	1 N	The PVKI (should be between 0 and 6).
PVV	4 N	The PVV for the PIN.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value ED.
Error code	2 N	00 : No errors 01 : Verification failure 10 : ZPK parity error 11 : PVK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block does not contain valid values 21 : Invalid user storage index 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits 27 : PVK not double length
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.

10.7 Verify a Terminal PIN Using the Comparison Method

Command: Verify a PIN received from an ATM (or terminal etc.) by comparing it with a value held on the Host database.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value BC.
TPK	16H or 1A+32H or 1A+48H	The TPK under which the PIN block is encrypted; encrypted under LMK pair 14-15.
PIN block	16 H	The PIN block containing the PIN for verification; encrypted under the TPK.
PIN block format code	2 N	One of the valid format codes.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN	L N or LH	The PIN from the Host database encrypted under LMK pair 02-03.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value BD.
Error code	2 N	00 : No errors 01 : Verification failure 10 : TPK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 14 : Error in PIN from Host database 15 : Error in input data 20 : PIN block does not contain valid values 21 : Invalid user storage index 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits
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.

10.8 Verify an Interchange PIN Using the Comparison Method

Command: Verify a PIN received from interchange by comparing it with a value held on the Host database.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value BE.
ZPK	16H or 1A+32H or 1A+48H	The ZPK under which the PIN block is encrypted; encrypted under LMK pair 06-07.
PIN block	16 H	The PIN block containing the PIN for verification; encrypted under the ZPK.
PIN block format code	2 N	One of the valid format codes.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN	L N or LH	The PIN from the Host database encrypted under LMK pair 02-03.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value BF.
Error code	2 N	00 : No errors 01 : Verification failure 10 : ZPK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 14 : Error in PIN from Host database 15 : Error in input data 20 : PIN block does not contain valid values 21 : Invalid user storage index 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits
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.

11 PIN TRANSLATION

Commands are provided to translate PIN blocks from encryption under one key to encryption under another. The commands can also translate the format of a PIN block, with the exception of those that translate to the LMK (where the PIN is not held in a standard format). The key translations available are as follows:

- From one ZPK to another ZPK
- From TPK to ZPK
- From ZPK to LMK
- From TPK to LMK
- From LMK to ZPK

11.1 Translate a PIN from One ZPK to Another

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

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value CC.
Source ZPK	16H or 1A+32H or 1A+48H	Source ZPK under which the PIN block is currently encrypted; encrypted under LMK pair 06-07.
Destination ZPK	16H or 1A+32H or 1A+48H	Destination ZPK under which the PIN block is to be encrypted; encrypted under LMK pair 06-07.
Maximum PIN length	2 N	Value 12.
Source PIN block	16 H	The source PIN block encrypted under the source ZPK.
Source PIN block format	2 N	The format code for the source PIN block.
Destination PIN block format	2 N	The format code for the destination PIN block.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value CD.
Error code	2 N	00 : No errors 10 : Source ZPK parity error 11 : Destination ZPK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block data error 21 : Invalid user storage index 22 : Invalid account number 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits
PIN length	2 N	Length of the returned PIN.
Destination PIN block	16 H	The destination PIN block encrypted under the destination ZPK.
Destination PIN block format	2 N	As received in the command message.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

11.2 Translate a PIN from TPK to ZPK Encryption

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

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value CA.
Source TPK	16H or 1A+32H or 1A+48H	Source TPK under which the PIN block is currently encrypted; encrypted under LMK pair 14-15.
Destination ZPK	16H or 1A+32H or 1A+48H	Destination ZPK under which the PIN block is to be encrypted; encrypted under LMK pair 06-07.
Maximum PIN length	2 N	Value 12.
Source PIN block	16 H	The source PIN block encrypted under the source TPK.
Source PIN block format	2 N	The format code for the source PIN block.
Destination PIN block format	2 N	The format code for the destination PIN block.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value CB.
Error code	2 N	00 : No errors 10 : Source TPK parity error 11 : Destination ZPK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block data error 21 : Invalid user storage index 22 : Invalid account number 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits
PIN length	2 N	Length of the returned PIN.
Destination PIN block	16 H	The destination PIN block encrypted under the destination ZPK.
Destination PIN block format	2 N	As received in the command message.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

11.3 Translate a PIN from ZPK to LMK Encryption

Command: Translate a PIN from encryption under a ZPK to encryption under the LMK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value JE.
Source ZPK	16H or 1A+32H or 1A+48H	The ZPK under which the PIN block is currently encrypted; encrypted under LMK pair 06-07.
PIN block	16 H	The source PIN block encrypted under the ZPK.
PIN block format	2 N	The format code for the PIN block.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value JF.
Error code	2 N	00 : No errors 10 : ZPK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block data error 21 : Invalid user storage index 22 : Invalid account number 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits
PIN	L N or LH	The PIN encrypted under LMK pair 02-03.
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.

11.4 Translate a PIN from TPK to LMK Encryption

Command: Translate a PIN from encryption under a TPK to encryption under the LMK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value JC.
Source TPK	16H or 1A+32H or 1A+48H	Source TPK under which the PIN block is currently encrypted; encrypted under LMK pair 14-15.
PIN block	16 H	The source PIN block encrypted under the TPK.
PIN block format	2 N	The format code for the PIN block.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value JD.
Error code	2 N	00 : No errors 10 : TPK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block data error 21 : Invalid user storage index 22 : Invalid account number 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits
PIN	L N or LH	The PIN encrypted under LMK pair 02-03.
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.

11.5 Translate a PIN from LMK to ZPK Encryption

Command: Translate a PIN from encryption under the LMK to encryption under a ZPK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value JG.
Destination ZPK	16H or 1A+32H or 1A+48H	The ZPK under which the PIN block is to be encrypted; encrypted under LMK pair 06-07.
PIN block format	2 N	The format code for the PIN block.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN	L N or LH	The PIN encrypted under LMK pair 02-03.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value JH.
Error code	2 N	00 : No errors 11 : ZPK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 14 : Error in PIN from Host 15 : Error in input data 20 : PIN block data error 21 : Invalid user storage index 23 : Invalid PIN block format code
PIN block	16 H	The PIN block encrypted under the ZPK.
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.

11.6 Translate PIN Algorithm

Command: Translate a PIN from encryption using the VISA PIN algorithm to encryption using the Racal algorithm.

Notes: The HSM must be configured for the Racal algorithm.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value BQ.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN	L N	The PIN encrypted under LMK pair 02-03 using the VISA algorithm.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value BR.
Error code	2 N	00 : No errors 13 : LMK error; report to supervisor 14 : Error in PIN from Host 15 : Error in input data 17 : Not in the Authorized state
PIN	L H	The PIN encrypted under new LMK pair 02-03 using the Racal algorithm.
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.

12 PIN MAILER PRINTING

The HSM can print PIN mailers (multicopy forms, the contents of which can be read only after the form has been opened) and other types of data that must be kept secret.

PIN mailers can be used to send PINs to cardholders. Also, if the cardholder is to be given the opportunity of selecting his/her own PIN by mail (instead of at an entry device), solicitation data can be sent; it is not necessary to send a PIN if only a solicitation request is to be sent.

The HSM provides the following print facilities:

- Print a PIN/PIN and solicitation data.
- Print solicitation data only.

Because the values that are printed on a mailer are not available to the Host, the HSM returns check data to the Host to give confidence that the data printed on the mailer is correct (i.e., the HSM has performed the correct cryptographic functions).

The data can be verified using the following commands:

- Verify the cryptography for the PIN/PIN and solicitation data.
- Verify the cryptography for the solicitation data.

(For RG7X10 series High-Speed HSMs, refer to Chapter 1).

12.1 Print PIN/PIN and Solicitation Data

Command: Print the PIN or the PIN plus solicitation data at the HSM-attached terminal.

Notes: The HSM must be in the Authorised state.

A printer must be attached to the HSM Auxiliary port.

The HSM must have a print format already defined.

The Channel Attach option does not return the second response message is delayed until after printing has been completed. This is because the channel protocol allows only one response per request.

Not available as part of the standard command set in the RG7X10 series of High-Speed HSMs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value PE.
Document type	1 A	A : for 1st mailer on a 2-up form B : for 2nd mailer on a 2-up form C : for a 1-up form
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN	L N or LH	The PIN encrypted under LMK pair 02-03.
Print Field 0	n A	The print field defined as Print Field 0 in the print format definition (must not contain a ";" character).
Delimiter	1 A	Value ";"
Print Field 1	n A	The print field defined as Print Field 1 in the print format definition (must not contain a ";" character).
.	.	.
.	.	.
.	.	.
Last print field	n A	The last print field defined in the print format definition (must not contain a ";" character).
End message delimiter	1 C	Optional. 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 (before printing)		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value PF.
Error code	2 N	00 : No errors 13 : LMK error; report to supervisor 14 : Error in PIN from Host 15 : Error in input data 16 : Printer not ready 17 : Not in the Authorized state 18 : Document definition not loaded
PIN and reference number check value	L+ 12 N	The cryptographic check on the PIN and solicitation reference number.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE (after printing)		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value PZ.
Error code	2 N	00 : No errors
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.

12.2 Print a PIN Solicitation Mailer

Command: Print PIN solicitation data at the HSM-attached terminal.

Notes: The HSM must be in the Authorised state.

A printer must be attached to the HSM Auxiliary port.

The HSM must have a print format already defined.

The Channel Attach option does not return the second response message and its first response message is delayed until after printing has been completed. This is because the channel protocol allows only one response per request.

Not available as part of the standard command set in the RG7X10 series of High-Speed HSMs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value OA.
Document type	1 A	A : for 1st mailer on a 2-up form. B : for 2nd mailer on a 2-up form. C : for a 1-up form.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
Print Field 0	n A	The print field defined as Print Field 0 in the print format definition (must not contain a ";" character).
Delimiter	1 A	Value ";"
Print Field 1	n A	The print field defined as Print Field 1 in the print format definition (must not contain a ";" character).
.	.	.
.	.	.
.	.	.
Last print field	n A	The last print field defined in the print format definition (must not contain a ";" character).
End message delimiter	1 C	Optional. 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 (before printing)		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value OB.
Error code	2 N	00 : No errors 13 : LMK error; report to supervisor 15 : Error in input data 16 : Printer not ready 17 : Not in the Authorized state 18 : Document definition not loaded
Reference number check value	12 N	The cryptographic check on the solicitation reference number.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE (after printing)		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value OZ.
Error code	2 N	00 : No errors.
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.

12.3 Verify PIN/PIN and Solicitation Mailer Cryptography

Command: Verify the PE command processing performed by the HSM.

Notes: It is suggested that a PE command performed by one HSM is verified by a PG command performed by a different HSM.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value PG.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN	L N or LH	The PIN encrypted under LMK pair 02-03.
Reference number check value	L + 12 N	The cryptographic check on the solicitation reference number.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value PH.
Error code	2 N	00 : No errors 01 : Verification fail 13 : LMK error; report to supervisor 14 : Error in PIN from Host 15 : Error in input 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.

12.4 Verify Solicitation Mailer Cryptography

Command: Verify the OA command processing performed by the HSM.

Notes: It is suggested that an OA command performed by one HSM is verified by an RC command performed by a different HSM.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RC.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
Reference number check value	12 N	The cryptographic check on the solicitation reference number.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value RD.
Error code	2 N	00 : No errors 01 : Verification fail 13 : LMK error; report to supervisor 15 : Error in input 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.

13 PIN SOLICITATION DATA PROCESSING

When a cardholder is given the option of selecting a PIN, he/she returns a form containing a PIN selection and a reference number. For security reasons, the only connection between the PIN and the cardholder's account is this reference number which is a cryptographic representation of the last 10 digits of the account number (excluding the account number check digit).

The HSM processes these values and returns the encrypted PIN and the last 10 digits of the account number (excluding check digit). The Host can match the account number digits and store the encrypted PIN for subsequent processing (for verification purposes or the creation of PIN offsets etc.).

Because the reference number is the only link to the cardholder's PIN, there must be a means of validating the data that is manually entered. There is no way to validate the PIN except through dual entry procedures or through the visual comparison of the value entered and the value recorded on the mailer form.

The 12-digit reference number, unlike the PIN, can be validated by a Host program. This reference number is a 10-digit number, followed by two check digits. The check digits can be validated during or after data entry.

The data is batch processed via Host commands. The number of records entered must be greater than or equal to the minimum batch size set when the HSM is configured. Each batch consists of at least one logical record. Each logical record contains a 12-digit reference number (obtained from the returned solicitation mailer) and the cardholder-selected PIN.

When the batch has been loaded to internal memory, the HSM encrypts the PINs under LMK pair 02-03, and decrypts the reference numbers, yielding a value which contains the 10 right-most digits of the account number (excluding the check digit). The PIN and 10 digits of the account number are returned to the Host.

The algorithm for validating the two check digits of a reference number is as follows:

First Check Digit:

The first of the two check digits is calculated as:

MOD 10 [10 - MOD 10 (Y)]

where Y is the sum of the products obtained by multiplying the 3rd to the 10th digits of the reference number by the following weights:

Digit	Weight
3	9
4	7
5	8
6	6
7	7
8	9
9	6
10	8

Second Check Digit:

The second check digit is calculated as:

MOD 10 [10 - MOD 10 (Z)]

where Z is the sum of the following:

$f(\text{digit 1}) + \text{digit 2} + f(\text{digit 3}) + \text{digit 4} + f(\text{digit 5}) + \text{digit 6} + f(\text{digit 7}) + \text{digit 8} + f(\text{digit 9}) + \text{digit 10} + f(\text{first check digit})$

The value of $f(\text{digit } n)$ is determined as follows:

Digit	$f(\text{digit } n)$
0	0
1	2
2	4
3	6
4	8
5	1
6	3
7	5
8	7
9	9

The MOD 10 (n) operation yields a value that is the remainder after dividing n by 10. This remainder is the same as the low-order digit on n.

The following example illustrates the validation of the reference number 936125183702, where 0 is the first check digit and 2 is the second check digit.

10-digit reference												check digits	
9	3	6	1	2	5	1	8	3	7	0	2		

CHECK DIGIT VALIDATION EXAMPLE														
FIRST CHECK DIGIT														
$ \begin{array}{cccccccccccccc} & 6 & & 1 & & 2 & & 5 & & 1 & & 8 & & 3 & & 7 \\ \times & 9 & x & 7 & x & 8 & x & 6 & x & 7 & x & 9 & x & 6 & x & 8 \\ \hline & 5 & + & 7 & + & 1 & + & 3 & + & 7 & + & 7 & + & 1 & + & 5 \\ & 4 & & 6 & & 0 & & 0 & & 2 & & 8 & & 8 & & 6 \end{array} = 260 $														
$ \begin{aligned} \text{MOD 10 } [10 - \text{MOD 10}(260)] &= 0 \\ \text{MOD 10 } [10-0] &= 0 \\ \text{MOD 10 } [10] &= 0 \end{aligned} $														
SECOND CHECK DIGIT														
$ \begin{aligned} f(9) + 3 + f(6) + 1 + f(2) + 5 + f(1) + 8 + f(3) + 7 + f(0) &= \\ 9 + 3 + 3 + 1 + 4 + 5 + 2 + 8 + 6 + 7 + 0 &= 48 \\ \text{mod 10 } [10 - \text{mod 10}(48)] &= 8 \\ \text{mod 10 } [10 - 8] &= 2 \\ \text{mod 10 } [2] &= 2 \end{aligned} $														

The HSM provides the following Host commands to support solicitation data entry:

- Load solicitation data to user storage.
- Final load of solicitation data and start processing.
- Enable solicitation data entry at the Console.
- Disable solicitation data entry at the Console.
- Response to solicitation data entry at the Console.

13.1 Load Solicitation Data to User Storage

Command: Load from 1 to 25 records of solicitation data to user storage.

Notes: The command can be used repeatedly to load the solicitation data. It overwrites any tables or keys stored in the user storage. Therefore, it is necessary to reload the tables and keys when solicitation processing has been completed.

This command will not operate in the RG7200 or RG7210 due to limitations of the channel protocol. To use PIN solicitation functions in channel connected HSMs the Final Load (QC) command must be used.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value QA.
Solicitation Data 1	n A	The 12-digit reference number. The selected PIN (4 to 12 digits). A semicolon ";" as a delimiter.
Solicitation Data 2	n A	The 12-digit reference number. The selected PIN. A semicolon ";" as a delimiter.
.	.	.
.	.	.
.	.	.
Last solicitation data	n A	The 12-digit reference number. The selected PIN. A semicolon ";" as a delimiter.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value QB.
Error code	2 N	00 : No errors 15 : Error in input data 30 : Invalid reference number
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.

13.2 Final Load of Solicitation Data to User Storage

Command: Load the last set of solicitation records to user storage and start processing data.

Notes: The command overwrites any tables or keys stored in user storage. Therefore, it is necessary to reload the tables and keys when solicitation processing has been completed. The response message is repeated until all the processed data has been returned to the Host.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value QC.
Solicitation Data 1	n A	The 12-digit reference number. The selected PIN (4 to 12 digits). A semicolon “;” as a delimiter.
Solicitation Data 2	n A	The 12-digit reference number. The selected PIN. A semicolon “;” as a delimiter.
.	.	.
.	.	.
.	.	.
Last solicitation data	n A	The 12-digit reference number. The selected PIN. A semicolon “;” as a delimiter.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value QD.
Error code	2 N	00 : No errors 13 : LMK error; report to supervisor 15 : Error in input data 30 : Invalid reference number 31 : Insufficient entries for batch
Processed Data 1	n N	The 10 right-most digits of the account number and PIN encrypted under LMK pair 02-03, truncated (if necessary). The length is L or L+1 (to ensure that the length is even; by padding with X'F).
Processed Data 2	n N	The 10 right-most digits of the account number and PIN encrypted under LMK pair 02-03, truncated (if necessary). The length is L or L+1 (to ensure that the length is even; by padding with X'F).
.	.	.
.	.	.
.	.	.
Last processed data	n N	The 10 right-most digits of the account number and PIN encrypted under LMK pair 02-03, truncated (if necessary). The length is L or L+1 (to ensure that the length is even; by padding with X'F).
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.

14 CLEAR PIN SUPPORT



CAUTION: THE USE OF CLEAR PIN FACILITIES PRESENTS A SIGNIFICANT SECURITY RISK.

The HSM provides two commands to support the use of clear PINs:

- Encrypt a clear PIN.
- Decrypt an encrypted PIN and return a reference number for solicitation data processing.

14.1 Encrypt a Clear PIN

Command: Encrypt a clear text PIN.

Notes: The HSM must be in the Authorised state.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value BA.
PIN	L H	The clear text PIN left-justified and padded with X'F to the encrypted PIN length L. Value set with Configure Security (CS) console command (range 5 – 13).
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value BB.
Error code	2 N	00 : No errors 13 : LMK error; report to supervisor 15 : Error in input data 17 : Not in the Authorized state
PIN	L N	The PIN encrypted under LMK pair 02-03.
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.

14.2 Decrypt an Encrypted PIN

Command: Decrypted an encrypted PIN and return a reference number.

Notes: The command is available only if selected during configuration (see Chapter 3 of Reference 1, the Operation and Installation manual).

The HSM must be in the Authorised state.

The reference number can be used in solicitation data processing.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value NG.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN	L N	The PIN encrypted under LMK pair 02-03.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value NH.
Error code		00 : No errors 13 : LMK error; report to supervisor 14 : Error in encrypted PIN 15 : Error in input data 17 : Not in the Authorized state
PIN	L N	The clear PIN left-justified and padded with X'F.
Reference number	12 N	The reference number derived by encrypting the account number under LMK pair 18-19.
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.

15 HOST WATCHWORD SUPPORT

The HSM provides general Watchword support, with commands to:

- Generate a Watchword Key.
- Translate a Watchword Key from encryption under the LMK to encryption under a ZMK.
- Translate a Watchword Key from encryption under a ZMK to encryption under the LMK.
- Verify a Watchword response.
- Generate a decimal MAC
- Verify a decimal MAC

15.1 Generate a Watchword Key

Command: Generate a Watchword Key (WWK).

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value F0.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ":". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV Backwards compatible 1 - Combined KCV 6H
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value FP.
Error code	2 N	00 : No errors 13 : LMK error; report to supervisor
WWK	16H or 1A+32H or 1A+48H	Watchword Key encrypted under LMK pair 22-23.
Check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the WWK. 16H or 6H depends upon KCV type option.
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.

15.2 Translate a Watchword Key from LMK to ZMK Encryption

Command: Translate a Watchword Key from encryption under the LMK to encryption under a ZMK.

Notes: If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value FQ.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK encrypted under LMK pair 04-05.
WWK	16H or 1A+32H or 1A+48H	Watchword encrypted under LMK pair 22-23.
Atalla Variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value FR.
Error code	2 N	00 : No errors 10 : ZMK parity error 11 : ZPK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
WWK	16H or 1A+32H or 1A+48H	WWK encrypted under ZMK.
Key check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the WWK. 16H or 6H depends upon KCV type option.
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.

15.3 Translate a Watchword Key from ZMK to LMK Encryption

Command: Translate a Watchword Key from encryption under a ZMK to encryption under the LMK.

Notes: If using a 32-character ZMK, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value FS.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK encrypted under LMK pair 04-05.
WWK	16H or 1A+32H or 1A+48H	Watchword encrypted under ZMK.
Atalla Variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value “;”. If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value FT.
Error code	2 N	00 : No errors 10 : ZMK parity error 11 : Imported key all zero 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
WWK	16H or 1A+32H or 1A+48H	WWK encrypted under LMK pair 22-23.
Key check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the WWK. 16H or 6H depends upon KCV type option.
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.

15.4 Verify a Watchword Response

Command: Verify a Watchword response.

Notes: The cipher scheme used depends upon the key length.

Single length WWK – Cipher scheme code 0

Double length WWK – Cipher scheme code 1

Triple length WWK – Cipher scheme code 2

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value FU.
WWK	16H or 1A+32H or 1A+48H	Watchword Key encrypted under LMK pair 22-23.
Flag	1 N	1 = response for PIN 1, 2 = response for PIN 2.
Challenge	7 N	Watchword challenge.
Response	7 N	Watchword response.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value FV.
Error code	2 N	00 : No errors 01 : Verification failure 10 : WWK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
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.

15.5 Generate a Decimal MAC

- Command: Generate a Decimal MAC on character.
- Notes: This command assumes that the data on which the MAC is to be generated consists of characters only.
The cipher scheme used depends upon the key length.
Single length WWK – Cipher scheme code 0
Double length WWK – Cipher scheme code 1 (X9.19 MAC)

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	(Subsequently returned to the Host unchanged).
Command Code	2 A	Value LK.
TAK	16H or 1A+32H	The TAK encrypted under LMK pair 16-17.
MAC Length	1 H	Number of characters required in Decimal MAC (range 1 to 12).
Data	0 - n	The data on which a MAC is to be generated, n= 1024 (512 for SNA-SDLC) systems.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value LL
Error Code	2 N	00 : No errors 10 : TAK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : Invalid key length
MAC	n N	The calculated decimal MAC with a length as specified in the command.
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19.
Message Trailer	n A	Will only be present if in the command message. Maximum length 32 characters.

15.6 Verify a Decimal MAC

Command: To verify a decimal MAC of user defined length

Notes: This command assumes that the data on which the MAC is to be generated consists of characters only

The cipher scheme used depends upon the key length.

Single length WWK – Cipher scheme code 0

Double length WWK – Cipher scheme code 1 (X9.19 MAC)

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	(Subsequently returned to the Host unchanged).
Command Code	2 A	Value LM.
TAK	16 H or 1A+32H	The TAK encrypted under LMK pair 16-17.
MAC length	1 H	The number of characters in the Decimal MAC (range 1 - 12).
MAC	n N	The MAC to be verified.
Data	0 - n	The data on which the MAC to be verified was calculated, n= 1024 (512 for SNA-SDLC systems).
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged
Response Code	2 A	Value LN
Error Code	2 N	00 : No errors 01 : MAC did not verify 27 : Invalid key length 10 : TAK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
End Message Delimiter	1 C	Will only be present if present in the command message. Value X'19.
Message Trailer	n A	Only present if in the command message. Maximum length 32 characters.

16 MESSAGE AUTHENTICATION CODE SUPPORT

The HSM provides commands to generate, verify and translate a MAC.

Because the HSM has no flow control, the application programmer is responsible for ensuring that the input buffer is not exceeded. The HSM input buffer is 2047 bytes in length for all models except the SNA-SDLC interface devices (RG7500 and RG7600), in which it is 1023 bytes. The length of the input buffer limits the amount of data over which a MAC can be calculated in a single call to the HSM. To be sure that there is no overflow, limit the amount of data to 1024 bytes, or 512 bytes if using SNA-SDLC.

The HSM normally calculates a MAC by converting the characters to ASCII (if they are received as EBCDIC (shown in the table), and filling the last 64-bit block with binary zeroes (if necessary). For this, the HSM must be configured for EBCDIC (and not ASCII) by the CH (Configure Host) console command. The HSM performs no other editing of the data.

The HSM provides commands to generate and verify MACs on short messages of up to 2047 bytes (1023 bytes for SNA-SDLC). For longer messages the MQ (Generate MAC (MAB) for Large Message) command divides the message data into blocks. It creates a MAB or IV (Initialisation Vector) for the first block, the last block and one or more blocks in between. The response message for the last data block includes the MAC for the whole message. The MAC is the first four bytes (eight characters) of the last MAB.

The MQ command handles the data in 8-bit binary form. It does not convert EBCDIC data to ASCII; it calculates the MAC on the data as presented to the HSM. Therefore, any necessary character conversion must be performed by the Host system.

The command used for large messages provides the Host with all the information needed for MAC generation, MAC verification and continuation IVs when chaining MACs.

EBCDIC to ASCII Translation Table

EBCDIC Hex	ASCII Cha	ASCII Hex	EBCDIC Hex	ASCII Cha	ASCII Hex	EBCDIC Hex	ASCII Cha	ASCII Hex
00	NUL	00	40	SP	20	80	a	61
01	SOH	01	41			81	b	62
02	STX	02	42			82	c	63
03	ETX	03	43			83		C3
04			44			84	d	64
05	HT	09	45			85	e	65
06			46			86	f	66
07	DEL	7F	47			87	g	67
08			48			88	h	68
09			49			89	i	69
0A			4A			8A		CA
0B	VT	0B	4B	.	2E	8B	{	7B
0C	FF	0C	4C	<	3C	8C		CC
0D	CR	0D	4D	(28	8D		CD
0E	SO	0E	4E	+	2B	8E		CE
0F	SI	0F	4F		7C	8F		CF
10	DLE	10	50	&	26	90		D0
11	DC1	11	51			91	j	6A
12	DC2	12	52			92	k	6B
13	DC3	13	53			93	l	6C
14			54			94	m	6D
15			55			95	n	6E
16	BS	08	56			96	o	6F
17			57			97	p	70
18	CAN	18	58			98	q	71
19	EM	19	59			99	r	72
1A			5A	!	21	9A		DA
1B			5B	\$	24	9B	}	7D
1C		1 C	5C	*	2 A	9C		DC
1D		1D	5D)	29	9D		DD
1E		1E	5E	;	3B	9E		DE
1F		1F	5F		5F	9F		DF
20			60	-	2D	A0		E0
21			61	/		A1	~	E1
22	FS	1 C	62			A2	s	E2
23			63			A3	t	E3
24			64			A4	u	E4
25	LF	0A	65			A5	v	E5
26	ETB	17	66			A6	w	E6
27	ESC	1B	67			A7	x	E7
28			68			A8	y	E8
29			69			A9	z	E9
2A			6A		7C	AA		EA
2B			6B	,	2C	AB		EB
2C			6C	%		AC		EC
2D	ENQ	05	6D		5F	AD	[ED
2E	ACK	06	6E	>	3E	AE		EE
2F	BEL	07	6F	?	3F	AF		EF
30			70			B0		F0
31			71			B1		F1
32	SYN	16	72			B2		F2
33			73			B3		F3
34			74			B4		F4
35			75			B5		F5
36			76			B6		F6
37	EOT	04	77			B7		F7
38			78			B8		F8
39			79	'	60	B9		F9
3A			7A	:	3A	BA		FA
3B			7B	#	23	BB		FB
3C	DC4	14	7C	@	40	BC		FC
3D	NAK	15	7D	'	27	BD]	FD
3E			7E	=	3D	BE		FE
3F	SUB	1A	7F	n	22	BF		FF

Empty locations translate to ASCII null X'00.

16.1 Generate a MAC

Command: Generate a MAC on given data.

Notes: The value n given for Data is the recommended maximum value; it can be increased towards 2047 (1023 for SNA-SDLC systems) with consideration for the overall buffer size compared to the size of the complete HSM command message.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value MA.
TAK	16H or 1A+32H or 1A+48H	TAK encrypted under LMK pair 16-17.
Data	0 - n	The data on which a MAC is to be generated, n = 1024 (512 for SNA-SDLC systems).
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value MB.
Error code	2 N	00 : No errors 10 : TAK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index. 27 : TAK not single length
MAC	8 H	The calculated 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.

16.2 Verify a MAC

Command: Verify a MAC.

Notes: The value n given for Data is the recommended maximum value; it can be increased toward 2047 (1023 for SNA-SDLC systems) with consideration for the overall buffer size compared to the size of the complete HSM command message.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value MC.
TAK	16H or 1A+32H or 1A+48H	TAK encrypted under LMK pair 16-17.
MAC	8 H	The MAC to be verified.
Data	0 - n	The data on which the MAC to be verified was calculated, n = 1024 (512 for SNA-SDLC systems).
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value MD.
Error code	2 N	00 : No errors 01 : MAC verification failure 10 : TAK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : TAK not single length
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.

16.3 Verify and Translate a MAC

Command: Verify a MAC and, if successful, generate a MAC on the same data with a different key.

Notes: If the source MAC does not verify, the HSM does not return a destination MAC.

The value n given for Data is the recommended maximum value; it can be increased toward 2047 (1023 for SNA-SDLC systems) with consideration for the overall buffer size compared to the size of the complete HSM command message.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value ME.
Source TAK	16H or 1A+32H or 1A+48H	The source TAK encrypted under LMK pair 16-17.
Destination TAK	16H or 1A+32H or 1A+48H	The destination key encrypted under LMK pair 16-17.
MAC	8 H	The MAC generated with the source key.
Data	0 - n	The data on which to verify and generate a MAC, n = 1024 (512 for SNA-SDLC systems).
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value MF.
Error code	2 N	00 : No errors 01 : MAC verification failure 10 : Source TAK parity error 11 : Destination TAK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : Source or Destination TAK not single length
MAC	8 H	The MAC generated using the destination TAK.
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.

16.4 Generate MAC (MAB) for Large Message

Command: Generate a MAC (MAB) for a large message.

Notes: The command operates on binary data. If the HSM is set for Async/ASCII operation, ensure that:

The Host port has been set for 8 data bit operation by the CH (Configure Host) command.

The data for which the MAC is to be generated does not contain either EM (X'19) or ETX (X'03).

The value n given for Data is the recommended maximum value; it can be increased toward 2047 (1023 for SNA-SDLC systems) with consideration for the overall buffer size compared to the size of the complete HSM command message.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value MQ.
Message block number	1 N	0 : The only block. 1 : The first block. 2 : A middle block. 3 : The last block.
ZAK	16H or 1A+32H or 1A+48H	ZAK encrypted under LMK pair 26-27
IV	16 H	Initialization value, present only when message block number is 2 or 3.
Message length	3 H	Message length in bytes.
Message block	n B	The clear text message block.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value MR.
Error code	2 N	00 : No errors 02 : ZAK not single length 05 : Invalid message block number 10 : ZAK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 80 : Data length error
MAB	16 H	Used as IV for next block when message block number is 1 or 2. Used as message authenticator when message block number is 0 or 3.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

16.5 Generate MAC (MAB) using ANSI X9.19 Method for a Large Message

Command: To generate a MAB for a large message using either a TAK or a ZAK. If the key is single length use ANSI X9.9 MAC generation or if the key is double length use ANSI X9.19 MAC generation.

Notes: The command can operate on binary data or expanded Hex. If the HSM is set for Async/ASCII operation and binary data used ensure that:

The host port has been set for 8 data bit operation by the CH (Configure Host) console command.

The data for which the MAC is to be generated does not contain either EM (X'19) or ETX(X'03).

Expanded Hex mode uses 2 hexadecimal characters for each binary byte.

If the message block is the first or a middle block it must be a multiple of 8 bytes.

Consideration to the buffer size of the HSM must be made before the value n message length is selected.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	mA	(Subsequently returned to the Host unchanged).
Command Code	2A	Value MS
Message Block Number	1N	Message block processing number 0 - Only Block 1 - First Block 2 - A Middle Block 3 - Last Block
Key Type	1N	Key type 0 – TAK (Terminal Authentication Key) 1 – ZAK (Zone Authentication Key)
Key Length	1N	Key length 0 – Single Length DES Key 1 – Double Length DES Key
Message Type	1N	Message Type 0 – Message data is binary 1 – Message data is expanded Hex
Key	16 or 32H or 1A+32H	Key, encrypted under appropriate LMK pair TAK under LMK pair 16 – 17 ZAK under LMK pair 26 – 27
IV	16H	Initialization value, present only when message block number is 2 or 3.
Message Length	4H	Length of Message to be MACED (length of following field if message type binary, Half the length of the following field if expanded Hex).
Message Block	nB or H	The message block either in binary or as expanded Hex.
End Message Delimiter	1C	Optional. Must be present if a message trailer is present. Value X'19.
Message Trailer	nA	Optional. Maximum length is 32 bytes.

Field	Length & Type	Details
RESPONSE MESSAGE		
Message Header	mA	Returned to the Host unchanged.
Response Code	2A	Value MT
Error Code	2N	00 : No errors 03 : Invalid Message Type Code 04 : Invalid Key Type Code 05 : Invalid Message Block Number 06 Invalid Key Length Code 10 : KEY parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : Invalid key length 80 : Incorrect input data length
MAB	16H	Used as IV for next block when message block number is 1 or 2 Used as message authenticator when message block is 0 or 3
End Message Delimiter	1C	Optional. Must be present if a message trailer is present. Value X'19.
Message Trailer	nA	Optional. Maximum length is 32 bytes.

17 BASE24 BINARY MAC COMMANDS

Binary MAC commands, used by ACI's Base24 Release 5, allow the HSM to compute a MAC on binary data. See also the MQ command which provides a binary MAC facility.

Some Host computers cannot handle binary data in a normal async environment. When the HSM is set up for normal async the binary data is assumed to be supplied in expanded hexadecimal notation (i.e., each binary byte is converted to two hexadecimal characters). This has the effect of doubling the amount of data sent to the HSM.

Unlike the standard MAC commands, MA, MC and ME, the Binary MAC commands make no assumptions about the format or representation of the supplied MAC data; they compute a MAC on the exact binary values supplied regardless of character format. Note, however, that the keys and other values are assumed to be in hexadecimal character format. Only the MAC data field accepts binary data.

17.1 Generate a Binary MAC (Base24)

Command: Generate a MAC on binary data using a TAK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value MK.
TAK	16H or 1A+32H or 1A+48H	The TAK used to generate the MAC, encrypted under LMK 16-17.
EITHER		
For Binary Communications Modes:		
Data length	3 H	X'001 to X'320 indicating the length of the data field.
Data	n B	Data to be MACed. 1 to 800 bytes.
OR		
For Normal Async Modes:		
Data length	3 H	X'002 to X'320 indicating the length of the data field.
Data	n H	Data to be MACed. 2 to 800 hexadecimal characters representing 1 to 400 bytes.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value ML.
Error code	2 N	00 : No errors 10 : TAK parity error 12 : No keys in user storage 13 : LMK parity error 15 : Error in input data 80 : Data length error 27 : TAK not single length
MAC	8 H	The computed 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.

17.2 Verify a Binary MAC (Base24)

Command: Verify a MAC on binary data using a TAK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value MM.
TAK	16H or 1A+32H or 1A+48H	The TAK used to generate the MAC, encrypted under LMK 16-17.
MAC	8 H	The MAC to be verified.
EITHER		
For Binary Communications Modes:		
Data length	3 H	X'001 to X'320 indicating the length of the data field.
Data	n B	Data to be MACed. 1 to 800 bytes.
OR		
For Normal Async Modes:		
Data length	3 H	X'002 to X'320 indicating the length of the data field.
Data	n H	Data to be MACed. 2 to 800 hexadecimal characters representing 1 to 400 bytes.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value MN.
Error code	2 N	00 : No errors 01 : MAC did not verify 10 : TAK parity error 12 : No keys in user storage 13 : LMK parity error 15 : Error in input data 27 : TAK not single length 80 : Data length error
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.

17.3 Verify and Translate a Binary MAC (Base24)

Command: Verify a MAC on binary data using a source TAK, then recompute the MAC using a destination TAK.

Notes: If the verify fails no destination MAC is computed.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value MO.
Source TAK	16H or 1A+32H or 1A+48H	The source TAK used to verify the MAC, encrypted under LMK 16-17.
Destination TAK	16H or 1A+32H or 1A+48H	The destination TAK used to verify the MAC, encrypted under LMK 16-17.
MAC	8 H	The MAC to be verified.
EITHER		
For Binary Communications Modes:		
Data length	3 H	X'001 to X'320 indicating the length of the data field.
Data	n B	Data to be MACed. 1 to 800 bytes.
OR		
For Normal Async Modes:		
Data length	3 H	X'002 to X'320 indicating the length of the data field.
Data	n H	Data to be MACed. 2 to 800 hexadecimal characters representing 1 to 400 bytes.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value MP.
Error code	2 N	00 : No errors 01 : MAC did not verify 10 : Source TAK parity error 11 : Destination TAK parity error 12 : No keys loaded in user storage 13 : LMK parity error 15 : Error in input data 27 : Source or destination TAK not single length 80 : Data length error
MAC	8 H	The computed 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.

18 USER STORAGE SUPPORT

The standard speed HSM contains 8192 bytes of memory allocated to the storage of keys and tables. The high speed HSM contains 98304 bytes of memory allocated to the storage of keys and tables. The Configure Security (CS) console command sets the block size for user storage locations.

The data can be loaded and read from this storage by the Host. This facility can be used to reload the contents after a power-down, a reset, or after batch solicitation data processing. In addition, a facility is provided to verify a Diebold table held in user storage.

18.1 Load Data to User Storage

Command: Load data to user storage.

Notes: Each block of data is 16 or 32 or 48 characters long (enough for one single, double or triple key) and this command can load a maximum of 32 blocks of data. If the block size is set to a larger setting than the data to be loaded the data should be padded with F to fill the block.

Ensure that the location within user storage does not conflict with any Diebold table already loaded.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value LA.
Index flag	1 A	Value K.
Index address	3 H	The 3-digit address identifying the first location at which to store the data.
Block count	2 H	The hexadecimal count of the number of blocks of data (0 to X'20).
Block 1	16H or 32H or 48H	The first encrypted key or other data
.	.	.
.	.	.
Last block	16H or 32H or 48H	The last encrypted key or other data.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value LB.
Error code	2 N	00 : No errors 15 : Error in input data 21 : Invalid user storage index
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.

18.2 Read Data from User Storage

Command: Read data from user storage.

Notes: Each block of data is 16 or 32 or 48 characters long (enough for one single, double or triple key), and this command can return a maximum of 32 blocks of data.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value LE.
Index flag	1 A	Value K.
Index address	3 H	The 3-digit address identifying the first location at which to read the data.
Block count	2 H	The hexadecimal count of the number of blocks of data (0 to X'20).
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value LF.
Error code	2 N	00 : No errors 12 : No data loaded in user storage 15 : Error in input data 21 : Invalid user storage index
Block 1	16H or 32H or 48H	The first encrypted key or other data.
.	.	.
.	.	.
.	.	.
Last block	16H or 32H or 48H	The last encrypted key or other 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.

18.3 Verify the Diebold Table in User Storage

Command: Verify the Diebold table held in user storage.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value LC.
Index flag	1 A	Value K.
Index address	3 H	The address of the start of the Diebold table for validation.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value LD.
Error code	2 N	00 : No errors 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 19 : Diebold table invalid 21 : Invalid user storage index
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.

19 PRINT OUTPUT FORMATTING

Forms for conveying and protecting PINs and keys can be produced on a printer attached to the HSM Auxiliary port of an RG7X00 series HSM (or an RG7X10 High-Speed HSM supplied with a print facility to special order). The documents are printed at the terminal in response to a command from the Host, as defined elsewhere in this manual.

Before using the HSM printer commands it is necessary to define the format of the mailer or document. The definition data is stored in the HSM until power is removed, or until a reset is performed. The PA and PC commands are used to send formatting symbols to the HSM. The formatting symbols for defining the print fields and any constant literals are given in the table that follows the two-up and one-up examples.

Use the PA command to create the mailer format. The PC command is a continuation of the PA command, used only if the format definition is too long to fit in a single message (i.e., the PA command exceeds the Host's maximum output record size).

The format definition can contain up to 299 formatting symbols and constants.

Example 1

Print Format for Two-up Mailers:

	. + 1 + 2 + 3 + 4 + 5 + 6		
1	THOMAS M SMITH		JOHN R JONES
2	APT 4B	1782	427 WEST 9 th ST
3	39 ELM DR		3690
4	MEDIA PA 19063		WAYNE PA 19132
5			
6	THANK YOU		THANK YOU
7			

Formatting symbols in PA command:

```
>L>003^0>033^4>L>003^1>023^P>033^5>053^Q>L>003^2>033^6>L>003^3>0
33^7>L>L>003THANK YOU>033THANK YOU>L>F
First line: >L>003^0>033^4
Second line: >L>003^1>023^P>033^5>053^Q
Third line: >L>003^2>033^6
Fourth line: >L>003^3>033^7
Fifth line: >L
Sixth line: >L>003THANK YOU>033THANK YOU
Seventh line: >L
Form feed: >F
```

Example 2**Print Format for One-up Mailers:**

.... + 1 + 2 + 3 + 4 + 5 + 6

1	THOMAS M SMITH	
2	APT 4B	1782
3	39 ELM DR	
4	MEDIA PA 19063	
5	YOUR FULL SERVICE BANK	
6		
1	JOHN R JONES	
2	427 WEST 9 th ST	3690
3	WAYNE PA 19132	
4		
5	YOUR FULL SERVICE BANK	
6		

Formatting symbols in PA command:

>L>013^0>L>013^1>041^P>L>013^2>L>013^3>L>013 YOUR FULL SERVICE
BANK>L>F>

First line: >L>013^0

Second line: >L>013^1>041^P

Third line: >L>013^2

Fourth line: >L>013^3

Fifth line: >L>013YOUR FULL SERVICE BANK

Sixth line: >L

Form feed: >F

Symbol	EBCDIC	ASCII	Meaning
>L	6E D3	3E 4C	Line feed, carriage return.
>V	6E E5	3E 56	Vertical tab.
>H	6E C8	3E 48	Horizontal tab.
>F	6E C6	3E 46	Form feed.
>nnn	6E Fn Fn Fn	3E 3n 3n 3n	Skip column nnn in relation to left margin, where nnn is a 3-digit decimal number.
^M	5F D6	5E 49	For a key document, print third clear component.
^P	5F D7	5E 50	For a PIN mailer, print clear PIN for mailer 1. For a key document, print clear component.
^Q	5F D8	5E 51	For a PIN mailer, print clear PIN for mailer 2. For a key document, print clear component or encrypted TMK (only one-up printing allowed for key documents).
^R	5F D9	5E 52	Print reference number for PIN mailer 1.
^S	5F E2	5E 53	Print reference number for PIN mailer 2.
^T	5F E3	5E 54	Print last 6 account number digits on PIN mailer 1.
^U	5F E4	5E 55	Print last 6 account number digits on PIN mailer 2.
<L><hh hh hh ..>	6A <L> <hh hh hh ..>	7C <L> <hh hh hh ..>	Send binary data to printer for example printer control string. character followed by the length of the string in bytes <L> 0 - F then the expanded hex string <hh hh ..>.
^0	5F F0	5E 30	Insert Print Field 0.
^1	5F F1	5E 31	Insert Print Field 1.
^2	5F F2	5E 32	Insert Print Field 2.
.	.	.	.
.	.	.	.
^F	5F C6	5F 46	Insert Print Field 15.

Print Formatting Symbols

19.1 Printing PINs in Word Format

Two print formatting symbols are provided for printing PINs in word format.

For example:

ONE TWO THREE FOUR.

English is used as the default setting. The symbols can be used in addition to the symbols for printing PINs in numeric format (e.g., 1234).

Symbol	EBCDIC	ASCII	Meaning
^V	5F E3	5E 56	Print the clear PIN in word format for mailer 1. Can be used for either a one-up or a two-up PIN mailer. e.g., ONE TWO THREE FOUR
^W	5F E6	5E 57	Print the clear PIN in word format for mailer 2. Can be used only for a two-up PIN mailer. e.g., ONE TWO THREE FOUR

Print Formatting Symbols for Printing PINs in Word Format

19.2 Printing PINs in Columns

Four print formatting symbols are provided for printing PINs (both words and numerics) in columns. For example:

1	ONE
2	TWO
3	THREE
4	FOUR

For the following definition of print symbols an n is used to indicate which digit of a PIN is to be printed. The relationship between PIN digits and n is as follows:

PIN Digit	1	2	3	4	5	6	7	8	9	10	11	12
'n'	1	2	3	4	5	6	7	8	9	A	B	C

Symbol	EBCDIC	ASCII	Meaning
^{^Pn}	5F D7 F1-F9 or C1-C3	5E 50 31-39 or 41-43	Print the clear PIN digit n in number format for mailer 1. Can be used for either a one-up or a two-up PIN mailer. e.g., 1
^{^Qn}	5F D8 F1-F9 or C1-C3	5E 51 31-39 or 41-43	Print the clear PIN digit n in number format for mailer 2. Can be used only for two-up PIN mailer. e.g., 1
^{^Vn}	5F E3 F1-F9 or C1-C3	5E 56 31-39 or 41-43	Print the clear PIN digit n in word format for mailer 1. Can be used for either a one-up or a two-up PIN mailer. e.g., ONE
^{^Wn}	5F E6 F1-F9 or C1-C3	5E 57 31-39 or 41-43	Print the clear PIN digit n in word format for mailer 2. Can be used only for two-up PIN mailer. e.g., ONE

Print Formatting Symbols for Printing PINs in Columns

19.3 Load Formatting Data to HSM

Command: Load formatting data to the HSM.

Notes: The HSM can store a maximum of 299 symbols and constants.

Not available as part of the standard command set in the RG7X10 series of High-Speed HSMs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value PA.
Data	n A	Symbols and constants defined in Print Formatting Symbols Tables.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value PB.
Error code	2 N	00 : No errors
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.

19.4 Load Additional Formatting Data to HSM

Command: Load additional formatting data to the HSM.

Notes: The PC command must be preceded by a PA command.

The HSM can store a maximum of 299 symbols and constants including the data sent with the PA command.

Not available as part of the standard command set in the RG7X10 series of High-Speed HSMs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value PC.
Data	n A	Symbols and constants defined in Print Formatting Symbols Tables.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value PD.
Error code	2 N	00 : No errors
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.

19.5 Load a PIN Text String

Command: Load a PIN text string.

Notes: The default PIN text string, used by the HSM when printing PINs in words is initialised at Cold-Start to English (ONE, TWO, THREE,). The Load PIN Text String command can be used to re-define the text string which is then stored in battery-backed not tamper-protected memory.

When re-defining the text strings, strings for all characters (0 to 9) must be supplied.

The value for the length fields can be in the range 0,1,2,... to F (Hex), with 0 representing length 16_{10} .

Not available as part of the standard command set in the RG7X10 series of High-Speed HSMs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value LJ.
Length	1 H	The length of the string for Character 0.
Character 0	n B	The text string representing Character 0.
Length	1 H	The length of the string for Character 1.
Character 1	n B	The text string representing Character 1.
Length	1 H	The length of the string for Character 2.
Character 2	n B	The text string representing Character 2.
Length	1 H	The length of the string for Character 3.
.	.	.
.	.	.
.	.	.
Character 9	n B	The text string representing Character 9.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value LJ.
Error code	2 N	00 : No errors 15 : Error in input 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.

20 TRANSLATE DATA AFTER CHANGE OF LOCAL MASTER KEYS

Much of the data held by the Host is encrypted under specific LMK pairs. If the value of a pair changes, the associated data cannot be used until it has been translated. To do this a facility is provided for the storage of the old LMK pair within the HSM. This storage location is known as "Key Change Storage".

When the old pair has been saved in key change storage, and the new pair loaded in the standard LMK storage, all data held on the Host, encrypted under the old LMK pair must be sent to the HSM for translation. Commands are provided for translating each type of key and PINs encrypted for Host storage.

20.1 Translate a ZMK

Command: Translate a ZMK encrypted under the LMK pair held in "key change storage" to encryption under LMK pair 04-05.

Note: If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value GE.
ZMK	16H or 32H or 1A+32H or 1A+48H	The ZMK encrypted under the LMK pair held in "key change storage".
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";" If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value GF.
Error code	2 N	00 : No errors 10 : ZMK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
ZMK	16H or 32H or 1A+32H or 1A+48H	The ZMK translated to encryption under LMK pair 04-05.
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.

20.2 Translate a ZPK

Command: Translate a ZPK encrypted under the LMK pair held in “key change storage” to encryption under LMK pair 06-07.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value KC.
ZPK	16H or 1A+32H or 1A+48H	The ZPK encrypted under the LMK pair held in “key change storage”.
Delimiter	1 A	Optional. If present the following three fields must be present. Value “;”. If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value KD.
Error code	2 N	00 : No errors 10 : ZPK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
ZPK	16H or 1A+32H or 1A+48H	The ZPK translated to encryption under LMK pair 06-07.
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.

20.3 Translate a TMK, TPK or PVK

Command: Translate a TMK, TPK or PVK encrypted under the LMK pair held in “key change storage” to encryption under LMK pair 14-15.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value AA.
TMK, TPK or PVK	16H or 1A+32H or 1A+48H	The TMK, TPK or PVK encrypted under the LMK pair held in “key change storage”.
Delimiter	1 A	Optional. If present the following three fields must be present. Value “;”. If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value AB.
Error code	2 N	00 : No errors 10 : TMK, TPK or PVK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
TMK, TPK or PVK	16H or 1A+32H or 1A+48H	The TMK, TPK or PVK translated to encryption under LMK pair 14-15.
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.

20.4 Translate a TAK

Command: Translate a TAK encrypted under the LMK pair held in “key change storage” to encryption under LMK pair 16-17.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value AC.
TAK	16H or 1A+32H or 1A+48H	The TAK encrypted under the LMK pair held in “key change storage”.
Delimiter	1 A	Optional. If present the following three fields must be present. Value “;”. If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value AD.
Error code	2 N	00 : No errors 10 : TAK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
TAK	16H or 1A+32H or 1A+48H	The TAK translated to encryption under LMK pair 16-17.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

20.5 Translate a PIN and PIN Length

Command: Translate a PIN and/or PIN length from encryption under the LMK pair held in “key change storage” to encryption under LMK pair 02-03. Also, translate the PIN length if a new value has been selected.

Notes: The command can be used to translate the PIN length only. In this case, load the same LMKs to “key change storage” that are loaded as the current LMK.

The PIN length is L_2N for PIN encryption algorithm A, and L_2H for PIN encryption algorithm B, as selected by the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value BG.
Account number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN	L_1N or L_1H	The PIN encrypted under the LMK pair in “key change storage”, where L_1 is the old encrypted PIN length.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value BH.
Error code	2 N	00 : No errors 13 : LMK error; report to supervisor 14 : Error in PIN from Host database 15 : Error in input data
PIN	L_2N or L_2H	The PIN encrypted under new LMK pair 02-03, where L_2 is the new encrypted PIN length.
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.

20.6 Translate Keys from Old LMK to New LMK

Command: Translate keys from encryption under the LMK held in “key change storage” to encryption under a new LMK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value BW.
Key type code	2 N	Indicates the LMK under which the key is encrypted: 00 : LMK pair 04-05 01 : LMK pair 06-07 02 : LMK pair 14-15 03 : LMK pair 16-17 04 : LMK pair 18-19 05 : LMK pair 20-21 06 : LMK pair 22-23 07 : LMK pair 24-25 08 : LMK pair 26-27 09 : LMK pair 28-29 0A : LMK pair 30-31 0B : LMK pair 32-33 10 : Variant 1 of LMK pair 04-05 42 : Variant 4 of LMK pair 14-15 FF : Use key type specified after delimiter
Key length flag	1 N	0 for single-length key, 1 for double-length key, 3 for triple-length key
Key	16H or 32H or 1A+32H or 1A+48H	Key encrypted under old LMK held in “key change storage”.
Delimiter	1 A	Optional. Only present if following field present. Value “;”.
Key type	3 H	See key type table.
Delimiter	1 A	Optional. If present the following three fields must be present. Value “;”. If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value BX.
Error code	2 N	00 : No errors 04 : Invalid key type code 05 : Invalid key length flag 10 : Key parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
Key	16H or 32H or 1A+32H or 1A+48H	Key encrypted under the new LMK.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

20.7 Erase the Key Change Storage

Command: Erase the key change storage area of memory.

Notes: It is recommended that this command is used after keys stored by the Host have been translated from old to new LMKs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value BS.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value BT.
Error code	2 N	00 : No errors
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.

21 MISCELLANEOUS COMMANDS

The following miscellaneous commands are supported by the HSM:

- Cancel the Authorized state.
- Generate a check value for a given key.
- Set HSM response delay.
- Perform diagnostics and obtain LMK check value.

21.1 Cancel the Authorised State

Command: Cancel the Authorised state.

Notes: The command should be used whenever the application has completed the current requirement for the Authorised state.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RA.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value RB.
Error code	2 N	00 : No errors
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.

21.2 Generate a Key Check Value (Not Double-Length ZMK)

Command: Generate a key check value for one of the following:

ZMK (single-length), ZPK, TMK, TPK, PVK, TAK

Notes: The command can be used to verify a key received from another party. The HSM generates the value by encrypting 64 binary zeroes under the key.

This command does not support the use of double-length ZMKs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value KA.
Encrypted key	16H or 1A+32H or 1A+48H	One of the following: ZMK, ZPK, TMK, TPK, PVK or TAK encrypted under the relevant LMK pair.
Key type code	2 N	The key type identifier: 00 : ZMK 01 : ZPK 02 : TMK, TPK or PVK 03 : TAK
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value KB.
Error code	2 N	00 : No errors 10 : Encrypted key parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
Key check value	16 H or 6 H	The check value for the given key. Calculated by encrypting 64 binary zeroes under the key. 16H or 6H depends upon KCV type option.
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.

21.3 Generate a Key Check Value

Command: Generate a check value for a key encrypted under a specified LMK pair.

Note: See key table for key useage.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value BU.
Key type code	2 N	Indicates the LMK under which the key is encrypted (see key table): 00 : LMK pair 04-05 01 : LMK pair 06-07 02 : LMK pair 14-15 03 : LMK pair 16-17 04 : LMK pair 18-19 05 : LMK pair 20-21 06 : LMK pair 22-23 07 : LMK pair 24-25 08 : LMK pair 26-27 09 : LMK pair 28-29 0A : LMK pair 30-31 0B : LMK pair 32-33 10 : Variant 1 of LMK pair 04-05 42 : Variant 4 of LMK pair 14-15 FF : Use key type specified after delimiter
Key length flag	1 N	0 for single-length key, 1 for double-length key, 2 for triple length key.
Key	16H or 1A+32H or 1A+48H	Key encrypted under the specified LMK.
Delimiter	1 A	Optional. Only present if following field present. Value ;
Key type	3 H	See key type table.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ;. If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method: 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value BV.
Error code	2 N	00 : No errors 04 : Invalid key type code 05 : Invalid key length flag 10 : Key parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
Key check value	16 H or 6 H	Result of encrypting 64 binary zeroes with the key. 16H or 6H depends upon KCV type option.
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.

21.4 Set HSM Response Delay

Command: Set the delay for which the HSM waits before it responds to a command

Notes: The command enables the Host to delay HSM output. This is for Host ports that are half duplex and require time to reconfigure from output to input mode.

The delay duration is from 0 to 255ms. The value is treated as MOD 256, so a setting of 256 results in a delay of 0.

The delay is not implemented until after the response to this command.

If the HSM is configured to any host configuration other than async, this command has no effect.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value LG.
Delay	3 N	Value 000 to 255.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value LH.
Error code	2 N	00 : No errors 15 : Error in input 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.

21.5 Perform Diagnostics

Command: Test the processor, firmware PROMs and the LMK pairs. Return the LMK check value.

Notes: The check value is the same as the value returned for the Console V command.

The Host system should time the NC command and generate an appropriate system message if a response is not received within 5 seconds. If an error is detected in the processor, HSM functions are suspended, and no message is returned to the Host.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value NC.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value ND.
Error code	2 N	00 : No errors 13 : LMK error; report to supervisor 40 : Firmware PROM error 41 : Hardware/software error 42 : DES crypto-processor failure
LMK check	16 H	The LMK check value.
Firmware number	9 A	The firmware reference number in the form: xxxx-xxxx This is the value returned for the Console VR command.
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.

21.6 HSM Status

Command: To return HSM status information

Notes: Mode 00 available all others reserved for future use

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value NO.
Mode flag	2 H	Mode Flag: 00 - Return status information 01 - : Reserved for future use FF -
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value NP.
Error code	2 N	00 : No errors 13 : LMK error; report to supervisor 15 : Error in input data
Mode 00		
I/O buffer size	1 N	I/O buffer size 0 - 2k 1 - 8k 2 - 16k 3 - 32k
Ethernet type	1 N	Type of Ethernet connection 0 - UDP 1 - TCP
Number of TCP Sockets	1 N	Number of TCP sockets configured
Firmware number	9 A	The firmware reference number in the form: xxxx-xxxx
DSP fitted	1 N	DSP fitted 0 - No 1 - Yes
DSP firmware number	4 A	DSP firmware number
Mode 01 - FF Reserved for future use		
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.

22 VISA CARD VERIFICATION VALUES

The CVV commands can also be used to generate and verify CVV2 and Mastercard CVC.

22.1 Generate a CVK Pair

Command: Generate a VISA CVK pair. Output the key pair encrypted under a variant of LMK pair 14-15.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value AS.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. If present must be 0.
Key scheme LMK	1 A	Optional. If present must be 0 or U.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. Not available for keys generated using new schemes 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value AT.
Error code	2 N	00 : No errors 13 : LMK error; report to supervisor 15 : Error in input data
CVK Key scheme = 0 or not specified		
CVK A	16 H	CVK A encrypted under a variant 4 of LMK pair 14-15.
CVK B	16 H	CVK B encrypted under a variant 4 of LMK pair 14-15.
CVK Key scheme not 0		
CVK A/B	1A + 32H	CVK A/B encrypted under a variant 4 of LMK pair 14-15.
KCV Type = 0 or not specified		
CVK A check value	6 H	The CVK A check value.
CVK B check value	6 H	The CVK B check value.
For KCV Type =1		
CVK A/B check value	6 H	The CVK A/B check value
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.

22.2 Translate a CVK Pair from LMK to ZMK Encryption

Command: Translate a CVK pair from encryption under a variant of LMK pair 14-15 to encryption under a ZMK.

Notes: If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value AU.
ZMK	16H or 32H or 1A+32H or 1A+48H	ZMK encrypted under LMK pair 04-05.
CVK A / B	32H or 1A+32H	CVK A / B encrypted under a variant 4 of LMK pair 14-15.
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. Not available for keys generated using new schemes 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value AV.
Error code	2 N	00 : No errors 10 : ZMK parity error 11 : CVK A or B parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : Incompatible key length
CVK A / B	32H or 1A+32H	CVK A/B encrypted under ZMK
KCV Type = 0 or not specified		
CVK A check value	6 H	The CVK A check value.
CVK B check value	6 H	The CVK B check value.
KCV Type = 1		
Key check value	6 H	Result of encrypting 64 binary zeros with the key
End message delimiter	1 C	Present only if present in the command message, value X'19
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

22.3 Translate a CVK Pair from ZMK to LMK Encryption

Command: Translate a CVK pair from encryption under a ZMK to encryption under a variant of LMK pair 14-15.

Notes: If a 32-character ZMK is required, the HSM must be configured for double-length ZMKs using the CS (Configure Security) console command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value AW.
ZMK	16 H or 32 H	ZMK encrypted under LMK pair 04-05.
CVK A / B	32H or 1A+32H	CVK A encrypted under the ZMK.
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method: 0 - KCV backwards compatible. Not available for keys generated using new schemes 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value AX.
Error code	2 N	00 : No errors 10 : ZMK parity error 11 : CVK A or B parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
CVK A / B	32H or 1A+32H	CVK A / B encrypted under a variant 4 of LMK pair 14-15.
KCV Type = 0 or not specified		
CVK A check value	6 H	The CVK A check value.
CVK B check value	6 H	The CVK B check value.
KCV Type = 1		
Key check value	6 H	Result of encrypting 64 binary zeros with the key
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

22.4 Translate a CVK Pair from Old LMK to New LMK Encryption

Command: Translate a CVK pair from encryption under a variant 4 of an old LMK pair 14-15 to encryption under a variant 4 of a new LMK pair 14-15.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value AY.
CVK A / B	32H or 1A+32H	CVK A / B pair encrypted under a variant 4 of the old LMK pair 14-15.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value AZ.
Error code	2 N	00 : No errors 10 : CVK A or B parity error 11 : ZPK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
CVK A / B	32H or 1A+32H	CVK A / B encrypted under a variant of LMK pair 14-15.
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.

22.5 Generate a VISA CVV

Command: Generate a VISA CVV for encoding on a card.

Notes: Used to generate Track 1 or Track 2 CVVs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value CW.
CVK A / B	32H or 1A+32H	VISA CVK A / B encrypted under a variant 4 of LMK pair 14-15.
Primary account number	n N	The primary account number for the card.
Delimiter	1 A	Value ";".
Expiration date	4 N	The card expiration date.
Service code	3 N	The card service code.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value CX.
Error code	2 N	00 : No errors 10 : CVK A or CVK B parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : CVK not double length
CVV	3 N	CVV to be encoded on card.
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.

22.6 Verify a VISA CVV

Command: Verify a VISA CVV.

Notes: The command issue to verify Track 1 or Track 2 CVVs.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value CY.
CVK A / B	32H or 1A+32H	VISA CVK A / B encrypted under a variant 4 of LMK pair 14-15.
CVV	3 N	CVV for verification.
Primary account number	n N	The primary account number for the card.
Delimiter	1 A	Value ";".
Expiration date	4 N	The card expiration data.
Service code	3 N	The card service code.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value CZ.
Error code	2 N	00 : No errors 01 : CVV failed verification 10 : CVK A or B parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : CVK not double length
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.

23 VISA CASH SYSTEM

The HSM supports the functions to load and unload value from Visa Cash cards.

Notes:

The use of the ALGL_{IEP} and VKL_{IEP} fields in following commands deserves special mention as these fields are optional. There are 3 scenarios controlled by these fields.

Scenario	Applicable Visa Cash cards	Single or Double length KDL used	Additional Notes
Neither VKL _{IEP} or ALGL _{IEP} supplied to HSM	Version 1.5 and earlier DES cards	Single	May be used with cards which do not report VKL _{IEP} or ALGL _{IEP} . Backwards compatible with earlier versions of HSM firmware
Only VKL _{IEP} supplied to HSM	Version 1.6 DES cards and Public Key cards	Double	May be used with later cards. Host must determine the value of ALGL _{IEP} and supply VKL _{IEP} if required. Backwards compatible with earlier versions of HSM firmware
Both VKL _{IEP} and ALGL _{IEP} supplied to HSM	Any card.	Single if ALGL _{IEP} has value 01, double if ALGL _{IEP} has value 04	Allows host to send both ALGL _{IEP} and VKL _{IEP} without concern about their values. VKL _{IEP} must always be supplied as a placeholder even if its value is not relevant (i.e. when ALGL _{IEP} is of value 01)

This set of scenarios accommodates all relevant combinations of Visa Cash cards and allows the host application to operate in one of two modes.

Host makes the decision about what ALGL_{IEP} is relevant for the current transaction and either supplies VKL_{IEP} if ALGL_{IEP} is of value 04, or does not supply VKL_{IEP} if ALGL_{IEP} is of value 01. ALGL_{IEP} itself is not sent to the HSM. Thus the first and second scenarios in the above table can be used to cater for all cards in use. This mode of operation is used by some (earlier) host systems and therefore must be supported for backwards compatibility. Note that earlier Visa Cash cards do not report a value of ALGL_{IEP} and so the host may have to determine this in other ways. Reference 4 discusses this point.

Host simply passes values of ALGL_{IEP} and VKL_{IEP} to HSM as supplied in the current transaction. Thus if a card does not supply ALGL_{IEP} or VKL_{IEP} no values are passed to the HSM and vice versa. Thus the first and third scenarios in the above table will be used. In this mode of operation the host is not required to make any decisions about the transaction; these are left to the HSM.

If Visa specifies alternative processing requirements in the future (and hence values of ALGL_{IEP} other than 1 or 4) the HSM will be upgraded to accommodate them.

The earlier Visa Cash cards which do not report ALGL_{IEP} or VKL_{IEP} will all eventually expire making the first scenario in the above table redundant.

23.1 Generate and Export a *KML

Command: Generate a double-length Master Load Key (*KML) and return it encrypted under Variant 2 of LMK pair 04-05, and also under a double length Zone Control Master Key (*ZCMK).

Notes: A check value for the *KML is also returned.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value DI.
*ZCMK	32H or 1A+32H or 1A+48H	*ZCMK encrypted under LMK pair 04-05.
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value DJ.
Error code	2 N	00 : No errors 10 : *ZCMK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : *KML not double length
*KML (*ZCMK)	32H or 1A+32H	*KML, encrypted under *ZCMK.
*KML (LMK)	32H or 1A+32H	*KML, encrypted under Variant 2 of LMK pair 04-05.
*KML check value	6 H	Check value formed by encrypting a block of 64 binary zeros with the *KML and returning the 24 left-most bits of the result.
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.

23.2 Import a *KML

Command: Translate a double-length Master Load Key (*KML) from encryption under a Zone Master Key (*ZCMK) to encryption under Variant 2 of LMK pair 04-05.

Notes: A check value for the *KML is also returned.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value DK.
*ZCMK	32H or 1A+32H or 1A+48H	*ZCMK encrypted under LMK pair 04-05.
*KML	32H or 1A+32H	*KML, encrypted under *ZCMK.
Atalla variant	1 N or 2 N	Optional. Atalla variant; for use in systems with Atalla equipment.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value DL.
Error code	2 N	00 : No errors 10 ; *ZCMK parity error 11 : *KML parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : *KML not double length
*KML	32H or 1A+32H	*KML, encrypted under Variant 2 of LMK pair 04-05.
*KML check value	6 H	Check value formed by encrypting a block of 64 binary zeros with the *KML and returning the left-most 24 bits of the result.
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.

23.3 Verify Load Signature S₁ and Generate Load Signature S₂

Command: Verify Load Signature S₁ and generate Load Signature S₂.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value DM.
*KML	32H or 1A+32H	*KML, encrypted under Variant 2 of LMK pair 04-05.
BIN _{IEP}	6 H	IEP Issuer Visa assigned BIN.
ID _{IEP}	10 H	IEP Serial number.
DEXP _{IEP}	6 H	IEP Expiration date (YYMMDD format).
NT _{IEP}	4 H	IEP Transaction counter.
M _{LDA}	8 H	Amount to be loaded.
CURR _{LDA}	4 H	Load device currency code.
CEXP _{LDA}	2 H	Load device currency exponent.
BAL _{IEP}	8 H	IEP Current balance.
ID _{ACQ}	8 H	Acquirer BIN.
R	8 H	Random number.
S ₁	16 H	Load request signature for validation.
VKL _{IEP}	2 H	Optional. Load Key version. If present but ALGL _{IEP} not present, then a double length KDL will be used; see Notes in Introduction. Must be present if ALGL _{IEP} is present.
ALGL _{IEP}	2 H	Optional. Load Algorithm. Can only take the values 01 and 04. If set to 01 a single length KDL is used and VKL _{IEP} is ignored. If 04, a double length KDL is used and VKL _{IEP} is used.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value DN.
Error code	2 N	00 : No errors 01 : S ₁ verification failure 03 : Invalid ALGL _{IEP} 10 : *KML parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : *KML not double length
S ₂	16 H	Returned load 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.

23.4 Verify Load Completion Signature S₃

Command: Verify Load Completion Signature S₃.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value DO.
*KML	32H or 1A+32H	*KML, encrypted under Variant 2 of LMK pair 04-05.
BIN _{IEP}	6 H	IEP Issuer Visa assigned BIN.
ID _{IEP}	10 H	IEP Serial number.
DEXP _{IEP}	6 H	IEP Expiration date (YYMMDD format).
NT _{IEP}	4 H	IEP Transaction counter.
ID _{ACQ}	8 H	Acquirer BIN.
R	8 H	Random number.
CC _{IEP}	4 H	Completion code.
S ₃	16 H	Load completion signature for validation.
VKL _{IEP}	2 H	Optional. Load Key version. If present but ALGL _{IEP} not present, then a double length KDL will be used; see Notes in Introduction. Must be present if ALGL _{IEP} is present.
ALGL _{IEP}	2 H	Optional. Load Algorithm. Can only take the values 01 and 04. If set to 01 a single length KDL is used and VKL _{IEP} is ignored. If 04, a double length KDL is used and VKL _{IEP} is used.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value DP.
Error code	2 N	00 : No errors 01 : S ₃ verification failure 03 : Invalid ALGL _{IEP} 10 : *KML parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : *KML not double length
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.

23.5 Verify Unload Signature S₁ and Generate Unload Signature S₂

Command: Verify Unload Signature S₁ and generate Unload Signature S₂.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value DQ.
*KML	32H or 1A+32H	*KML, encrypted under Variant 2 of LMK pair 04-05.
BIN _{IEP}	6 H	IEP Issuer Visa assigned BIN.
ID _{IEP}	10 H	IEP Serial number.
DEXP _{IEP}	6 H	IEP Expiration date (YYMMDD format).
NT _{IEP}	4 H	IEP Transaction counter.
M _{LDA}	8 H	Amount to be unloaded.
CURR _{LDA}	4 H	Load device currency code.
CEXP _{LDA}	2 H	Load device currency exponent.
BAL _{IEP}	8 H	IEP Current balance.
ID _{ACQ}	8 H	Acquirer BIN.
R	8 H	Random number.
S ₁	16 H	Unload request signature for validation.
VKL _{IEP}	2 H	Optional. Load Key version. If present but ALGL _{IEP} not present, then a double length KDL will be used; see Notes in Introduction. Must be present if ALGL _{IEP} is present.
ALGL _{IEP}	2 H	Optional. Load Algorithm. Can only take the values 01 and 04. If set to 01 a single length KDL is used and VKL _{IEP} is ignored. If 04, a double length KDL is used and VKL _{IEP} is used.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value DR.
Error code	2 N	00 : No errors. 01 : S ₁ verification failure 03 : Invalid ALGL _{IEP} 10 : *KML parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index. 27 : *KML not double length
S ₂	16 H	Returned unload 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.

23.6 Verify Unload Completion Signature S₃

Command: Verify Unload Completion Signature S₃.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value DS.
*KML	32H or 1A+32H	*KML, encrypted under Variant 2 of LMK pair 04-05.
BIN _{IEP}	6 H	IEP Issuer Visa assigned BIN.
ID _{IEP}	10 H	IEP Serial number.
DEXP _{IEP}	6 H	IEP Expiration date (YYMMDD format).
NT _{IEP}	4 H	IEP Transaction counter.
ID _{ACQ}	8 H	Acquirer BIN.
R	8 H	Random number.
CC _{IEP}	4 H	Completion code.
S ₃	16 H	Unload completion signature for validation.
VKL _{IEP}	2 H	Optional. Load Key version. If present but ALGL _{IEP} not present, then a double length KDL will be used; see Notes in Introduction. Must be present if ALGL _{IEP} is present.
ALGL _{IEP}	2 H	Optional. Load Algorithm. Can only take the values 01 and 04. If set to 01 a single length KDL is used and VKL _{IEP} is ignored. If 04, a double length KDL is used and VKL _{IEP} is used.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Return to the Host unchanged.
Response code	2 A	Value DT.
Error code	2 N	00 : No errors 01 : S ₃ verification failure 03 : Invalid ALGL _{IEP} 10 : *KML parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : *KML not double length
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.

24 CHIP CARD

This section specifies the Host Security Module functionality which is needed to support on-line transaction processing for the various payment schemes under the EMV umbrella. Whilst EMV specifies most of the details pertaining to cards and terminals, the individual schemes have defined their own cryptographic processes for on-line authorisation functions.

There are three functions supported:

- A function which will validate ARQC (or TC/AAC) or generate ARPC (or perform both in one call)
- A function to verify a Data Authentication Code or a Dynamic Number
- Generate Secure Message with Integrity and optional Confidentiality

These functions have been designed to be as general purpose as possible.

Key Naming Conventions

The various schemes have adopted different naming conventions for the keys used. For consistency the following convention is used:

Key Description	Name used in this specification	VSDC/UKIS name used	Europay/Master Card name used
Master Key for Authentication Cryptograms	MK-AC	DMK	Issuer MK
Master Key for Secure Messaging Integrity	MK-SMI	DMK	Issuer MK
Master Key for Secure Messaging Confidentiality	MK-SMC	DMK	Issuer MK
Master Key for Data Authentication Codes	MK-DAC	-	Issuer MK
Master Key for Dynamic Numbers	MK-DN	-	Issuer MK
Derived Key for Authentication Cryptograms	DK-AC	UDK	ICC MK
Derived Key for Secure Messaging Integrity	DK-SMI	UDK	ICC MK
Derived Key for Secure Messaging Confidentiality	DK-SMC	UDK	ICC MK
Derived Key for Dynamic Numbers	DK-DN	-	ICC MK

24.1 ARQC (or TC/AAC) Verification and/or ARPC Generation

Command: Validate an ARQC (or TC/AAC) and, optionally, generate an ARPC.
 Alternatively, the command can be used to generate an ARPC alone. This function is a general purpose command which will validate an ARQC, TC or AAC.

Notes: Diagnostic data is produced by this command only if the HSM is in Authorised State.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value KQ.
Mode Flag	1 H	Mode of operation: 0 = Perform ARQC verification only 1 = Perform ARQC Verification and ARPC generation 2 = Perform ARPC Generation only
Scheme ID	1 H	Identifier of the EMV scheme; 0 = Visa VSDC or UKIS 1 = Europay or MasterCard M/Chip
*MK-AC(LMK)	32H or 1A+32H	The Issuer Master Key for Application Cryptograms encrypted under Variant 1 of LMK pair 28-29.
PAN/PAN Sequence No	8 B	Pre-formatted PAN/PAN Sequence No.
ATC	2 B	Application Transaction Counter. Present for all modes. Any two byte value must be supplied, though it is not used, for Scheme ID = 0.
UN	4 B	Unpredictable Number. Present for all modes. Any four byte value must be supplied, though it is not used, for Scheme ID = 0
Transaction Data Length	2 H	Length of next field. Can be any length from 1 to 255 bytes. Only present for Modes 0 and 1.
Transaction Data	n B	Variable length data. Only present for Modes 0 and 1. If the data supplied is a multiple of 8 bytes, no extra padding is added. If it is not a multiple of 8 bytes additional zero padding is added.
Delimiter	1A	Delimiter, to indicate end of Transaction Data, value “;”. Only present for Modes 0 and 1.
ARQC/TC/AAC	8 B	ARQC/TC/AAC to be validated and/or used for ARPC generation. Present for both Mode 0,1 and 2.
ARC	2 B	Authorization Response Code to be used for ARPC Generation. Not required for Mode 0. Must be present for Mode 1 and Mode 2.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value KR.
Error Code	2 N	00 : No error 01 : ARQC/TC/AAC verification failed 04 : Mode Flag not 0, 1 or 2 05 : Unrecognised Scheme ID 10 : MK parity error 12 : No keys in user storage 13 : LMK parity error 15 : Error in input data 21 : Invalid user storage index 80 : Data length error 81 : Zero length Transaction Data
ARPC	8 B	The calculated ARPC. Only present for Modes 1 and 2 if no error is encountered.
Diagnostic data	8 B	Calculated ARQC/TC/AAC returned only if the error code is 01 and the HSM is in Authorised State.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

24.2 Data Authentication Code and Dynamic Number Verification

Command: Verify a Data Authentication Code (DAC) or Dynamic Number (DN).

Notes: Diagnostic data is produced by this command only if the HSM is in Authorised State.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value KS.
Mode Flag	1 H	Mode of operation: 0 = Perform DAC Verification 1 = Perform DN Verification
Scheme ID	1 H	Identifier of the Scheme: 1 = Europay/MasterCard
*MK-DAC(LMK)	32 H or 1A+32H	The Issuer Master Key for Data Authentication Codes encrypted under Variant 4 of LMK pair 28-29. Present only for Mode 0.
*MK-DN(LMK)	32 H or 1A+32H	The Issuer Master Key for Dynamic Numbers encrypted under Variant 5 of LMK pair 28-29. Present only for Mode 1.
PAN/PAN Sequence No	8 B	Pre-formatted PAN/PAN Sequence No. Present for both Mode 0 and 1.
DAC	2 B	Data Authentication Code for validation. Only present for Mode 0.
DN	2 B	Dynamic Number for validation. Only present for Mode 1.
ATC	2B	Application Transaction Counter. Only present for Mode 1.
UN	4B	Unpredictable Number. Only present for Mode 1.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value KT.
Error Code	2 N	00 : No error 01 : DAC or DN verification failed 04 : Mode Flag not 0 or 1 05 : Unrecognised Scheme ID 10 : MK parity error 12 : No keys in user storage 13 : LMK parity error 15 : Error in input data 21 : Invalid user storage index
Diagnostic Data	2 B	The calculated DAC or DN (depending on the mode selected). Only provided if error code 01 is returned and the HSM is in Authorised State.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

24.3 Generate Secure Message with Integrity and optional Confidentiality and PIN Change

Command: Generate a Secure Message with Integrity over data to be sent from the Issuer back to the Card. Optionally, Secure Messaging with Confidentiality is provided in which case the message data must be supplied encrypted under a Transport Key. In this latter case the command first decrypts the message data using the Transport Key before re-encrypting it using a Session Key.

Notes: This command is also used to change or unblock a PIN.

To change the PIN held by an EMV card, the issuer has to validate the existing PIN, then accept a new PIN in a standard PIN block format. This PIN block is then translated from a standard ATM PIN block format (encrypted under a terminal or zone key) to an application specific PIN block format (encrypted under a confidentiality session key).

To generate a PIN unblock script, "Mode 0" should be used (integrity only), with an EMV PIN Unblock APDU supplied in the "Plaintext Message Data" field.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value KU.
Mode Flag	1 N	0 = Provide only Integrity functionality 1 = Provide Integrity and Confidentiality using the same Issuer Master Key 2 = Provide Integrity and Confidentiality using different Master Keys 3 = Provide Integrity and PIN Block translation for PIN Change, using the same Issuer Master Key 4 = Provide Integrity and PIN Block translation for PIN Change, using different Issuer Master Keys
Scheme-ID	1 N	Identifier for the Scheme: 0 = Visa VSDC and UKIS 1 = Europay/MasterCard
*MK-SMI(LMK)	32 H or 1A+32H	The Master Key for Secure Messaging with Integrity encrypted under Variant 2 of LMK pair 28-29.
PAN/PAN Sequence No	8 B	Pre-formatted PAN/PAN Sequence number
Integrity Session Data	8 B	Data used for Integrity Session Key Generation. For Scheme-ID = 0 (Visa/UKIS) this is the ATC (2 bytes) right justified and padded on the left with 6 zero bytes. For Scheme-ID = 1 (Europay/MasterCard) this is an 8 byte random number, RANDi.
Plaintext Message Data Length	4 H	Length in bytes of data in next field. For the standard model HSM (RG7x00) the maximum size is 512 bytes (hex 0200).
Plaintext Message Data	n B	Plaintext Message Data.
Delimiter	1 A	Delimiter of previous field, ";".
*MK-SMC(LMK)	32 H or 1A+32H	The Master Key for Secure Messaging with Confidentiality encrypted under Variant 3 of LMK pair 28-29. Only present if Mode Flag = 2 or 4.
TK(LMK)	32 H or 1A+32H	Transport Key encrypted under LMK pair 30-31. This key was used to encrypt the supplied message. Only present if Mode Flag = 1 or 2.

Field	Length & Type	Details
Confidentiality Session Data	8 B	Used for Confidentiality Session Key Generation. For Scheme ID = 0, (Visa/UKIS) this is the 2 byte ATC right justified and padded on the left with 6 zero bytes. For Scheme ID = 1 (Europay/MasterCard) this is a random number, RANDc. Only present if Mode Flag = 1, 2, 3 or 4.
Offset	4 H	Position within Plaintext data to insert Ciphertext data. Must be between 0000 and Plaintext Message Data length. If Offset = n, Ciphertext is inserted AFTER the nth byte of the Plaintext (i.e. if length of Plaintext data is 0039, and Offset is 39, Ciphertext data is placed at the end of the plaintext message). Only present if Mode Flag = 1, 2, 3 or 4. If Mode Flag = 3 or 4, this is used to specify the new PIN Block position.
Cipher Text Message Data Length	4 H	Length in bytes of data in next field. For the standard model HSM (RG7x00) the maximum size is 32 bytes (hex 0020). Must be a multiple of 8 bytes (i.e. 8, 16, 24 or 32). Only Present if Mode Flag = 1, 2, 3 or 4. If Mode Flag = 3 or 4, this is used for the New PIN Block. If Destination PIN Block Type = 42, this is used for Current PIN Block concatenated with New PIN Block.
Cipher Text Message Data	n B	Cipher Text Message supplied encrypted using a Transport Key (TK). It must be a multiple of 8 bytes long. Note that no additional padding is performed on the decrypted message before the re-encryption process. Only Present if Mode Flag = 1, 2, 3 or 4. If Mode Flag = 3 or 4, this is used for the New PIN Block. If Destination PIN Block Type = 42, this is used for Current PIN Block concatenated with New PIN Block.
Delimiter	1 A	Delimiter of previous field, ",". Only Present if Mode Flag = 1, 2, 3 or 4.
Source PIN Encryption Key Type	1 N	0 = ZPK 1 = TPK Only present if Mode Flag = 3 or 4
Source PIN Encryption Key	16 H or 1A+32H or 1A+48H	Source PIN Encryption Key, encryption depending on the Source PIN Encryption Key Type:- - encrypted under LMK pair 06-07 if ZPK - encrypted under LMK pair 14-15 if TPK Only present if Mode Flag = 3 or 4.
Source PIN Block Format	2 N	The format code for the source PIN block. Only Present if Mode Flag = 3 or 4.
Destination PIN Block format	2 N	34 = Standard EMV PIN Block 35 = Europay/Mastercard Pay Now & Pay Later 41 = Visa Format Without Using Current PIN 42 = Visa Format using Current PIN Only Present if Mode Flag = 3 or 4.
Account Number	12 N	The 12 right most digits of the account number, excluding the check digit, used for PIN Block translation. Only Present if Mode Flag = 3 or 4.
*MK-AC(LMK)	32H or 1A+32H	The Issuer Master Key for Application Cryptograms, encrypted under variant 1 of LMK pair 28-29. Only present if Mode Flag = 3 or 4 and Destination PIN Block Format = 41 or 42.

Field	Length & Type	Details
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value KV
Error Code	2 N	00 : No error 04 : Mode flag not set to 0, 1, 2, 3 or 4 05 : Unrecognized Scheme-ID 06 : Invalid Offset 07 : Invalid ciphertext message length parameter 08 : Ciphertext message length error 09 : TK or ZPK/TPK parity error 10 : MK-SMI parity error 11 : MK-SMC parity error 12 : No keys in user storage 13 : LMK parity error 15 : Error in input data 21 : Invalid user storage index 23 : Invalid PIN block format code 50 : Source PIN Encryption Key Type not set to 0 or 1 51 : MK-AC parity error 80 : Data length error 81 : Data not a multiple of 8 bytes
MAC	8 B	The calculated 64 bit MAC.
Re-encrypted ciphertext	4 H	Length in bytes of data in next field. Only present for modes 1, 2, 3 or 4.
Data Length		
Re-encrypted ciphertext message Data	n B	Re-encrypted Ciphertext message. Only present for modes 1, 2, 3 or 4.
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.

25 AMERICAN EXPRESS CARD SECURITY CODE

25.1 Generate a *CSCK

Command: Generate a random dual-length *CSCK and encrypt it under LMK 14-15 variant 4.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	(Subsequently returned to the Host unchanged).
Command Code	2 A	Value RY.
Mode	1 N	Value 0
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged
Response Code	2 A	Value RZ.
Error Code	2 N	00 : No error 13 : LMK parity error 15 : Error in input data
Mode	1 N	Value 0
*CSCK	32H or 1A+32H	The *CSCK encrypted under LMK 14-15 variant 4.
Key check value	16 H or 6 H	Result of encrypting 64 binary zeros with the *CSCK. 16H or 6H depends upon KCV type option.
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.

25.2 Export a *CSCK

Command: Decrypt a *CSCK from under LMK 14-15 variant 4 and re-encrypt it under a supplied *ZMK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	(Subsequently returned to the Host unchanged).
Command Code	2 A	Value RY.
Mode	1 N	Value 1
*ZMK	32H or 1A+32H or 1A+48H	The Zone Master Key, encrypted under LMK 04-05.
*CSCK	32H or 1A+32H	The *CSCK encrypted under LMK 14-15 variant 4.
Atalla variant	1 N or 2 N	Optional.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method: 0 - KCV backwards compatible. 1 - KCV 6H.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19
Message Trailer	n A	Optional. Maximum length 32 characters
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged.
Response Code	2 A	Value RZ.
Error Code	2 N	00 : No error 10 : *ZMK parity error 11 : *CSCK parity error 12 : No keys in user storage 13 : LMK parity error 15 : Error in input data 27 : *CSCK not double length
Mode	1 N	Value 1.
*CSCK encrypted for export	32H or 1A+32H	The *CSCK encrypted under the supplied *ZMK.
Key check value	16 H or 6 H	Result of encrypting 64 binary zeros with the *CSCK. 16H or 6H depends upon KCV type option.
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

25.3 Import a *CSCK

Command: Decrypt a *CSCK from under a supplied *ZMK and re-encrypt it under LMK 14-15 variant 4.

Notes: Parity on the incoming *CSCK is ignored, but odd parity will be forced before re-encryption. Error code "01" will be returned if the incoming key did not have odd parity.

If the incoming key is found to be all zeros, Error Code 02 is returned and the key is not translated.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	(Subsequently returned to the Host unchanged).
Command Code	2 A	Value RY.
Mode	1 N	Value 2
*ZMK	32H or 1A+32H or 1A+48H	The Zone Master Key, encrypted under LMK 04-05.
*CSCK	32H or 1A+32H	The *CSCK, encrypted under the *ZMK.
Atalla variant	1 N or 2 N	Optional.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End Message Delimiter	1 C	Optional. 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 RZ.
Error Code	2 N	00 : No error 01 : Incoming key did not have odd parity 02 : Incoming key was all zero 10 : *ZMK parity error 12 : No keys in user storage 13 : LMK parity error 15 : Error in input data 27 : *CSCK not double length
Mode	1 N	Value 2
*CSCK	32 H	The *CSCK encrypted under LMK 14-15 variant 4.
Key check value	16 H or 6 H	Result of encrypting 64 binary zeros with the *CSCK. 16H or 6H depends upon KCV type option.
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

25.4 Calculate Card Security Codes

Command: This command will compute and return the 5-digit, 4-digit and 3-digit Card Security Code Values from the supplied data.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	(Subsequently returned to the Host unchanged).
Command Code	2 A	Value RY.
Mode	1 N	Value 3
Flag	1 N	A flag to indicate special processing options; value "0".
*CSCK	32H or 1A+32H	The *CSCK encrypted under LMK 14-15 variant 4.
Account number	19 N	The full account number, left-justified and zero-filled if less than 19 digits.
Expiration date	4 N	The expiration date in YYMM format.
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged
Response Code	2 A	Value RZ.
Error Code	2 N	00 : No error 10 : *CSCK parity error 12 : No keys in user storage 13 : LMK parity error 15 : Error in input data 27 : *CSCK not double length
Mode	1 N	Value 3
5-digit CSC	5 N	The 5-digit Card Security Code Value.
4-digit CSC	4 N	The 4-digit Card Security Code Value.
3-digit CSC	3 N	The 3-digit Card Security Code Value.
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

25.5 Verify Card Security Codes

Command: This command verifies the 5-digit, 4-digit and 3-digit Card Security Code.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	(Subsequently returned to the Host unchanged).
Command Code	2 A	Value RY.
Mode	1 N	Value 4
Flag	1 N	A flag to indicate special processing options; value 0.
*CSCK	32H or 1A+32H	The *CSCK encrypted under LMK 14-15 variant 4.
Account number	19 N	The full account number, left-justified and zero-filled if less than 19 digits.
Expiration date	4 N	The expiration date in YYMM format.
5-digit CSC	5 N	5-digit Card Security code. If not present value FFFFF
4-digit CSC	4 N	4-digit Card Security code. If not present value FFFF
3-digit CSC	3 N	3-digit Card Security code. If not present value FFF
End Message Delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message Trailer	n A	Optional. Maximum length 32 characters
RESPONSE MESSAGE		
Message Header	m A	Returned to the Host unchanged
Response Code	2 A	Value RZ
Error Code	2 N	00 : No error 01 : Card security code verification failure 10 : *CSCK parity error 12 : No keys in user storage 13 : LMK parity error 15 : Error in input data 21 : Invalid user storage index 27 : *CSCK not double length
Mode	1 N	Value 4
5-digit CSC verification	1 N	0 if pass. 1 if not present. 2 if verification failed.
4-digit CSC verification	1 N	0 if pass. 1 if not present. 2 if verification failed.
3-digit CSC verification	1 N	0 if pass. 1 if not present. 2 if verification failed.
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

26 RACAL TRANSACTION KEY SCHEME (RTKS)

The Racal Transaction Key Scheme (RTKS) is a key management technique that is closely coupled with message authentication. The functions provided by the HSM include key management in addition to MAC generation and verification.

The functions are all for use at an acquirer site:

- Transaction request with PIN (T/AQ key). Used to receive a cardholder request message from a terminal with a PIN encrypted under the T/AQ key.
- Transaction request without PIN. Used to receive a cardholder request message from a terminal with no PIN.
- Transaction request with PIN (T/CI key). Used to receive the request from the terminal when the PIN key cannot be determined by the acquirer.
- KEYVAL translation. Used to pass KEYVAL to the card issuer (required to derive the PIN key) when the PIN key cannot be determined by the acquirer.
- Administration request. Used to receive an administration request message (such as a reconciliation request).
- Transaction response originating at the card issuer. Used when authorization is generated at the card issuer.
- Transaction response originating at the acquirer. Used when authorization is generated by the acquirer.
- Verify confirmation message from terminal. Used to verify the MAC on a confirmation message from the terminal.

The commands RI, RK, RM, RO, RQ, RS and RU are only available when Racal Transaction Key Scheme is selected using the configure security command.

The existing Racal Transaction key commands have been modified to support longer messages the new commands are backward compatible with existing systems the details of the modifications are as follows.

Old style:	Pointer (not all functions)	2 H	
	Message Length	2 H	
	Message Text	n A	
New style:	Pointer (if required)	2 H	
	Message Length	2 H	
	Message Text	n A	
	Delimiter	1 C	Optional, only if original length is 0
	Extended Message Pointer(s)	4 H	Optional, only if original length is 0 and function requires one or two pointers
	Extended Message Length	4 H	Optional, only if original length is 0
	Extended Message	n A	Optional, only if above field is non zero

To use the extended message length option, the calling application has to set the Message Length field to zero, whereupon the Message Text field will be of zero length, i.e. not present. The zero Message Length enables the HSM to check for the optional Delimiter, any Extended Message Pointer(s), and the Extended Message Length field which defines the length of the Extended Message.

Some of the functions do not include a pointer to items included in the message, whilst other functions include either one or two pointers. If a function does include one or two pointers, one or two Extended Message Pointers are included after the Delimiter as appropriate. The original pointer(s) in the function are ignored when extended messages are used, however the 2 hex digit placeholder(s) for the original pointer(s) must still be supplied.

Whilst the extended commands allow for message sizes up to 65537 characters long (hex FFFF), in practice the limit is imposed by the maximum size of the HSM input buffer. For the standard HSM (Models RG7x00), the input buffer size is limited to 2047 characters. Allowing for the other parts of a command message, the maximum message size will be in the region of

1900 characters. The high speed HSM (Models RG7x10) has a much larger input buffer (32K) although the interface option in use may impose limits which are smaller than this. The HSM will check that the message lengths (and the pointers) are within sensible limits for the HSM platform executing the function.

Users may, if they wish, use the Extended Message Length scheme for small messages (i.e. less than 160 bytes).

26.1 Transaction Request With a PIN (T/AQ Key)

Command: Validate a MAC on request from a terminal and return the TPK under the LMK and the MAC residue under the LMK.

Notes: The command does not accept an all zero account number element of the 'message text' field.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RI.
Terminal key register	16 H	The terminal key register encrypted under LMK pair 14-15.
Account number pointer	2 H	00 if the account number starts at the first character in the message text field, and one value greater for each subsequent character into the field. The account number is terminated by the first non-numeric character. This is ignored if extended length messages are used but 2 hex digits must still be supplied.
Fields C & D	16 H	The C & D fields from the magnetic stripe of a card as defined in the Racal Security Scheme.
PIN block pointer	2 H	00 if the PIN block starts at the first character in the message text field, and one value greater for each subsequent character into the field. The PIN block is assumed to be 16 (hexadecimal) characters and is assumed to be formatted according to ANSI X9.8. . This is ignored if extended length messages are used but 2 hex digits must still be supplied.
Message length	2 H	Value X'00 to X'A0 (decimal 160) indicating the length of the next field. This field should be set to X'00 and the next field omitted if extended length messages required.
Message text	n A	The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. An all zero account number cannot be used. Omitted if extended length messages are required.
Delimiter	1 C	Optional. Value ";". Only present if extended length messages to be used.
Extended account number pointer	4 H	Optional. Only present if extended length messages are to be used. 0000 if the account number starts at the first character in the message text field, and one value greater for each subsequent character into the field. The account number is terminated by the first non-numeric character.
Extended PIN block pointer	4 H	Optional. Only present if extended length messages are to be used. 0000 if the PIN block starts at the first character in the message text field, and one value greater for each subsequent character into the field. The PIN block is assumed to be 16 (hexadecimal) characters and is assumed to be formatted according to ANSI X9.8.

Field	Length & Type	Details
Extended Message Length	4 H	Optional. Only present if extended length messages are to be used. Defines the length of the next field. Maximum value is determined by the maximum size of the HSM input buffer.
Extended Message Text	n A	Optional. Only present if extended length messages are to be used. The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. An all zero account number cannot be used.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value RJ.
Error code	2 N	00 : No errors 01 : MAC verification fail 10 : Key register parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block does contain valid values 21 : Invalid user storage index 22 : All zero account number used (processing is terminated) 24 : PIN is fewer than 4 or more than 12 digits 80 : Message length error
MAC residue	8 H	The MAC residue encrypted under LMK 10.
TPK	16 H	The TPK encrypted under LMK pair 14-15.
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.

26.2 Transaction Request Without a PIN

Command: Verify the MAC and return the MAC residue.

Notes: Similar to the previous command, but does not return the derived TPK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RK.
Terminal key register	16 H	The terminal key register encrypted under LMK pair 14-15.
Account number pointer	2 H	00 if the account number starts at the first character in the message text field, and one value greater for each subsequent character into the field. The account number is terminated by the first non-numeric character. This is ignored if extended length messages are used but 2 hex digits must still be supplied.
Message length	2 H	Value X'00 to X'A0 (decimal 160) indicating the length of the next field. This field should be set to X'00 and the next field omitted if extended length messages required.
Message text	n A	The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. Omitted if extended length messages are required.
Delimiter	1 C	Optional. Value ":". Only present if extended length messages to be used.
Extended account number pointer	4 H	Optional. Only present if extended length messages are to be used. 0000 if the account number starts at the first character in the message text field, and one value greater for each subsequent character into the field. The account number is terminated by the first non-numeric character.
Extended Message Length	4 H	Optional. Only present if extended length messages are to be used. Defines the length of the next field. Maximum value is determined by the maximum size of the HSM input buffer.
Extended Message Text	n A	Optional. Only present if extended length messages are to be used. The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. An all zero account number cannot be used.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value RL.
Error code	2 N	00 : No errors 01 : MAC verification fail 10 : Key register parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 80 : Message length error
MAC residue	8 H	The MAC residue encrypted under LMK 10.
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.

26.3 Transaction Request With a PIN (T/CI Key)

Command: Verify the MAC and return the MAC residue and KEYVAL encrypted under the LMK.

Notes: The command does not accept an all zero account number element of the 'message text' field.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RU.
Terminal key register	16 H	The terminal key register encrypted under LMK pair 14- 15.
Account number pointer	2 H	00 if the account number starts at the first character in the message text field, and one value greater for each subsequent character into the field. The account number is terminated by the first non-numeric character. This is ignored if extended length messages are used but 2 hex digits must still be supplied.
Message length	2 H	Value X'00 to X'A0 (decimal 160) indicating the length of the next field. This field should be set to X'00 and the next field omitted if extended length messages required.
Message text	n A	The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. An all zero account number cannot be used. Omitted if extended length messages are required.
Delimiter	1 C	Optional. Value ";". Only present if extended length messages to be used.
Extended account number pointer	4 H	Optional. Only present if extended length messages are to be used. 0000 if the account number starts at the first character in the message text field, and one value greater for each subsequent character into the field. The account number is terminated by the first non-numeric character.
Extended Message Length	4 H	Optional. Only present if extended length messages are to be used. Defines the length of the next field. Maximum value is determined by the maximum size of the HSM input buffer.
Extended Message Text	n A	Optional. Only present if extended length messages are to be used. The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. An all zero account number cannot be used.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value RV.
Error code	2 N	00 : No errors 01 : MAC verification fail 10 : Key register parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 80 : Message length error
MAC residue	8 H	The MAC residue encryption under LMK 10.
End message delimiter	1C	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.

26.4 Translate KEYVAL

Command: Translate KEYVAL from encryption under the LMK to encryption under a ZPK

Notes: Used to send KEYVAL to another party.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RW.
ZPK	16H or 1A+32H or 1A+48H	The ZPK encrypted under LMK pair 06-07.
KEYVAL	16 H	KEYVAL encrypted under LMK pair 14-15.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value RX.
Error code	2 N	00 : No errors 10 : ZPK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index
KEYVAL	16 H	KEYVAL encrypted under the ZPK.
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.

26.5 Administration Request Message

Command: Verify the MAC on an administration request message and return the MAC residue encrypted under the LMK. Used to support terminal administration request messages.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RM.
Terminal key register	16 H	The terminal key register encrypted under LMK pair 14-15.
Fields A & B	16 H	The A & B fields as defined in the Racal Security Scheme.
Message length	2 H	Value X'00 to X'A0 (decimal 160) indicating the length of the next field. This field should be set to X'00 and the next field omitted if extended length messages required.
Message text	n A	The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. Omitted if extended length messages are required.
Delimiter	1 C	Optional. Value ";" . Only present if extended length messages to be used.
Extended Message Length	4 H	Optional. Only present if extended length messages are to be used. Defines the length of the next field. Maximum value is determined by the maximum size of the HSM input buffer.
Extended Message Text	n A	Optional. Only present if extended length messages are to be used. The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. An all zero account number cannot be used.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value RN.
Error code	2 N	00 : No errors 01 : MAC verification fail 10 : Key register parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 80 : Message length error
MAC residue	8 H	The MAC residue encrypted under LMK 10.
End message delimiter	1C	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.

26.6 Transaction Response with Auth Para from Card Issuer

Command: Generate a MAC on a response message to a terminal and the new Key Register value encrypted under the LMK. Also, generate new MAC residue under the LMK.

Notes: The command is used to respond to requests from terminals at the acquirer Host.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RO.
Terminal key register	16 H	The terminal key register encrypted under LMK pair 14-15.
Fields A & B	16 H	The A & B fields as defined in the Racal Security Scheme.
ZPK or flag	16H or 1A+32H or 1A+48H or A	The ZPK under which Auth Para is encrypted, or the character L if Auth Para is encrypted under the LMK.
Auth Para	16 H	The authorization parameter either encrypted under ZPK or under LMK pair 14-15 (as indicated in the previous field).
MAC residue	8 H	The MAC residue from the request message processing; encrypted under LMK 10.
Message length	2 H	Value X'00 to X'A0 (decimal 160) indicating the length of the next field. This field should be set to X'00 and the next field omitted if extended length messages required.
Message text	n A	The response message on which the response MAC should be calculated. Omitted if extended length messages are required.
Delimiter	1 C	Optional. Value ":". Only present if extended length messages to be used.
Extended Message Length	4 H	Optional. Only present if extended length messages are to be used. Defines the length of the next field. Maximum value is determined by the maximum size of the HSM input buffer.
Extended Message Text	n A	Optional. Only present if extended length messages are to be used. The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. An all zero account number cannot be used.
End message delimiter	1C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value RP.
Error code	2 N	00 : No errors 10 : Key register parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 80 : Message length error
MAC residue	8 H	The MAC residue encrypted under LMK 10.
MAC	8 H	The generated MAC to be sent to the terminal.
End message delimiter	1C	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.

26.7 Generate Auth Para and Transaction Response

Command: Generate Auth Para, the response MAC on a response message to a terminal and the new key register value encrypted under the LMK.

Notes: The command used to respond to requests from terminals at the acquirer Host.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RQ.
Terminal key register	16 H	The terminal key register encrypted under LMK pair 14-15.
Fields A & B	16 H	The A & B fields from the card as defined in the Racal Security Scheme.
Auth Para data block	16 H	The data block used to generate Auth Para.
MAC residue	8 H	The MAC residue from the request message processing; encrypted under LMK 10.
Message length	2 H	Value X'00 to X'A0 (decimal 160) indicating the length of the next field. This field should be set to X'00 and the next field omitted if extended length messages required.
Message text	n A	The response message on which the response MAC should be calculated. Omitted if extended length messages are required.
Delimiter	1 C	Optional. Value ":". Only present if extended length messages to be used.
Extended Message Length	4 H	Optional. Only present if extended length messages are to be used. Defines the length of the next field. Maximum value is determined by the maximum size of the HSM input buffer.
Extended Message Text	n A	Optional. Only present if extended length messages are to be used. The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. An all zero account number cannot be used.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value RR.
Error code	2 N	00 : No errors 10 : Key register parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 80 : Message length error
MAC residue	8 H	The MAC residue encrypted under LMK 10.
MAC	8 H	The generated MAC to be sent to the terminal.
Terminal key register	16 H	The new terminal key register to replace the current value; encrypted under LMK pair 14-15.
End message delimiter	1C	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.

26.8 Confirmation

Command: Verify MAC on incoming confirmation message from the terminal.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RS.
Terminal key register	16 H	The terminal key register encrypted under LMK pair 14-15.
Fields A & B	16 H	The A & B fields from the card as defined in the Racal Security Scheme.
MAC residue	8 H	The MAC residue from the previous message processing; encrypted under LMK 10.
Message length	2 H	Value X'00 to X'A0 (decimal 160) indicating the length of the next field. This field should be set to X'00 and the next field omitted if extended length messages required.
Message text	n A	The response message on which the response MAC should be calculated, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. Omitted if extended length messages are required.
Delimiter	1 C	Optional. Value ";". Only present if extended length messages to be used.
Extended Message Length	4 H	Optional. Only present if extended length messages are to be used. Defines the length of the next field. Maximum value is determined by the maximum size of the HSM input buffer.
Extended Message Text	n A	Optional. Only present if extended length messages are to be used. The message to be authenticated as received from the terminal, but excluding the STX, ETX and LRC. The last 8 characters are assumed to be the MAC. An all zero account number cannot be used.
End message delimiter	1C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value RT.
Error code	2 N	00 : No errors 01 : MAC verification failure 10 : Key register parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 80 : Message length error.
End message delimiter	1C	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.

27 DERIVED UNIQUE KEY PER TRANSACTION (DUKPT) SYSTEM

The Derived Unique Key per Transaction system accesses the following commands via the Host port:

- Generate a Base Derivation Key (*BDK) and encrypt it under LMK pair 28-29 for Host storage.
- Translate a PIN from *BDK to interchange key encryption.
- Verify a PIN using the IBM method.
- Verify a PIN using the Visa PVV method.
- Verify a PIN using the Diebold method.
- Verify a PIN using the encrypted PIN method.
- Translate an encrypted *BDK from *ZMK to LMK.
- Translate an encrypted *BDK from LMK to *ZMK.

27.1 Generate an Base Derivation Key (*BDK)

Command: Generate a *BDK and encrypt it under LMK pair 28-29 for Host storage.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value BI.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value BJ.
Error code	2 N	00 : No errors 13 : LMK error; report to supervisor 15 : Error in input data
*BDK	32H or 1A+32H	The *BDK encrypted under LMK pair 28-29.
End message delimiter	1 C	Present only if present in the command message.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

27.2 Translate a PIN from *BDK Encryption to Interchange Key Encryption

Command: Translate a PIN from encryption under the unique *BDK to encryption under an interchange key (ZPK) for transmission to another node.

Notes: The command performs the same function as CA and CC, except the Host supplies the HSM with the information necessary to compute the current key. The *BDK, the KSN, and the KSN descriptor are supplied by the PIN pad.

The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value CI.
*BDK	32H or 1A+32H	The *BDK pair encrypted under LMK pair 28-29.
ZPK	16H or 1A+32H or 1A+48H	The Zone Pin Key encrypted under LMK pair 06-07.
KSN descriptor	3 H	The descriptor for the KSN (in the next field).
Key serial number	12 - 20 H	The KSN supplied by the PIN pad.
Source encrypted block	16 H	The encrypted PIN block received from the POS PIN terminal.
Destination PIN block format code	2 N	One of the following codes: 01 : ANSI format 04 : Plus format
Account number	12 N	The 12 right-most digits of the PAN excluding the check digit.
End message delimiter	1 C	Present only if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value CJ.
Error code	2 N	00: No errors 10 : *BDK parity error 11 : Interchange key parity error 12 : No keys loaded in user storage 15 : Error in input data 23 : Invalid PIN block format code 27 : *BDK not double length
PIN length	2 N	Length of the translated PIN.
Encrypted PIN	16 H	The PIN block encrypted under the interchange key and formatted according to the destination PIN block format code.
Destination PIN block format code	2 N	Returned to the Host unchanged.
End message delimiter	1 C	Present only if present in the command message.
Message trailer	n A	Present only if present in the command message.

27.3 Verify a PIN Using the IBM Method

Command: Verify a PIN using the IBM method.

Notes: The command performs the same function as DA and EA, plus it computes the PIN pad key. The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

The HSM can be configured to disallow the use of known weak values in the decimalization tables. This table checking is enabled by default but can be disabled using the CS (Configure Security) console command.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues verifying the PIN using TDES in place of DES.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value CK.
*BDK	32H or 1A+32H	The *BDK encrypted under LMK pair 28-29.
PVK	16H or 1A+32H or 1A+48H	The PVK encrypted under LMK pair 14-15
KSN descriptor	3 H	The descriptor for the KSN (in the next field).
Key serial number	12 - 20 H	The KSN supplied by the PIN pad.
Source encrypted block	16 H	Encrypted PIN block received from the POS PIN terminal.
Check length	2 N	The minimum PIN length.
Account number	12 N	The 12 right-most digits of the primary account number (PAN), excluding the check digit.
Decimalization table	16 N	Table for converting encrypted characters to decimal digits.
PIN validation	12 A	User-defined data consisting of hexadecimal characters, and the letter N, which indicates where the HSM is to insert the last five digits of the account number specified in the Host request message (the digits must be left-justified).
Offset	12 H	The IBM offset value, left-justified and padded with "F".
End message delimiter	1 C	Present only if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value CL.
Error code	2 N	00: No errors 01 : Verification failure 02 : Warning PVK not single length 10 : *BDK parity error 11 : PVK parity error 12 : No keys loaded in user storage 15 : Error in input data 27 : *BDK not double length
End message delimiter	1 C	Present only if present in the command message.
Message trailer	n A	Present only if present in the command message.

27.4 Verify a PIN Using the VISA PVV Method

Command: Verify a PIN using the VISA PVV method.

Notes: The command performs the same function as DC and EC.

The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value CM.
*BDK	32H or 1A+32H	The *BDK encrypted under LMK pair 28-29.
*PVK	32H or 1A+32H	The PIN verification key, encrypted under LMK pair 14-15.
KSN descriptor	3 H	The descriptor for the KSN (in the next field).
Key serial number	12 - 20 H	The KSN supplied by the PIN pad.
Source encrypted block	16 H	The encrypted PIN block received from the POS PIN terminal.
Account number	12 N	The 12 right-most digits of the PAN, excluding the check digit.
PVKI	1 N	The PIN verification key indicator.
PVV	4 N	The PIN verification value from the card or data base.
End message delimiter	1 C	Present only if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value CN.
Error code	2 N	00 : No errors 01 : Verification failure 10 : *BDK parity error 11 : *PVK parity error 12 : No keys loaded in user storage 15 : Error in input data 27 : *BDK or PVK not double length
End message delimiter	1 C	Present only if present in the command message.
Message trailer	n A	Present only if present in the command message.

27.5 Verify a PIN Using the Diebold Method

Command: Verify a PIN using the Diebold method.

Notes: The command performs the same function as CG and EG. The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value CO.
*BDK	32H or 1A+32H	The *BDK encrypted under LMK pair 28-29.
Index flag	1 A	Value K.
Base index	3 H	The index pointing to the start of the Diebold table in user storage.
Diebold algorithm number	2 H	The algorithm number required by the Diebold method.
KSN descriptor	3 H	The descriptor for the KSN (in the next field).
Key serial number	12 - 20 H	The KSN supplied by the PIN pad.
Source encrypted block	16 H	The encrypted PIN block received from the POS PIN terminal.
Account number	12 N	The 12 right-most digits of the PAN, excluding the check digit.
PIN validation	16 H	User-defined data consisting of hexadecimal characters, and the letter N, which indicates where the HSM is to insert the last five digits of the account number specified in the Host request message. (The digits must be left-justified).
Offset	4 N	The Diebold offset value.
End message delimiter	1 C	Present only if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value CP.
Error code	2 N	00 : No errors 01 : Verification failure 10 : *BDK parity error 12 : No keys loaded in user storage 15 : Error in input data 19: Specified Diebold table is invalid. 27 : *BDK not double length
End message delimiter	1 C	Present only if present in the command message.
Message trailer	n A	Present only if present in the command message.

27.6 Verify a PIN Using the Encrypted PIN Method

Command: Verify a PIN using the Encrypted PIN method.

Notes: The command performs the same function as BC and BE. The PIN block is assumed to be in the ANSI X9.8 format; no source PIN block format codes are required.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value CQ.
*BDK	32H or 1A+32H	The *BDK encrypted under LMK pair 28-29.
KSN descriptor	3 H	The descriptor for the KSN (in the next field).
Key serial number	12 - 20 H	The KSN supplied by the PIN pad.
Source encrypted block	16 H	The encrypted PIN block received from the POS PIN terminal.
Account number	12 N	The 12 right-most digits of the PAN, excluding the check digit.
Encrypted data base PIN	L N	The PIN from the Host database encrypted under LMK pair 02-03.
End message delimiter	1 C	Present only if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value CR.
Error code	2 N	00 : No errors 01 : Verification failure 10 : *BDK parity error 12 : No keys loaded in user storage 15 : Error in input data 27 : *BDK not double length
End message delimiter	1 C	Present only if present in the command message.
Message trailer	n A	Present only if present in the command message.

27.7 Translate a Base Derivation Key from *ZMK to LMK Encryption

Command: Translate a *BDK from encryption under a *ZMK to encryption under LMK pair 28-29.

Notes: The command ignores the S/D (single/double length) parameter set by the CS (Configure Security) console command.

A key check value (KCV) is produced for the *BDK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value DW.
*ZMK	32H or 1A+32H or 1A+48H	The *ZMK encrypted under LMK pair 04-05.
*BDK	32H or 1A+32H	The *BDK encrypted under the *ZMK.
Atalla variant	1 N or 2 N	Optional. For use in networks that use a *ZMK variant.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible (8H for this command). 1 - KCV 6H. 2 - KCV 8H.
End message delimiter	1 C	Present only if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value DX.
Error code	2 N	00 : No errors 10 : *ZMK parity error 11 : *BDK parity error 12 : No keys loaded in user storage 13: LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : *BDK not double length
*BDK	32H or 1A+32H	The *BDK encrypted under LMK pair 28-29.
Key check value	6H or 8 H	Result of encrypting 64 binary zeros with the *BDK.
End message delimiter	1 C	Present only if present in the command message.
Message trailer	n A	Present only if present in the command message.

27.8 Translate a Base Derivation Key from LMK to *ZMK Encryption

Command: Translate a *BDK from encryption under a LMK pair 28-29 to encryption under *ZMK.

Notes: The command ignores the S/D (single/double length) parameter set by the CS (Configure Security) console command.

A key check value (KCV) is produced for the *BDK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value DY.
*ZMK	32H 1A+32H or 1A+48H	The *ZMK encrypted under LMK pair 04-05.
*BDK	32H or 1A+32H	The *BDK encrypted under LMK pair 28-29
Atalla variant	1 N or 2 N	Optional. For use in networks that use a *ZMK variant.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ":". If an option is not required by the command fill with a valid value or 0.
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible (8H for this command). 1 - KCV 6H. 2 - KCV 8H.
End message delimiter	1 C	Present only if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value DZ.
Error code	2 N	00 : No errors 10 : *ZMK parity error 11 : *BDK parity error 12 : No keys loaded in user storage 13: LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : *BDK not double length
*BDK	32H or 1A+32H	The *BDK encrypted under the *ZMK.
Key check value	6H or 8 H	Result of encrypting 64 binary zeros with the key
End message delimiter	1 C	Present only if present in the command message.
Message trailer	n A	Present only if present in the command message.

28 AUSTRALIAN TRANSACTION KEY SCHEME (ATKS)

The Australian Transaction Key Scheme accesses the following commands via the Host port:

Terminal-to-acquirer requests:

- Transaction request without a PIN. Used to receive a cardholder request message from a terminal with no PIN.
- Transaction request with PIN (T/AQ key). Used to receive a cardholder request message from a terminal with a PIN encrypted under the T/AQ key.
- Transaction request with PIN (T/CI key). Used to receive a request from the terminal when the PIN key cannot be determined by the acquirer.

Acquirer-to-terminal responses:

- Transaction response originating at the acquirer. Used when authorization is generated by the acquirer.
- Transaction response originating at the card issuer. Used when authorization is generated at the card issuer.

Acquirer PIN translation:

- Translate a PIN from encryption under the PEK to encryption under a ZPK.

Acquirer completion:

- Verify completion confirmation message from terminal. Used to verify the MAC on a confirmation message from the terminal.
- Generate completion response.

Card issuer support:

- Verify a PIN at the card issuer using one of the following methods:
 - IBM.
 - Diebold.
 - Visa.
 - Comparison.
- Generate authorization at the card issuer.

Binary message authentication:

- Generate a MAC on a binary message.
- Verify a MAC on a binary message.

The commands RI, RK, RM, RO, RQ, RS and RU are only available when Racal Transaction Key Scheme is selected using the configure security command.

28.1 Transaction Request Without a PIN

Command: Validate the MAC on incoming data and return the MAC residue for subsequent processing.

Notes: The command is used by the Acquirer for normal transaction message processing, and for Administration Request messages.

If the Host is unable to support binary data transfers, the command can be used in standard (ASCII character) asynchronous mode (in which the message containing the MAC is transferred in expanded hexadecimal notation).

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RE.
Terminal key	16 H	The terminal key encrypted under LMK pair 14-15.
AB	16 H	Formed in accordance with the terminal specification by the Host.
EITHER		
For Binary Communications Modes:		
Message length	3 H	X'001 to X'320 indicating the length of the next field.
Message text	n B	1 to 800 bytes of message. The last 64 bits (8 bytes) are the MAC field of which the left-most 32 bits contain the MAC.
OR		
For Normal Async Modes:		
Message length	3 H	X'002 to X'320 indicating the number of characters in the next field.
Message text	n H	2 to 800 hexadecimal characters representing 1 to 400 bytes of message. The last 16 characters contain the MAC field as above.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value RF.
Error code	2 N	00 : No errors 01 : MAC verification failure 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 80 : Message length error (including odd number of characters when using standard async mode) 90 : Communications link parity error 91 : Communications link LRC error 92 : Transparent async data length error
MAC residue	8 H	Encrypted under LMK 10
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.

28.2 Transaction Request With a PIN (T/AQ Key)

Command: Validate the MAC on incoming data and return the MAC residue for subsequent processing.

Notes: The command allows an Acquirer to process a message which is to be authorised by the Acquirer on behalf of a Card Issuer. It is assumed that the Acquirer has access to the CD fields from the user's card. This command does not perform any PIN verification (this is performed by one of the other commands, DA, CG, DC).

The main outputs are the MAC residue from the incoming message, the PIN block encrypted under a Terminal PIN Key (TPK), and the TPK. The TPK is derived by the function.

If the Host is unable to support binary data transfers, the command can be used in standard (ASCII character) asynchronous mode (in which the message containing the MAC is transferred in expanded hexadecimal notation).

The PIN block pointer represents the count in bytes of the binary message. Therefore the value supplied is the same irrespective of the communications mode in use. In the case of standard async mode, the pointer can be used only AFTER the compression of the message into its binary form has taken place.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RG.
Terminal key	16 H	The terminal key encrypted under LMK pair 14-15.
AB	16 H	Formed in accordance with the terminal specification by the Host.
CD	16 H	Formed in accordance with the terminal specification by the Host.
PIN block pointer	3 H	X'000 to X'310. Count in bytes. X'000 indicates that the PIN block is the first 64 bits.
EITHER		
For Binary Communications Modes:		
Message length	3 H	X'001 to X'320 indicating the length of the next field.
Message text	n B	1 to 800 bytes of message. The last 64 bits (8 bytes) are the MAC field of which the left-most 32 bits contain the MAC.
OR		
For Standard Async Communications Mode:		
Message length	3 H	X'002 to X'320 indicating the number of characters in the next field.
Message text	n H	2 to 800 hexadecimal characters representing 1 to 400 bytes of message. The last 16 characters contain the MAC field as above.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value RH.
Error code	2 N	00 : No errors 01 : MAC verification failure 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block error 21 : Invalid user storage index 80 : Message length error (including odd number of characters when using standard async mode) 90 : Communications link parity error 91 : Communications link LRC error 92 : Transparent async data length error
Terminal PIN key	16 H	The derived TPK encrypted under LMK pair 14-15.
Derived PIN block	16 H	The decrypted PIN block re-encrypted under the derived TPK
MAC residue	8 H	Encrypted under LMK 10.
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.

28.3 Transaction Request With a PIN (T/CI Key)

Command: Validate the MAC on incoming data and return the MAC residue for subsequent processing.

Notes: The command allows an Acquirer to process a message before passing on the details to a Card Issuer. No knowledge of the CD fields from the card is required by the Acquirer. This command is used with PIN transaction command RO.

If the Host is unable to support binary data transfers, the command can be used in standard (ASCII character) asynchronous mode (in which the message containing the MAC is transferred in expanded hexadecimal notation).

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RI.
Terminal key	16 H	The terminal key encrypted under LMK pair 14-15.
AB	16 H	Formed in accordance with the terminal specification by the Host.
EITHER		
For Binary Communications Modes:		
Message length	3 H	X'001 to X'320 indicating the length of the next field.
Message text	n B	1 to 800 bytes of message. The last 64 bits (8 bytes) are the MAC field of which the left-most 32 bits contain the MAC.
OR		
For Standard Async Communications Mode:		
Message length	3 H	X'002 to X'320 indicating the number of characters in the next field.
Message text	n H	2 to 800 hexadecimal characters representing 1 to 400 bytes of message. The last 16 characters contain the MAC field as above.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value RJ.
Error code	2 N	00 : No errors 01 : MAC verification failure 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block error 21 : Invalid user storage index. 80 : Message length error (including odd number of characters when using standard async mode) 90 : Communications link parity error 91 : Communications link LRC error 92 : Transparent async data length error
PIN encrypting key	16 H	PEK encrypted under LMK pair 14-15.
MAC residue	8 H	Encrypted under LMK 10.
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.

28.4 Transaction Response With Auth Para Generated by the Acquirer

Command: Generate a transaction response with Auth Para generated by the Acquirer.

Notes: The command enables the Acquirer to generate the response message to a terminal, when the Acquirer is delegated to authorise a transaction on behalf of a Card Issuer. The Authorisation Parameter, Auth Para, is generated directly and included in the output MAC if appropriate. Auth Para is included if the transaction is approved, and not included if the transaction is declined.

The function can also be used to generate a MAC and update the Terminal Key for an Administration message response. For this purpose, the AP Include flag is E.

If the Host is unable to support binary data transfers, the command can be used in standard (ASCII character) asynchronous mode (in which the message to be MACed is transferred in expanded hexadecimal notation).

The AT, STAN and CATID pointers are in integral bytes and refer to the locations of the various values in the binary message. They are therefore the same irrespective of the communications mode in use. In standard async mode, they can be used only AFTER re-compression to a binary message.

AT is 6 bytes long (12 digits).

STAN is 3 bytes long (6 digits).

CATID is 8 bytes long (16 digits).

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RK.
Terminal key	16 H	The terminal key encrypted under LMK pair 14-15.
AB	16 H	Formed in accordance with the terminal specification by the Host.
MAC residue (MR ₁)	8 H	Encrypted under LMK 10.
AP include flag	1 A	I = include, E = exclude.
CD	16 H	Present only if flag is I.
AT pointer	3 H	Pointer to message text. Present only if flag is I.
STAN pointer	3 H	Pointer to message text. Present only if flag is I.
CATID pointer	3 H	Pointer to message text. Present only if flag is I.

Field	Length & Type	Details
EITHER		
For Binary Communications Modes:		
Message length	3 H	X'001 to X'320 indicating the length of the next field.
Message text	n B	1 to 800 bytes of message.
OR		
For Standard Async Communications Mode:		
Message length	3 H	X'002 to X'320 indicating the number of characters in the next field.
Message text	n H	2 to 800 hexadecimal characters representing 1 to 400 bytes of message.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value RL.
Error code	2 N	00 : No errors 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 80 : Message length error (including odd number of characters when using standard async mode) 90 : Communications link parity error 91 : Communications link LRC error 92 : Transparent async data length error
MAC residue (MR ₂)	8 H	Encrypted under LMK 10.
MAC	8 H	Newly-generated MAC.
Terminal key	16 H	The new derived TK encrypted under LMK pair 14-15.
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.

28.5 Transaction Response With Auth Para Generated by the Card Issuer

Command: Generate a response message to be sent to the Terminal, with Auth Para generated by the Card Issuer.

Notes: The command is used where a Card Issuer has generated Auth Para and sent it to the Acquirer encrypted under a Zone PIN Key (ZPK). Its main functions are to generate the MAC for the response message and to update the Terminal Key.

If the Host is unable to support binary data transfers, the command can be used in standard (ASCII character) asynchronous mode (in which mode the message to be MACed is transferred in expanded hexadecimal notation).

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RM.
Terminal key	16 H	The terminal key encrypted under LMK pair 14-15.
AB	16 H	Formed in accordance with the terminal specification by the Host.
MAC residue (MR ₁)	8 H	MR from the request message encrypted under LMK 10.
AP include flag	1 A	I = include, E = exclude.
Zone PIN key	16H or 1A+32H or 1A+48H	ZPK encrypted under LMK pair 06-07. Present only if AP include flag is I.
Auth Para	16 H	AP encrypted under a variant of ZPK. Present only if AP include flag is I.
EITHER		
For Binary Communications Modes:		
Message length	3 H	X'001 to X'320 indicating the length of the next field.
Message text	n B	1 to 800 bytes of message.
OR		
For Standard Async Communications Mode:		
Message length	3 H	X'002 to X'320 indicating the number of characters in the next field.
Message text	n H	2 to 800 hexadecimal characters representing 1 to 400 bytes of message.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value RN.
Error code	2 N	00 : No errors 11 : Zone PIN key parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 80 : Message length error (including odd number of characters when using standard async mode) 90 : Communications link parity error 91 : Communications link LRC error 92 : Transparent async data length error
MAC residue (MR ₂)	8 H	The MR from the response message encrypted under LMK 10.
MAC	8 H	Newly-generated MAC.
Terminal key	16 H	The new derived TK encrypted under LMK pair 14-15.
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.

28.6 Translate a PIN from PEK to ZPK Encryption

Command: Translate an encrypted PIN block from encryption under PEK to encryption under a Zone PIN Key (ZPK).

Notes: Used with the RI command, transaction request with PIN (T/CI key).

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RO.
PIN encrypting key	16 H	PEK encrypted under LMK pair 14-15.
Zone PIN key	16H or 1A+32H or 1A+48H	ZPK encrypted under LMK pair 06-07.
Encrypted PIN block	16 H	From terminal, encrypted under card key and PEK.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value RP.
Error code	2 N	00 : No errors 10 : PEK parity error 11 : ZPK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 90 : Communications link parity error 91 : Communications link LRC error 92 : Transparent async data length error
Encrypted PIN block	16 H	Now encrypted under card key and ZPK.
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.

28.7 Verify a Transaction Completion Confirmation Request

Command: Verify a transaction Completion Confirmation message and produce sufficient information for the subsequent generation of a Completion Response message.

Notes: The command allows the Acquirer to use the original TK that was used when the original request message and subsequent response message were processed. It does not use the new TK generated as a result of the response.

If the Host is unable to support binary data transfers, the command can be used in standard (ASCII character) asynchronous mode (in which the message containing the MAC is transferred in expanded hexadecimal notation).

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RQ.
Terminal key	16 H	TK encrypted under LMK pair 14-15.
AB	16 H	Formed in accordance with the terminal specification by the Host.
MAC residue	8 H	MR ₂ from transaction response encrypted under LMK 10.
EITHER		
For Binary Communications Modes:		
Message length	3 H	X'001 to X'320 indicating the length of the next field.
Message text	n B	1 to 800 bytes of message. The last 64 bits (8 bytes) are the MAC field of which the left-most 32 bits contain the MAC.
OR		
For Standard Async Communications Mode:		
Message length	3 H	X'002 to X'320 indicating the number of characters in the next field.
Message text	n H	2 to 800 hexadecimal characters representing 1 to 400 bytes of message. The last 16 characters contain the MAC field as above.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value RR.
Error code	2 N	00 : No errors 01 : MAC verification failure 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 80 : Message length error (including odd number of characters when using standard async mode) 90 : Communications link parity error 91 : Communications link LRC error 92 : Transparent async data length error
MAC residue	8 H	Resultant MR3 encrypted under LMK 10 (only if there is no error).
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.

28.8 Generate a Transaction Completion Response

Command: Generate a transaction Completion Response.

Notes: The command allows the Acquirer to use the TK that was used to process the original request/response. It does not use the new TK generated as a result of the response.

If the Host is unable to support binary data transfers, the command can be used in standard (ASCII character) asynchronous mode (in which the message to be MACed is transferred in expanded hexadecimal notation).

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RS.
Terminal key	16 H	TK encrypted under LMK pair 14-15.
AB	16 H	Formed in accordance with the terminal specification by the Host.
MAC residue	8 H	MR3 encrypted under LMK 10 from previous transaction.
EITHER		
For Binary Communications Modes:		
Message length	3 H	X'001 to X'320 indicating the length of the next field.
Message text	n B	1 to 800 bytes of message.
OR		
For Standard Async Communications Mode:		
Message length	3 H	X'002 to X'320 indicating the number of characters in the next field.
Message text	n H	2 to 800 hexadecimal characters representing 1 to 400 bytes of message.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value RT.
Error code	2 N	00 : No errors 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 80 : Message length error (including odd number of characters when using standard async mode) 90 : Communications link parity error 91 : Communications link LRC error 92 : Transparent async data length error
MAC	8 H	Resultant 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. Max. length 32 characters.

28.9 Verify a PIN at the Card Issuer Using the IBM Method

Command: Verify a PIN using the IBM algorithm and generate Auth Para at the Card Issuer.

Note: The command enables a Card Issuer to recover an encrypted PIN block sent by the Acquirer.

If a double or triple length PVK is used, Error Code 02 is returned as a warning but processing continues verifying the PIN using TDES in place of DES.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value QQ.
Source zone PIN key	16H or 1A+32H or 1A+48H	ZPK _s encrypted under LMK pair 06-07.
Destination zone PIN key	16H or 1A+32H or 1A+48H	ZPK _d encrypted under LMK pair 06-07.
PIN verification key	16H or 1A+32H or 1A+48H	PVK encrypted under LMK pair 14-15.
AB	16 H	
CD	16 H	
STAN	6 N	
CATID	16 H	Representing the 64 bit field.
AT	12 H	
Maximum PIN length	2 N	Value 12.
PIN block	16 H	As received from acquirer.
PIN block format code	2 N	One of the valid format codes.
Check length	2 N	
Account number	12 N	
Decimalization table	16 N	
PIN validation data	16 H	Note: This must be the full 16-hexadecimal character field, exactly as it is to be used.
Offset	12 N	
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value QR.
Error code	2 N	00 : No errors 01 : PIN verification 02 : Warning PVK not single length 10 : ZPK _s parity error 11 : ZPK _d or PVK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block does not contain valid values 21 : Invalid user storage index 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits in length 90 : Communications link parity error 91 : Communications link LRC error 92 : Transparent async data length error
Auth Para	16 H	Auth Para encrypted under a variant of ZPK _d (only if there is no error).
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.

28.10 Verify a PIN at the Card Issuer Using the Diebold Method

Command: Verify a PIN using the Diebold algorithm and generate Auth Para at the Card Issuer.

Notes: The command enables a Card Issuer to recover an encrypted PIN block sent by the Acquirer.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value QS.
Source zone PIN key	16H or 1A+32H or 1A+48H	ZPK _s encrypted under LMK pair 06-07.
Destination zone PIN key	16H or 1A+32H or 1A+48H	ZPK _d encrypted under LMK pair 06-07.
PIN verification key	16 H	PVK encrypted under LMK pair 14-15.
AB	16 H	
CD	16 H	
STAN	6 N	
CATID	16 H	Representing the 64 bit field.
AT	12 H	
Index flag	1 A	Value K.
Index pointer	3 H	Points at Diebold table.
Algorithm number	2 H	Diebold algorithm required.
PIN block	16 H	
PIN block format code	2 N	One of the valid format codes.
Account number	12 N	
Validation data	20 H	Note: This must be the full 20-hexadecimal character field, exactly as it is to be used.
Offset	4 N	
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value QT.
	2 N	00 : No errors 01 : PIN verification 10 : ZPK _s parity error 11 : ZPK _d or PVK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block does not contain valid values 21 : Invalid user storage index 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits in length 90 : Communications link parity error 91 : Communications link LRC error 92 : Transparent async data length error
Auth Para	16 H	Auth Para encrypted under a variant of ZPK _d (only if there is no error).
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.

28.11 Verify a PIN at the Card Issuer Using the Visa Method

Command: Verify a PIN using the Visa PVV and generate Auth Para at the Card Issuer.

Note: The command enables a Card Issuer to recover an encrypted PIN block sent by the Acquirer.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value QU.
Source zone PIN key	16H or 1A+32H or 1A+48H	ZPK _s encrypted under LMK pair 06-07.
Destination zone PIN key	16H or 1A+32H or 1A+48H	ZPK _d encrypted under LMK pair 06-07.
PVK	32H or 1A+32H	PVK encrypted under LMK pair 14-15.
AB	16 H	
CD	16 H	
STAN	6 N	
CATID	16 H	Representing the 64 bit field.
AT	12 H	
PIN block	16 H	As received from the acquirer.
PIN block format code	2 N	One of the valid format codes.
Account number	12 N	
PVKI	1 N	
PVV	4 N	
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value QV.
Error code	2 N	00 : No errors 01 : PIN verification 10 : ZPK _s parity error 11 : ZPK _d or PVK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 20 : PIN block does not contain valid values 21 : Invalid user storage index 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits in length 27 : PVK not double length 90 : Communications link parity error 91 : Communications link LRC error 92 : Transparent async data length error
Auth Para	16 H	Auth Para encrypted under a variant of ZPK _d (only if there is no error).
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.

28.12 Verify a PIN at the Card Issuer by Comparison

Command: Verify a PIN by comparison and generate Auth Para at the Card Issuer.

Notes: The command enables a Card Issuer to recover an encrypted PIN block sent by the Acquirer.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value QW.
Source zone PIN key	16H or 1A+32H or 1A+48H	ZPK _s encrypted under LMK pair 06-07.
Destination zone PIN key	16H or 1A+32H or 1A+48H	ZPK _d encrypted under LMK pair 06-07.
AB	16 H	
CD	16 H	
STAN	6 N	
CATID	16 H	Representing the 64 bit field.
AT	12 H	
PIN block	16 H	As received from the acquirer.
PIN block format code	2 N	One of the valid format codes.
Account number	12 N	
PIN	L N	Encrypted under LMK pair 02-03 from Host database. L is the encrypted PIN length.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value QX.
Error code	2 N	00 : No errors. 01 : PIN verification 10 : ZPK _s parity error 11 : ZPK _d or PVK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 14: Error in PIN from Host database 15 : Error in input data 20 : PIN block does not contain valid values 21 : Invalid user storage index 23 : Invalid PIN block format code 24 : PIN is fewer than 4 or more than 12 digits in length 90 : Communications link parity error 91 : Communications link LRC error 92 : Transparent async data length error
Auth Para	16 H	Auth Para encrypted under a variant of ZPK _d (only if there is no error).
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.

28.13 Generate Auth Para at the Card Issuer

Command: Generate Auth Para at the Card Issuer.

Note: The command enables the Card Issuer to generate Auth Para when no PIN is to be verified, but the CD fields are not known at the Acquirer. Auth Para is returned encrypted under a variant of a Zone PIN key (ZPK).

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value RU.
Source zone PIN key	16H or 1A+32H or 1A+48H	ZPK encrypted under LMK pair 06-07.
AB	16 H	
CD	16 H	
STAN	6 N	
CATID	16 H	Representing the 64 bit field.
AT	12 H	
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value RV.
Error code	2 N	00 : No errors 10 : ZPK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 90 : Communications link parity error 91 : Communications link LRC error 92 : Transparent async data length error
Auth Para	16 H	Auth Para encrypted under a variant of ZPK _d (only if there is no error).
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.

28.14 Message Authentication Mode Numbers

The MAC commands specified in the following sections have associated "mode" numbers in the range 0 to 3, as follows:

- Mode 0: Normal mode. Used to generate the MAC for a message which completely fits in the HSM buffer, which is 800 bytes or characters long.
- Mode 1: Extended message (first block). Used to process the first 800 characters (maximum) of a message greater than 800 characters. The output is an intermediate value to be used as the Initialisation Vector for the next stage.
- Mode 2: Extended message (middle block(s)). Used to process each complete 800 (maximum) character block after the first block for a message that exceeds 1600 characters. Requires an Initialisation Vector, and produces one for the next stage.
- Mode 3: Extended message (last block). Used to process the last block of less than 800 characters of an extended message. Requires an Initialisation Vector, and produces the final MAC.

For binary MAC functions, using modes 1 and 2, the number of message bytes supplied must be a multiple of eight, otherwise a length error (error 80) is returned. For MAC functions where binary data is input as two hexadecimal characters, the number of characters supplied must be a multiple of sixteen (i.e. 8 bytes when compressed).

For modes 0 and 3 the HSM appends binary zeros up to an eight byte (64 bit) boundary if insufficient data is supplied.

28.15 Generate a MAC on a Binary Message

Command: Generate a MAC on a binary message.

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

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value MU.
Mode number	1 N	The MAC calculation mode number: 0 to 3. 0: The only block. 1: The first block. 2: A middle block. 3: The last block
Terminal authentication key	16H or 1A+32H or 1A+48H	TAK encrypted under LMK pair 16-17.
Initialization vector	16 H	Modes 2,3. IV returned from either mode 1 or 2 encrypted under variant 1 of LMK pair 16-17.
EITHER		
For Binary Communications Modes:		
Message length	3 H	X'001 to X'320 indicating the length of the next field.
Message text	n B	1 to 800 bytes of message.
OR		
For Standard Async Communications Mode:		
Message length	3 H	X'002 to X'320 indicating the number of characters in the next field.
Message text	n H	2 to 800 hexadecimal characters representing 1 to 400 bytes of message.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value MV.
Error code	2 N	00 : No errors 10 : TAK parity error 12 : No keys loaded in user storage 13 : LMK error; report to supervisor 15 : Error in input data 21 : Invalid user storage index 27 : TAK not single length 80 : Message length error (including odd number of characters when using standard async mode) 90 : Communications link parity error 91 : Communications link LRC error 92 : Transparent async data length error
IV	16 H	Present only in modes 1 and 2. The IV encrypted under variant 1 of LMK pair 16-17.
MAC	8 H	Present only in modes 0 and 3.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

28.16 Verify a MAC on a Binary Message

Command: Verify a MAC on a binary message.

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

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value MW.
Mode number	1 N	The MAC calculation mode number: 0 to 3. 0: The only block. 1: The first block. 2: A middle block. 3: The last block
Terminal authentication key	16H or 1A+32H or 1A+48H	TAK encrypted under LMK pair 16-17.
Initialization vector (IV)	16 H	Modes 2,3. IV returned from either mode 1 or 2 encrypted under variant 1 of LMK pair 16-17.
MAC	8 H	Modes 0,3. The MAC received with the unsolicited message.
EITHER		
For Binary Communications Modes:		
Message length	3 H	X'001 to X'320 indicating the length of the next field.
Message text	n B	1 to 800 bytes of message.
OR		
For Standard Async Communications Mode:		
Message length	3 H	X'002 to X'320 indicating the number of characters in the next field.
Message text	n H	2 to 800 hexadecimal characters representing 1 to 400 bytes of message.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value MX.
Error code	2 N	00 : No errors. 01 : MAC verification failure. 10 : TAK parity error. 12 : No keys loaded in user storage. 13 : LMK error; report to supervisor. 15 : Error in input data. 21 : Invalid user storage index. 27 : TAK not single length. 80 : Message length error (including odd number of characters when using standard async mode). 90 : Communications link parity error. 91 : Communications link LRC error. 92 : Transparent async data length error.
IV	16 H	Present only in modes 1 and 2. The IV encrypted under variant 1 of LMK pair 16-17.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

29 USING THE OPTIONAL RSA CRYPTOSYSTEM

The RSA cryptosystem is available in the RG7100, RG7110, RG7200, RG7210, RG7300, RG7310, RG7710 and RG7400 operating in Async mode. It is not supported in the RG7500, RG7600 or RG7400 operating in Bisync mode.

When installed, the optional RSA cryptosystem provides the following functions:

- Generation of variable-length RSA keys.
- Validation of public key certificates.
- Generation and validation of digital signatures.
- Secure DES key management using RSA public master keys.
- Generation of hash values.

These functions are implemented by the host commands detailed in the following subsections:

- 29.1 Generate an RSA Key Set (EI)
- 29.2 Load a Secret Key (EK)
- 29.3 Translate a Secret Key from the Old LMK to a New LMK (EM)
- 29.4 Generate a MAC on a Public Key (EO)
- 29.5 Verify a MAC on a Public Key (EQ)
- 29.6 Validate a Certificate and Generate a MAC on its Public Key (ES)
- 29.7 Translate a MAC on a Public Key (EU)
- 29.8 Generate a Signature (EW)
- 29.9 Validate a Signature (EY)
- 29.10 Import a DES Key (GI)
- 29.11 Export a DES Key (GK)
- 29.12 Hash a Block of Data (GM)

Within these functions certain common parameters are defined as follows:

DES Key Type

The DES Key Type field is 4 digits. The first two digits indicate the LMK pair used to encrypt the key, the last two digits indicate the LMK variant. For example:

- If the DES Key Type is 0600, LMK pair 06-07 is used (no variant).
- If the DES Key Type is 3007, variant 7 of LMK pair 30-31 is used.

Signature Algorithm

01 = RSA

Encryption Identifier

01 = RSA

Hash Identifier

- 01 = SHA-1, produces a 20 byte result.
- 02 = MD5, produces a 16 byte result.
- 03 = ISO 10118-2, produces a 16 byte result.
- 04 = No hash.

01 = SHA-1 hashing algorithm

The ASN.1 DER object identifier for this hashing function is:

{iso(1) identified-organisation(3) oiw(14) secsig(3) 2 26}

which encodes as:

2B 0E 03 02 1A

02 = MD5 hashing algorithm

The ASN.1 DER object identifier for this hashing function is:

{iso(1) member-body(2) US(840) rsadsi(113549) digest Algorithm(2) 5 }

which encodes as:

2A 86 48 86 F7 0D 02 05

03 = ISO 10118-2 hashing algorithm

The ASN.1 DER object identifier for this hashing function is:

{2 10 67 4}

which encodes as:

5A 43 04

04 = No hash

The no-hash option can be used when the HSM provides signature generation or validation, or certificate validation, on data that is hashed outside the HSM.

If the no-hash option is chosen, the data that is provided in the Validate a Certificate, Generate a Signature and Validate a Signature commands is not modified in any way by the HSM, so it must be precisely the data in the plain signature block (which depends on the pad mode selected by the Pad Mode Identifier). It is the responsibility of the Host application to ensure that the precise data to be included in the signature block is supplied in the command.

Example:

If the SHA-1 algorithm is used to hash the data and the resultant hash value is:

0123456789ABCDEF0123456789ABCDEF01234567

and if the PKCS#1 pad mode is used, the data to be provided must be the complete ASN.1 DER encoded DigestInfo, which is:

30 21 300906052B0E03021A0500 04140123456789ABCDEF0123456789ABCDEF01234567.

Note that when using the no-hash mode, the HSM checks that the DER encoded DigestInfo syntax is correct. If there is a digest info syntax error, the HSM returns error code 74.

Pad Mode Identifier

01 = PKCS#1 v1.5

02 = OAEP

The PKCS#1 standard (see References 2 and 3 at the beginning of this manual) defines the padding method to be used before operating with a public or secret RSA key.

01 = PKCS#1 v1.5

This simple padding scheme was introduced in the original PKCS#1 specification. The data to be encrypted or decrypted is padded as follows:

00 BT PS 00 D, where:

- BT is a single byte indicating the block type. BT is 01 for a secret key operation; 02 for a public key operation.
- PS is a padding string consisting of bytes FF....FF for block type 01, random non-zero bytes for block type 02. PS must contain at least 8 bytes.
- D is the data block.
- The total length of the padded block is equal to the length (in bytes) of the RSA key modulus

The data block D is the ASN.1 encoded message digest, or DES key (depending on the command used), as follows:

DigestInfo ::	SEQUENCE {
digestAlgorithm	DigestAlgorithmIdentifier,
digest	OCTET STRING
}	
DigestAlgorithmIdentifier ::	SEQUENCE {
algorithm	OBJECT IDENTIFIER,
parameters	NULL
}	
KeyBlock ::	SEQUENCE {
deskey	OCTET STRING,
iv	OCTET STRING SIZE (8)
}	

Example 1:

Assume that the SHA-1 algorithm is used to produce the 20-byte digest:

0123456789ABCDEF0123456789ABCDEF01234567.

The DigestAlgorithmIdentifier for SHA-1 is:

30 09 06 05 2B0E03021A 05 00.

Thus, the ASN. 1 DER encoded DigestInfo is:

30 21 300906052B0E03021A0500 04140123456789ABCDEF0123456789ABCDEF01234567

Example 2:

If a single-length DES key 0123456789ABCDEF and IV = 9999999999999999 are used, the ASN. 1 DER encoding of KeyBlock is:

30 14 04080123456789ABCDEF 04089999999999999999.

When the PKCS#1 pad mode is used, the following validity checks are carried out:

For a validation operation (Validate a Certificate, Validate a Signature):

- The length of the data to be validated is equal to the length (in bytes) of the modulus of the key to be used for the validation. If not, error code 76 is returned.
- The first byte of the clear data block is 00. If not, error code 77 is returned.
- The second byte of the clear data block is 01. If not, error code 77 is returned.
- Subsequent bytes consist of at least 8 bytes of binary 1s, followed by a zero byte. If not, error code 77 is returned.
- The hash algorithm object identifier corresponds to that of the identifier of the hash algorithm supplied in the command message. If not, error code 79 is returned.
- The digest is compared with the hash of the supplied data. If the two values are not equal, error code 02 is returned.

For a generation operation (Generate a Signature):

- The length (in bytes) of the data block D is at most m-11 (where m is the length, in bytes, of the modulus of the key to be used). If not, error code 76 is returned.

For an import key operation (Import a DES Key):

- The length of the imported key block is equal to the length (in bytes) of the modulus of the secret key to be used to decrypt the block. If not, error code 76 is returned.
- The first byte of the clear data block is 00 and the second byte is 02. If not, error code 77 is returned.
- Subsequent bytes consist of at least 8 bytes of random non-zero bytes, followed by a zero byte. If not, error code 77 is returned.
- The data block D conforms to the ASN.1 encoding rules. If not, error code 77 is returned.

For an export key operation (Export a DES Key):

- The length (in bytes) of the data block D is at most m-11 (where m is the length, in bytes, of the modulus of the key to be used). If not, error code 76 is returned.

02 = OAEP

Optimal Asymmetric Encryption Padding (OAEP) was introduced in PKCS#1 v2.0, as an improvement on the original, simple PKCS#1 v 1.5 method described above. OAEP requires four additional parameters:

- **Mask Generation Function**
01 = MGF1
- **MGF Hash Function**
01 = SHA1
- **OAEP Encoding Parameters Length**
Specifies the length of the encoding parameters.
- **OAEP Encoding Parameters**
The host may optionally supply a set of OAEP encoding parameters. If OAEP padding is used, but no Encoding Parameters are required, then OAEP Encoding Parameters Length should be "00", and this field will be empty.

The OEAP fields are encoded according to PKCS#1 version 2.0 section 11.2.1 (see Reference 3 at the beginning of this manual). The HSM does not interpret or validate the contents of this field, it applies the Hash Algorithm to it and feeds the result into the OAEP process.

Key Block Type

- 01 = Standard Key Block Type
- 02 = Key Block Template
- 03 = Unformatted Key Block

This parameter specifies the type of data structure used to carry a DES key.

01 = Standard Key Block Type

This is the standard key block format as supported in versions 5.05/1.05 and 5.06/1.06 of the HSM firmware. The format is as shown in the PKCS#1v1.5 padding scheme above, i.e.:

```
KeyBlock ::=
deskey          SEQUENCE {
iv               OCTET STRING,
}                OCTET STRING SIZE (8)
```

02 = Key Block Template

This method supports any valid ASN.1 DER encoded Key Block format, which may consist of arbitrary encoded data with a Key Block field containing a plain-text DES Key of single, double or triple length.

The Host must supply a block of data, which conforms to ASN.1 DER encoding, with an indication of the position in which the key is located (DES Key Offset). The key data area of the template must be zero filled.

For key export, the HSM overlays the zero filled data with a DES or Triple DES key as appropriate.

For key import, the HSM will verify that the decrypted data conforms to the specified padding, than check that the supplied template matches the decoded data. It will then extract the data at the position indicated by the DES Key Offset, and use this as the key for import.

An example Key Block structure and template is shown below. This structure is used for Diebold Remote Key Transport:

Example Key Block Structure

RecipientInfo ::=	SEQUENCE {
version	Version,
issuerAndSerialNumber	IssuerAndSerialNumber,
keyEncryptionAlgorithm	KeyEncryptionAlgorithmIdentifier,
keyOrKeyBlock	KeyOrKeyBlock}
KeyOrKeyBlock ::=	CHOICE {
encryptedKey	EncryptedKey
EncryptedKeyBlock	encryptedKeyBlock}
EncryptedKey ::=	OCTET STRING
EncryptedKeyBlock ::=	ENCRYPTED KeyBlock – a BIT STRING
KeyBlock ::=	SEQUENCE {
version	Version, -- 0
originatorIssuerAndSerialNumber	IssuerAndSerialNumber,
keyId	KeyId,
key	Key,
keyUsage [0]	KeyUsage OPTIONAL}

Example Key Block Template

A key block template corresponding to the above structure is shown below:

30 61	KeyBlock
02 01 00	version = 0
30 47	originatorIssuerAndSerialNumber
30 42	issuer
31 10	
30 0E	
06 03 55 04 03	attributeType = commonName
13 07 52 6F 6F 74 20 43 41	attributeValue = "Root CA"
31 2E	
30 2C	
06 03 55 04 0A	attributeType = organizationName
13 25	attributeValue = "Initial Certificate Authority Company"
49 6E 69 74 69 61 6C 20 43 65 72 74 69	
66 69 63 61 74 65 20 41 75 74 68 6F 72	
69 74 79 20 43 6F 6D 70 61 6E 79	
02 01 02	serialNumber = 2
02 01 00	keyIdentifier = 0, A key
04 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	key

The Key Block Template requires four additional parameters:

- **Key Block Template Length**
The length of the key block data
- **Key Block Template**
The actual template, as shown in the example above
- **DES Key Length**
The length of the DES key within the key block.
- **DES Key Offset**
Offset to the location of the DES key within the key block. In the example above this points to the beginning of the block of zeros shown in bold italics and the offset is 83 (decimal) bytes.

Another two optional parameters support a check value. The Check Value is not required for the Diebold implementation, but provides flexibility to support applications that require a check value in the key block.

- **Check Value Length**
Length in bytes of the check value field. This field should be 0 if no check value is used.
- **Check Value Offset**
Offset to the location of the check value within the key block.

03 = Unformatted Key Block

This is the format required for remote ATM key loading for NCR ATMs. It consists of only 8, 16 or 24 bytes of key data (for a single, double or triple length DES key), with no encoding or additional information.

Public Key Encoding

01 = DER encoding for ASN.1 public key

An ASN.1 RSA PublicKey has the following definition:

```
RSA PublicKey ::= SEQUENCE {
    modulus           INTEGER, -- n
    publicExponent   INTEGER -- e }
```

Sequence Identifier	Byte Length	Integer Identifier	Modulus length	Modulus	Integer Identifier	Exponent length	Exponent
---------------------	-------------	--------------------	----------------	---------	--------------------	-----------------	----------

Example:

For a 1024 bit modulus with an exponent of 03:

X'30	X'81 X'86	X'02	X'81 X'80	128 byte Modulus	X'02	X'01	X'03
------	-----------	------	-----------	------------------	------	------	------

Where:

- X'30 is the identifier specifying the start of a sequence.
- X'81 X'86 specifies the length of the following field in bytes:
 - If value is between X'01 and X'7F then this directly specifies length of following field in bytes (1byte to 127 bytes).
 - If value is greater than X'80 it defines the number of bytes to define the length of the next field in the above example X'81 therefore length i.e. 1 byte (X'86 - 134 bytes).
- X'02 is the identifier specifying the start of the integer.
- X'81 X'80 specifies the length of the following field in bytes using the same definition as above (128 Bytes).
- The modulus in this example is 128 bytes.
- X'02 is the identifier specifying the start of the second integer.
- X'01 specifies the length of the following field in bytes using the same definition as above (1 Byte).
- X'03 is the value of the exponent.

29.1 Generate an RSA Key Set

Command: Generate an RSA key set.

Notes: Depending on key size, the function may take several minutes to execute.

The HSM must be in the Authorised state.

If a Public Exponent is supplied in the command message, it must be an odd value (i.e. the least-significant bit must be 1). If an even Public Exponent is supplied, an error code is returned.

Field	Length & Type	Details
COMMAND MESSAGE		
Message Header	m A	(Subsequently returned to the Host unchanged).
Command Code	2 A	Value E1.
Key type	1 N	Key type indicator: 0 : Signature only 1 : Key management only 2 : Both signature and key management
Key length	4 N	Modulus length in bits. Minimum 0320, maximum 2048 for all key types.
Public key encoding	2 N	Encoding rules for public key (must allow public key length to be inferred).
Public exponent length	4 N	Optional. Must be present if a public exponent is supplied. Indicates the length (in bits) of the public exponent.
Public exponent	n B	Optional. Must be an odd value. If not supplied, a default exponent of 65537 is assumed.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value EJ.
Error code	2 N	00 : No errors 03 : Invalid public key encoding type 04 : Length error 05 : Invalid key type 06 : Public exponent length error 08 : Supplied public exponent is even 13 : LMK error; report to supervisor 15 : Error in input data 17 : Not in Authorized state 47 : DSP error; report to supervisor
Public key	n B	Public key, encoded appropriately.
Secret key length	4 N	Length (in bytes) of the next field.
Secret key	n B	Secret key, encrypted under 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.

29.2 Load a Secret Key

Command: Load a secret key (encrypted using LMK pair 34-35) into the HSM's tamper-protected memory.

Notes: It is the responsibility of the Host application to ensure that a previously-loaded secret key is not accidentally overwritten by this command.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value EK.
Key index	2 N	Index number for secret key to be stored (used if multiple storage of keys is required). Standard HSM: must be set to 00. High-Speed HSM: can be 00 to 20.
Secret key length	4 N	Length (in bytes) of the next field.
Secret key	n B	Secret key, encrypted under LMK pair 34-35.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value EL.
Error code	2 N	00 : No error 03 : Invalid key index 04 : Insufficient memory for secret key storage 13 : LMK error; report to supervisor 15 : Error in input data 49 : Secret key error; report to supervisor 78 : Secret key length error
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.

29.3 Translate a Secret Key from the Old LMK to a New LMK

Command: Translate a secret key from encryption under the old LMK pair 34-35 held in key change storage, to encryption under a new LMK pair 34-35.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value EM.
Secret key length	4 N	Length (in bytes) of the next field.
Secret key	n B	Secret key, encrypted under LMK pair 34-35.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value EN.
Error code	2 N	00 : No error 13 : LMK error; report to supervisor 15 : Error in input data 49 : Secret key error; report to supervisor 78 : Secret key length error
Secret key length	4 N	Length (in bytes) of the next field.
Secret key	n B	Secret key, encrypted under new 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.

29.4 Generate a MAC on a Public Key

Command: Generate a MAC on an uncertified public key, using LMK pair 36-37.

Notes: The function can be used, for example, to protect a certification authority public key.

The HSM must be in the Authorised state.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value EO.
Public key encoding	2 N	Encoding rules for the supplied public key (must allow the public key length to be inferred).
Public key	n B	Public key.
Authentication data	n A	Optional. Additional data to be included in the MAC calculation (must not include ";").
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value EP.
Error code	2 N	00 : No error 03 : Invalid public key encoding type 04 : Public key does not conform to encoding rules 13 : LMK error; report to supervisor 15 : Error in input data 17 : Not in Authorized state
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.
Public key	n B	Public key, DER encoded in ASN. 1 format (sequence of modulus, exponent).
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.

29.5 Verify a MAC on a Public Key

Command: Verify a MAC on a public key, using LMK pair 36-37.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value EQ.
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.
Public key	n B	Public key, DER encoded in ASN.1 format (sequence of modulus, exponent).
Authentication data	n A	Optional. Additional data to be included in the MAC calculation (must not include ";").
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value ER.
Error code	2 N	00 : No error 01 : MAC verification failure 04 : Public key does not conform to encoding rules 13 : LMK error; report to supervisor 15 : Error in input 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.

29.6 Validate a Certificate and Generate a MAC on its Public Key

Command: Validate a certificate and generate a MAC on the public key contained in the certificate, using LMK pair 36-37.

Notes: The command can (optionally) check whether the public key in the certificate corresponds to a secret key encrypted under the LMK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value ES.
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.
Public key	n B	Public key, DER encoded in ASN.1 format (sequence of modulus, exponent).
Authentication data	n A	Optional. Additional data to be included in the MAC calculation (must not include ";").
Delimiter	1 A	Delimiter, indicates the end of the authentication data field. Value ";".
Certificate length	4 N	Certificate length (in bytes).
Hash offset	4 N	Offset to the first byte in the certificate data to be included in the hash calculation.
Hash length	4 N	Length (in bytes) of the data within the certificate which is included in the hash calculation.
Signature offset	4 N	Offset to the first byte of the signature contained in the certificate data.
Signature length	4 N	Length (in bytes) of the signature contained in the certificate data.
Certificate	n B	Certificate data to be validated.
Delimiter	1 A	Delimiter, indicates the end of the certificate field. Value ";".
Hash identifier	2 N	Identifier of the hash algorithm used to hash the certificate data.
Signature algorithm	2 N	Identifier of the signature algorithm used to sign the certificate data.
Pad mode identifier	2 N	Identifier of the pad mode used in certificate signature generation. 01 = PKCS#1 v1.5 method 02 = OAEP
Mask Generation Function	2N	01 = MGF1 as defined in PKCS#1 v2.0 (see Reference 3) Optional, only present if PAD Mode Identifier is 02 (OAEP)
MGF Hash Function	2N	01 = SHA-1 This field defines the hash function to be used in the MGF. Optional, only present if Pad Mode Identifier is 02 (OAEP)
OAEP Encoding Parameters Length	2N	Optional, only present if Pad Mode Identifier is 02 (OAEP).

Field	Length & Type	Details
OAEP Encoding Parameters	NB	Optional, only present if Pad Mode Identifier is 02 (OAEP) If present, this field should be encoded according to Reference 3 section 11.2.1. The HSM does not interpret or validate the contents of this field. If OAEP padding is used, but no Encoding Parameters are provided, then OAEP Parameters Length should be "00", and this field will be empty.
OAEP Encoding Parameters Delimiter	1A	Value ";".
Public key encoding	2 N	Optional, only present if Pad Mode Identifier is 02 (OAEP) Encoding rules for the public key contained in the certificate (must allow the public key length to be inferred).
Public key offset	4 N	Offset to the first byte of the public key field contained in the certificate
Authentication data	n A	Optional. Additional data to be included in the MAC calculation (must not include ";").
Delimiter	1 A	Delimiter, indicates the end of the authentication data field. Value ";" .
Secret key length	4 N	Optional. Length (in bytes) of the next field. Must be present if the secret key field is present.
Secret key	n B	Optional. Secret key, encrypted under LMK pair 34-35.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value ET.
Error code	2 N	00 : No error 01 : MAC verification failure 02 : Certificate validation failure 03 : Invalid public key encoding type 04 : Public key does not conform to encoding rules 05 : Invalid hash identifier 06 : Invalid signature identifier 07 : Invalid pad mode identifier 13 : LMK error; report to supervisor 15 : Error in input data 47 : DSP error; report to supervisor 49 : Secret key error; report to supervisor 74 : Invalid digest info syntax (no-hash mode only) 75 : Invalid public key / secret key pair 76 : Public key length error 77 : Clear data block error 78 : Secret key length error 79 : Hash algorithm object identifier error 80 : Certificate length error 81 : Certificate offset and length error 85 : Invalid OAEP Mask Generation Function 86 : Invalid OAEP MGF Hash Function 87 : OAEP Parameter Error 88 : OAEP Error
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.
Public key	n B	Public key, DER encoded in ASN. 1 format (sequence of modulus, exponent).
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.

29.7 Translate a MAC on a Public Key

Command: Verify a MAC on a public key, using old LMK pair 36-37, held in key change storage, and calculate a MAC using the new LMK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value EU.
MAC	4 B	MAC on the public key and authentication data, calculated using old LMK pair 36-37.
Public key	n B	Public key, DER encoded in ASN.1 format (sequence of modulus, exponent).
Authentication data	n A	Optional. Additional data to be included in the MAC calculation (must not include ";").
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value EV.
Error code	2 N	00 : No error 01 : MAC verification failure 04 : Public key does not conform to encoding rules 13 : LMK error; report to supervisor 15 : Error in input data
MAC	4 B	MAC on the public key and authentication data, calculated using new LMK pair 36-37.
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.

29.8 Generate a Signature

Command: Generate a signature on a message using a secret key.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value EW.
Hash identifier	2 N	Identifier of the hash algorithm used to hash the message.
Signature Identifier	2 N	Identifier of the signature algorithm used to sign the message.
Pad mode identifier	2 N	Identifier of the pad mode used in signature generation. 01 = PKCS#1 v1.5 method 02 = OAEP
Mask Generation Function	2N	01 = MGF1 as defined in PKCS#1 v2.0 (see Reference 3) Optional, only present if PAD Mode Identifier is 02 (OAEP)
MGF Hash Function	2N	01 = SHA-1 This field defines the hash function to be used in the MGF. Optional, only present if Pad Mode Identifier is 02 (OAEP)
OAEP Encoding Parameters Length	2N	Optional, only present if Pad Mode Identifier is 02 (OAEP).
OAEP Encoding Parameters	NB	Optional, only present if Pad Mode Identifier is 02 (OAEP) If present, this field should be encoded according to Reference 3 section 11.2.1. The HSM does not interpret or validate the contents of this field. If OAEP padding is used, but no Encoding Parameters are provided, then OAEP Parameters Length should be "00", and this field will be empty.
OAEP Encoding Parameters Delimiter	1A	Value ";". Optional, only present if Pad Mode Identifier is 02 (OAEP).
Data length	4 N	Length (in bytes) of the message data to be signed.
Message data	n B	Data to be signed.
Delimiter	1 A	Delimiter, indicates the end of the message data field. Value ";".
Secret key flag	2 N	Flag, indicates the location of the secret key. The number is the index of the stored secret key, except 99 which means use the key supplied in the command.
Secret key length	4 N	Length (in bytes) of the next field (present only if the secret key flag is 99).
Secret key	n B	Secret key, encrypted using LMK pair 34-35 (present only if the secret key flag is 99).
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value EX.
Error code	2 N	00 : No error 03 : Invalid secret key type 04 : Invalid secret key flag 05 : Invalid hash identifier 06 : Invalid signature identifier 07 : Invalid pad mode identifier 13 : LMK error; report to supervisor 15 : Error in input data 47 : DSP error; report to supervisor 49 : Secret key error; report to supervisor 74 : Invalid digest info syntax (no-hash mode only) 76 : Hash length error 78 : Secret key length error 80 : Message length error 85 : Invalid OAEP Mask Generation Function 86 : Invalid OAEP MGF Hash Function 87 : OAEP Parameter Error 88 : OAEP Error
Signature length	4 N	Length (in bytes) of the signature.
Signature	n B	Calculated 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.

29.9 Validate a Signature

Command: Validate a signature on a message using a public key.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value EY.
Hash identifier	2 N	Identifier of the hash algorithm used to hash the message.
Signature Identifier	2 N	Identifier of the signature algorithm used to sign the message.
Pad mode identifier	2 N	Identifier of the pad mode used in signature generation. 01 = PKCS#1 v1.5 method 02 = OAEP
Mask Generation Function	2N	01 = MGF1 as defined in PKCS#1 v2.0 (see Reference 3) Optional, only present if PAD Mode Identifier is 02 (OAEP)
MGF Hash Function	2N	01 = SHA-1 This field defines the hash function to be used in the MGF. Optional, only present if Pad Mode Identifier is 02 (OAEP)
OAEP Encoding Parameters Length	2N	Optional, only present if Pad Mode Identifier is 02 (OAEP).
OAEP Encoding Parameters	NB	Optional, only present if Pad Mode Identifier is 02 (OAEP) If present, this field should be encoded according to Reference 3 section 11.2.1. The HSM does not interpret or validate the contents of this field. If OAEP padding is used, but no Encoding Parameters are provided, then OAEP Parameters Length should be "00", and this field will be empty.
OAEP Encoding Parameters Delimiter	1A	Value ";". Optional, only present if Pad Mode Identifier is 02 (OAEP)
Signature length	4 N	Signature length (in bytes).
Signature	n B	Signature to be verified.
Delimiter	1 A	Delimiter, indicates the end of the signature field. Value ";".
Data length	4 N	Length (in bytes) of the message data to be validated.
Message data	n B	Data to be validated.
Delimiter	1 A	Delimiter, indicates the end of the message data field. Value ";".
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.
Public key	n B	Public key, DER encoded in ASN.1 format (sequence of modulus, exponent).
Authentication data	n A	Optional. Additional data to be included in the MAC calculation (must not include ";").
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value EZ.
Error code	2 N	00 : No error 01 : MAC verification failure 02 : Signature verification failure 04 : Public key does not conform to encoding rules 05 : Invalid hash identifier 06 : Invalid signature identifier 07 : Invalid pad mode identifier 13 : LMK error; report to supervisor 15 : Error in input data 47 : DSP error; report to supervisor 74 : Invalid digest info syntax (no-hash mode only) 76 : Public key length error 77 : Clear data block error 79 : Hash algorithm object identifier error 80 : Message length error 81 : Signature length error 85 : Invalid OAEP Mask Generation Function 86 : Invalid OAEP MGF Hash Function 87 : OAEP Parameter Error 88 : OAEP Error
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.

29.10 Import a DES Key

Command: To translate a DES key from encryption under a public key to encryption under the LMK.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value GI.
Encryption identifier	2 A	Identifier of the algorithm used to encrypt the DES key.
Pad mode identifier	2 N	Identifier of the pad mode used in the encryption process: 01 = PKCS#1 v1.5 method 02 = OAEP
Mask Generation Function	2N	01 = MGF1 as defined in PKCS#1 v2.0 (see Reference 3) Optional, only present if PAD Mode Identifier is 02 (OAEP)
MGF Hash Function	2N	01 = SHA-1 This field defines the hash function to be used in the MGF. Optional, only present if Pad Mode Identifier is 02 (OAEP)
OAEP Encoding Parameters Length	2N	Optional, only present if Pad Mode Identifier is 02 (OAEP).
OAEP Encoding Parameters	NB	Optional, only present if Pad Mode Identifier is 02 (OAEP) If present, this field should be encoded according to Reference 3 section 11.2.1. The HSM does not interpret or validate the contents of this field. If OAEP padding is used, but no Encoding Parameters are provided, then OAEP Parameters Length should be "00", and this field will be empty.
OAEP Encoding Parameters Delimiter	1A	Value ";". Optional, only present if Pad Mode Identifier is 02 (OAEP)
DES key type	4 N	Indicates the required LMK pair, including the LMK variant.
Encrypted key length	4 N	Length (in bytes) of the encrypted DES key.
DES key (PK)	n B	DES key, encrypted under the public key.
Delimiter	1 A	Delimiter, indicates the end of the encrypted DES key field. Value ";".
Secret key flag	2 N	Flag, indicates the location of the secret key. The number is the index of the stored secret key, except 99 which means use the key supplied in the command.
Secret key length	4 N	Length (in bytes) of the next field (present only if the secret key flag is 99).
Secret key	n B	Secret key, encrypted using LMK pair 34-35 (present only if the secret key flag is 99).
Delimiter	1 A	Optional. If present the following three fields must be present. Value ";".
Key scheme ZMK	1 A	Optional. Key scheme for encrypting key under ZMK.
Key scheme LMK	1 A	Optional. Key scheme for encrypting key under LMK.

Field	Length & Type	Details
Key check value type	1 A	Optional. Key check value calculation method 0 - KCV backwards compatible. 1 - KCV 6H.
Delimiter	1A	Value “=”. Only Present if Key Block Type follows Note: The “=” delimiter is used to distinguish from the normal “;” delimiter.
Key Block Type	2N	01 = Key Block format backward compatible with 5.06/1.06 firmware 02 = Key Block Template 03 = Unformatted Key Block Only present if the “=” delimiter above is present.
Key Block Template Length	4N	Length of Key Block data Only present if Key Block Type = 02.
Key Block Template	NH	Key Block, DER encoded in ASN.1 format. Key data zero filled. Only present if Key Block Type = 02.
Delimiter	1A	Value “,”. Only present if Key Block Type = 02.
DES Key Offset	4N	Offset to the location of the DES Key within the Key Block Only present if Key Block Type = 02.
Check value length	1N	Length in bytes of Check value field. Permitted values 0-8. If no check value is supplied then this field will be 0. If Check Value is supplied then the HSM will perform a validation check using the extracted DES key. If Key Block Type = 02 then Check Value is expected at position indicated by Check Value Offset. Only present if Key Block Type = 02.
Check value offset	4N	Offset to the location of the check value within the Key Block. If Check Value length is 00 then this field is ignored. Only present if Key Block Type = 02.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value GJ.
Error code	2 N	00 : No error 03 : Invalid secret key type 04 : Invalid secret key flag 05 : Invalid DES key type 06 : Invalid encryption identifier 07 : Invalid pad mode identifier 13 : LMK error; report to supervisor 15 : Error in input data 47 : DSP error; report to supervisor 49 : Secret key error; report to supervisor 76 : Key block length error 77 : Clear data block error 78 : Secret key length error 80 : Encrypted DES key length error 81 : Invalid Key Block type 82 : Invalid check value length 83 : Key block format error 84 : Key block check value error 85 : Invalid OAEP Mask Generation Function 86 : Invalid OAEP MGF Hash Function 87 : OAEP Parameter Error 88 : OAEP Error
Initialization value	16 H	Initialization value for the DES key. Optional. Only present if Key Block Type = 01.
DES key (LMK)	16H or 32H or 1A+32H or 1A+48H	DES key, encrypted under the LMK pair indicated by the DES key type.
Key check value	16 H or 6 H	Check value on the DES key. 16H or 6H depends upon KCV type option.
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.

29.11 Export a DES Key

Command: Translate a DES key from encryption under an LMK pair to encryption under a public key.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value GK.
Encryption identifier	2 A	Identifier of the algorithm used to encrypt the DES key.
Pad mode identifier	2 N	Identifier of the pad mode used in the encryption process. 01 = PKCS#1 v1.5 method 02 = OAEP
Mask Generation Function	2N	01 = MGF1 as defined in PKCS#1 v2.0 (see Reference 3) Optional, only present if PAD Mode Identifier is 02 (OAEP)
MGF Hash Function	2N	01 = SHA-1 This field defines the hash function to be used in the MGF. Optional, only present if Pad Mode Identifier is 02 (OAEP)
OAEP Encoding Parameters Length	2N	Optional, only present if Pad Mode Identifier is 02 (OAEP).
OAEP Encoding Parameters	NB	Optional, only present if Pad Mode Identifier is 02 (OAEP) If present, this field should be encoded according to Reference 3 section 11.2.1. The HSM does not interpret or validate the contents of this field. If OAEP padding is used, but no Encoding Parameters are provided, then OAEP Parameters Length should be "00", and this field will be empty.
OAEP Encoding Parameters Delimiter	1A	Value ";". Optional, only present if Pad Mode Identifier is 02 (OAEP)
DES key type	4 N	Indicates the required LMK pair, including the LMK variant.
DES key flag	1 N	Flag indicates the length of the DES key: 0 : single-length key 1 : double-length key 2 : triple-length key
DES key (LMK)	16H or 32H or 1A+32H or 1A+48H	DES key, encrypted under the LMK pair indicated by DES key type (length indicated by DES key flag).
Check value	16 H	Check value on the DES key.
MAC	4 B	MAC on the public key and authentication data, calculated using LMK pair 36-37.
Public key	n B	Public key, DER encoded in ASN.1 format (sequence of modulus, exponent). Modulus length 0320 to 2048 bits.
Authentication Data	n A	Optional. Additional data to be included in the MAC calculation (must not include ";").
Delimiter	1A	Value ";". Only Present if the Key Block Type below is present.

Field	Length & Type	Details
Key Block Type	2N	01 = Key Block format backward compatible with 5.06/1.06 firmware 02 = Key Block Template (format of template is specified below) 03 = Unformatted Key Block This field is Optional for Key Block Type 01, but must be provided if alternative Key Block Type is used.
Key Block Template Length	4N	Length of Key Block data Optional. Only present if Key Block Type = 02.
Key Block Template	NH	Key Block, DER encoded in ASN.1 format. Key data and Check Value data (if present) zero filled. Optional. Only present if Key Block Type = 02.
Delimiter	1A	Value ";". Optional. Only present if Key Block Type = 02.
DES Key Offset	4N	Offset to the position within the Key Block to insert the DES Key Optional. Only present if Key Block Type = 02.
Check value length	2N	Length in bytes of Check value field. Permitted values 0-8. If no check value is required then this field will be 0. If Check Value is supplied then the HSM will generate a check value and include it in the Key Block. If Key Block Type = 02 then Check Value is inserted at position indicated by Check Value Offset. Optional. Only present if Key Block Type = 02.
Check Value Offset	4N	Offset to the position within the Key Block to insert a check value. If Check Value length is 0 then this field is ignored. Optional. Only present if Key Block Type = 02.
End message delimiter	1 C	Optional. 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	n A	Returned to the Host unchanged.
Response code	2 A	Value GL.
Error code	2 N	00 : No error 01 : MAC verification failure 02 : Check value verification failure 04 : Public key does not conform to encoding rules 05 : Invalid DES key type 06 : Invalid encryption identifier 07 : Invalid pad mode identifier 10 : Key parity error 13 : LMK error ; report to supervisor 15 : Error in input data 47 : DSP error; report to supervisor 51 : Invalid Key Block Type 76 : Public key length error 81: Invalid Key Block type 82 : Invalid check value length 83 : Key block format error 84 : Key block check value error 85 : Invalid OAEP Mask Generation Function 86 : Invalid OAEP MGF Hash Function 87 : OAEP Parameter Error 88 : OAEP Error
Initialization value	16 H	Initialization value for the DES key. Optional. Only present if Key Block Type = 01.
DES key length	4 N	Length (in bytes) of the next field.
DES key (PK)	n B	DES key, encrypted under the public key.
End message delimiter	1 C	Present only if present in the command message. Value X'19.
Message trailer	n A	Present only if present in the command message. Maximum length 32 characters.

29.12 Hash a Block of Data

Command: Hash a block of data.

Notes: It is the responsibility of the application program to ensure that the amount of data supplied in this command does not cause a buffer overflow.

Field	Length & Type	Details
COMMAND MESSAGE		
Message header	m A	(Subsequently returned to the Host unchanged).
Command code	2 A	Value GM.
Hash identifier	2 N	Identifier of the hash algorithm used to hash the data.
Data length	5 N	Length of the message data to be hashed.
Message data	n B	Data to be hashed.
End message delimiter	1 C	Optional. Must be present if a message trailer is present. Value X'19.
Message trailer	n A	Optional. Maximum length 32 characters.
RESPONSE MESSAGE		
Message header	n A	Returned to the Host unchanged.
Response code	2 A	Value GN.
Error code	2 N	00 : No error 05 : Invalid hash identifier 15 : Error in input data 80 : Data length error
Hash value	n B	Hash result (length depends on the algorithm used)
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

PIN BLOCK FORMATS

1	GENERAL	3-1
2	FORMAT 01	3-2
3	FORMAT 02	3-3
4	FORMAT 03	3-4
5	FORMAT 04	3-5
6	FORMAT 05	3-6
7	FORMAT 34	3-7
8	FORMAT 35	3-8
9	FORMAT 41	3-9
10	FORMAT 42	3-10

1 GENERAL

For PIN verification and PIN translation, the HSM requires the PIN to be input as a 16-digit PIN block. The HSM supports a number of PIN block formats, each identified by a 2-digit PIN block format code. Formats 34, 35, 41 and 42 are used for EMV PIN change operations and are only available to the KU command.

2 FORMAT 01

Format 01 is the format adopted by the American National Standards Institute (ANSI X9.8) and is one of two formats supported by the International Standards Organisation (ISO 95641 - format 0).

The format combines the customer PIN and account number as follows:

- A 16-digit block is made from the digit 0, the length of the PIN, the PIN, and a pad character (hexadecimal F). For example, for the 5-digit PIN 92389, the block is:

0592 389F FFFF FFFF

- Another 16-digit block is made from four zeros and the 12 right-most digits of the account number, excluding the check digit. For example, for the 13-digit account number 4000 0012 3456 2, where the check digit is 2, the block is:

0000 4000 0012 3456

- The two blocks are exclusive-OR added:

	05	92	38	9F	FF	FF	FF	FF
	00	00	40	00	00	12	34	56
PIN block:	05	92	78	9F	FF	ED	CB	A9

3 FORMAT 02

Format 02 supports Docutel ATMs. A PIN block is created from the PIN length, a 6-digit PIN, and a user-defined numeric padding string.

If the PIN has fewer than 6 digits, it is left-justified and zero filled.

For example, for the 5-digit PIN 92389, the PIN digits are 923890.

With pad characters added, the PIN block could be, for example:

5923 8909 8765 4321

where 98765 4321 is the padding string.

4 FORMAT 03

Format 03 supports Diebold and IBM ATMs. It also applies to the Docutel format that does not include a PIN length. The PIN block is created from the customer PIN and the hexadecimal F padding character. For example, for the 5-digit PIN 92389, the PIN block is:

9238 9FFF FFFF FFFF

5 FORMAT 04

Format 04 is the PIN block format adopted by the PLUS network. The format combines the customer PIN and the related account number as follows:

- A 16-digit block is made from the digit 0, the length of the PIN, the PIN, and a pad character (hexadecimal F). For example, for the 5-digit PIN 92389, the block is:

0592 389F FFFF FFFF

- Another 16-digit block is made from four zeros and the left-most 12 digits of the account number. For example, for the 16-digit account number 2283 4000 0012 3456, where the check digit is 6, the block is:

0000 2283 4000 0012

- The two blocks are exclusive-OR added:

	0592	389F	FFFF	FFFF
	0000	2283	4000	0012
PIN block:	0592	1A1C	BFFF	FFED

Note: Any transaction that requires a PIN block as a parameter accepts Format 04. The major impact of this format is on the account number field length: when a PIN block is formatted according to Format 04, the account number field becomes 18 digits in length.

For the PIN translation CA and CC commands, there are two format fields; if either is 04, the account number field must be 18 digits. If the account number is less than 18 digits, it must be right-justified and padded with X'F' on the left.

The following commands can use this format:

BC, BE, CA, CC, CG, DA, DC, EA, EC, EG, JC, JE. When reviewing the details for these commands, consider the change to the account field that this format requires.

6 FORMAT 05

Format 05 is the ISO 9564-1 Format 1 PIN Block represented by the following 16 hexadecimal values:

1NP 1..P N R .. R

Where

N is the PIN length (4 - C),
P 1..P N is the N-digit PIN,
R .. R is random padding.

The following validity checks are carried out on incoming Format 05 PIN blocks:

- The first character of the PIN block has value 1.
Error code 20 is returned if this check fails.
- The PIN digits (in positions 3 - (N+2)) are in the range 0 to 9.
Error code 20 is returned if this check fails.
- The second character (N) is in the hexadecimal range 4 - C.
Error code 24 is returned if this check fails.

7 FORMAT 34

Format 34 is the standard EMV PIN block format. It supports the PIN block format specified in EMV '96 Errata, dated January 31 1998. The PIN block is created from a fixed Control Field, the length of the PIN, the customer PIN itself and the hexadecimal F padding character. PINs from 4 to 12 digits in length are accommodated.

The 16-digit (8 byte) block is constructed as follows:

C	N	P	P	P	P	P/F	F	F							
---	---	---	---	---	---	-----	-----	-----	-----	-----	-----	-----	-----	---	---

Where:

- C is a fixed control field of binary value 0010 (H' 2).
- N is the length of the PIN and can be any binary value from 0100 to 1100 (H' 4 to H' C).
- P is a digit of the PIN and can be any binary value from 0000 to 1001 (H' 0 to H' 9).
- P/F is either a PIN digit or the binary 1111 (hex F) filler depending on the length of the PIN.
- F is filler of binary value 1111 (hex F).

Thus for a 5 digit PIN of 34567, the PIN block would hold the 16 hex values as shown below:

2	5	3	4	5	6	7	F	F	F	F	F	F	F	F	F
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

8 FORMAT 35

PIN Block format 35 is the PIN Block required by Europay/MasterCard for their Pay Now & Pay Later products.

The PIN block is created from a fixed Control Field, the length of the PIN, the customer PIN itself and the hexadecimal F padding character. PINs from 4 to 12 digits in length are accommodated.

The 16-digit (8 byte) block is constructed as follows:

C	N	P	P	P	P	P/F	F	F							
---	---	---	---	---	---	-----	-----	-----	-----	-----	-----	-----	-----	---	---

Where:

C is a fixed control field of binary value 0010 (hex 2).

N is the length of the PIN and can be any binary value from 0100 to 1100 (hex 4 to hex C).

P is a digit of the PIN and can be any binary value from 0000 to 1001 (hex 0 to hex 9).

P/F is either a PIN digit or the binary 1111 (hex F) filler depending on the length of the PIN.

F is filler of binary value 1111 (hex F).

Thus for a 5 digit PIN of 34567, the block would hold the 16 hex values as shown below:

2	5	3	4	5	6	7	F	F	F	F	F	F	F	F	F
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Another 16-digit block is made from four zeros and the 12 right-most digits of the account number, excluding the check digit.

For account number 1234 0000 0123 4562 where 2 is the check digit, the block is:

0	0	0	0	4	0	0	0	0	0	1	2	3	4	5	6
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

The two blocks are exclusive-ORed on a bit by bit basis:

2	5	3	4	5	6	7	F	F	F	F	F	F	F	F	F
0	0	0	0	4	0	0	0	0	0	1	2	3	4	5	6

2	5	3	4	1	6	7	F	F	F	E	D	C	B	A	9
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

9 FORMAT 41

PIN Block Format 41 is the Visa format for PIN change without using the current PIN. The method for constructing the PIN block is defined in section C.11.2 of reference 4.

The PIN Block is created using the new PIN and part of the card's unique DEA Key as follows:

1. Construct a 16 hexadecimal digit block of data, by extracting the eight rightmost digits of the card application's Unique DEA Key A (UDK-A)¹ and zero filling it on the left with eight hexadecimal zeros:

0	0	0	0	0	0	0	0									
←8 Rightmost digits of card app's unique DEA key A→																

2. Create a second 16 hexadecimal digit block of data as follows:

C	N	P	P	P	P	P/F	F	F								
---	---	---	---	---	---	-----	-----	-----	-----	-----	-----	-----	-----	-----	---	---

Where:

- C is a fixed control field of binary value 0000 (hex 0).
- N is the length of the new PIN and can be any binary value from 0100 to 1100 (hex 4 to hex C).
- P is a digit of the new PIN and can be any binary value from 0000 to 1001 (hex 0 to hex 9).
- P/F is either a PIN digit or the binary 1111 (hex F) filler depending on the length of the PIN.
- F is filler of binary value 1111 (hex F).

3. Perform an exclusive-OR operation on the blocks of data created in steps 1 and 2.

¹ HSM terminology for UDK-A is *DK-AC. This is the card-unique key derived from *MK-AC, the Master Key for Application Cryptograms.

10 FORMAT 42

PIN Block Format 42 is the Visa format for PIN change using current (old) PIN. The method for constructing the PIN block is defined in section C.11.1 of reference 4.

The PIN Block is created using the old PIN, the new PIN and part of the card's unique DEA Key as follows:

1. Construct a 16 hexadecimal digit block of data, by extracting the eight rightmost digits of the card application's Unique DEA Key A (UDK-A)² and zero filling it on the left with eight hexadecimal zeros:

0	0	0	0	0	0	0	0								
←8 Rightmost digits of card app's unique DEA key A→															

2. Create a second 16 hexadecimal digit block of data as follows:

C	N	P	P	P	P	P/F	F	F							
---	---	---	---	---	---	-----	-----	-----	-----	-----	-----	-----	-----	---	---

Where:

- C is a fixed control field of binary value 0000 (hex 0).
- N is the length of the new PIN and can be any binary value from 0100 to 1100 (H' 4 to H' C).
- P is a digit of the new PIN and can be any binary value from 0000 to 1001 (H' 0 to H' 9).
- P/F is either a PIN digit or the binary 1111 (hex F) filler depending on the length of the PIN.
- F is filler of binary value 1111 (hex F).

3. Create a third 16 decimal digit block of data using the old PIN as follows:

P	P	P	P	P	P/0	0	0	0							
---	---	---	---	---	-----	-----	-----	-----	-----	-----	-----	-----	---	---	---

Where:

- P is a digit of the old PIN and can be any binary value from 0000 to 1001 (H' 0 to H' 9).
- P/0 is either a PIN digit or the binary 0000 (hex 0) filler depending on the length of the PIN.
- 0 is filler of binary value 0000 (hex 0).

4. Perform an exclusive-OR operation on the blocks of data created in steps 1,2 and 3. The result is called the "Delta PIN".

² HSM terminology for UDK-A is *DK-AC. This is the card-unique key derived from *MK-AC, the Master Key for Application Cryptograms.

CHAPTER 4

ERROR CODES

1 GENERAL

4-1

1 GENERAL

The standard error codes returned by the HSM to the Host are listed in the table. Details of which error codes are applicable to each command are documented in Chapter 2.

Code	Description
00	No errors.
01	Verification failure / Warning Imported key parity error
02	Key inappropriate length for algorithm
04	Invalid key type code.
05	Invalid key length flag.
10	Source key parity error.
11	Destination key parity error / Key all 0
12	Contents of user storage not available. Reset, power-down or overwrite.
13	Master Key parity error.
14	PIN encrypted under LMK pair 02-03 is invalid.
15	Invalid input data (invalid format, invalid characters, or not enough data provided).
16	Console or printer not ready or not connected.
17	HSM not in the Authorized state, or not enabled for clear PIN output, or both.
18	Document format definition not loaded.
19	Specified Diebold Table is invalid.
20	PIN block does not contain valid values.
21	Invalid index value, or index/block count would cause an overflow condition.
22	Invalid account number.
23	Invalid PIN block format code.
24	PIN is fewer than 4 or more than 12 digits in length.
25	Decimalization table error.
26	Invalid key scheme
27	Incompatible key length
28	Invalid key type
29	Key function not permitted
30	Invalid reference number.
31	Insufficient solicitation entries for batch.
33	LMK key change storage is corrupted.
40	Invalid firmware checksum.
41	Internal hardware/software error: bad RAM, invalid error codes, etc.
42	DES failure.
80	Data length error. The amount of MAC data (or other data) is greater than or less than the expected amount.
90	Data parity error in the request message received by the HSM.

Code	Description
91	Longitudinal Redundancy Check (LRC) character does not match the value computed over the input data (when the HSM has received a transparent async packet).
92	The Count value (for the Command/Data field) is not between limits, or is not correct (when the HSM has received a transparent async packet).