HOST SECURITY MODULE 8000

SECURITY OPERATIONS MANUAL

1270A350 Issue 8.4

HOST SECURITY MODULE 8000
SECURITY OPERATIONS MANUAL

List of Chapters

Table of Contents

Host Security Module 8000 Security Operations Manual

Revision Status

Revision	HSM Functional Revision	Changes	Release Date
1270A350-001	HSM 8000 v1.0	First Issue.	December 2002
1270A350-002	HSM 8000 v2.0	Updated to include new features of base software v2.0.	June 2004
1270A350-003	HSM 8000 v2.1	Updated to include new features of base software v2.1.	September 2005
1270A350-004	HSM 8000 v2.2	Updated to include new features of base software v2.2.	November 2005
1270A350-005	HSM 8000 v2.3	Updated to include new features of base software v2.3.	March 2006
1270A350-006	HSM 8000 v2.4	Updated to include new features of base software v2.4.	December 2006
1270A350-007	HSM 8000 v3.0	Updated to include new features of base software v3.0.	March 2008
1270A350-008	HSM 8000 v3.1a	Updated to include new features of base software v3.1.	March 2009
1270A350-008.1	HSM 8000 v3.1b	Updated to correct errors and omissions.	June 2009
1270A350-008.2	HSM 8000 v3.1c	Updated to correct errors and omissions.	March 2010
1270A350-008.3	HSM 8000 v3.1c	Updated EULA.	April 2010
1270A350-008.4	HSM 8000 v3.1d	Updated APAC contact information.	August 2010

This manual describes the functionality within the 3.1d base release of HSM 8000 software. For all other versions please refer to appropriate manual and associated HSM software specifications.

Contact Information

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 US)
+1 954-888-6200 (outside US)
Fax: +1 954-888-6211

Support

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

support@thalesesec.com

Asia Pacific

Unit 4101, 41/F
248 Queen's Road East
Wanchai
Hong Kong, PRC

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

Support

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

asia.support@thales-esecurity.com

http://www.thalesgroup.com/iss

End User License Agreement

("EULA")

Please read this Agreement carefully. Use of the Product constitutes your acceptance of the terms and conditions of this License.

This document is a legal agreement between **Thales e-Security Ltd**., ("THALES") and the company that has purchased a THALES product containing a computer program ("Customer"). If you do not agree to the terms of this Agreement, promptly return the product and all accompanying items (including cables, written materials, software disks, etc.) at your mailing or delivery expense to the company from whom you purchased it or to *Thales e-Security, Ltd,* Meadow View House, Crendon Industrial Estate, Long Crendon, Aylesbury, Bucks HP18 9EQ, United Kingdom and you will receive a refund.

1. **OWNERSHIP.** Computer programs, ("Software") provided by THALES are provided either separately or as a bundled part of a computer hardware product. Software shall also be deemed to include computer programs which are intended to be run solely on or within a hardware machine, ("Firmware").Software, including any documentation files accompanying the Software, ("Documentation") distributed pursuant to this license consists of components that are owned or licensed by THALES or its corporate affiliates. Other components of the Software consist of free software components ("Free Software Components") that are identified in the text files that are provided with the Software. ONLY THOSE TERMS AND CONDITIONS SPECIFIED FOR, OR APPLICABLE TO, EACH SPECIFIC FREE SOFTWARE COMPONENT SHALL BE APPLICABLE TO SUCH FREE SOFTWARE COMPONENT. Each Free Software Component is the copyright of its respective copyright owner. The Software is licensed to Customer and not sold. Customer has no ownership rights in the Software. Rather, Customer has a license to use the Software. The Software is 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 or Documentation, and to reproduce any such copyright or trademark notice on all copies of the Software 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.

2. **LICENSE GRANT.** THALES grants Customer a non-exclusive license to use the Software with THALES provided computer equipment hardware solely for Customer's internal business use only. This license only applies to the version of Software shipped at the time of purchase. Any future upgrades are only authorised pursuant to a separate maintenance agreement. Customer may copy the Documentation for internal use. Customer may not decompile, disassemble, reverse engineer, copy, or modify the THALES owned or licensed components of the Software unless such copies are made in machine readable form for backup purposes. In addition, Customer may not create derivative works based on the Software except as may be necessary to permit integration with other technology and Customer shall not permit any other person to do any of the same. Any rights not expressly granted by THALES to Customer are reserved by THALES and its licensors and all implied licenses are disclaimed. Any other use of the Software by any other entity is strictly forbidden and is a violation of this EULA. The Software and any accompanying written materials are protected by international copyright and patent laws and international trade provisions.

3. **NO WARRANTY.** EXCEPT AS MAY BE PROVIDED IN ANY SEPARATE WRITTEN AGREEMENT BETWEEN CUSTOMER AND THALES, THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, THALES DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THALES DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS CUSTOMER MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW FOR THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

4. **LIMITATION OF LIABILITY.** IN NO EVENT WILL THALES BE LIABLE TO CUSTOMER OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF THALES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THALES' AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE. HOWEVER NOTHING IN THESE TERMS AND CONDITIONS SHALL HOWEVER LIMIT OR EXCLUDE THALES' LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM NEGLIGENCE, FRAUD OR FRAUDULENT MISREPRESENTATION OR FOR ANY OTHER LIABILITY WHICH MAY NOT BE EXCLUDED BY LAW. BECAUSE SOME COUNTRIES AND STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY.

5. **EXPORT RESTRICTIONS.** THE SOFTWARE IS SUBJECT TO THE EXPORT CONTROL LAWS OF THE UNITED KINGDOM, THE UNITED STATES AND OTHER COUNTRIES. THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ALL APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME.

CUSTOMER SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS.

6. **TERM & TERMINATION.** This EULA is effective until terminated. Customer may terminate this EULA at any time by destroying or erasing all copies of the Software and accompanying written materials in Customer's possession or control. This license will terminate automatically, without notice from THALES if Customer fails to comply with the terms and conditions of this EULA. Upon such termination, Customer shall destroy or erase all copies of the Software (together with all modifications, upgrades and merged portions in any form) and any accompanying written materials in Customer's possession or control.

7. **SPECIAL PROCEDURE FOR U.S. GOVERNMENT.** If the Software and Documentation is acquired by the U.S. Government or on its behalf, the Software is furnished with "RESTRICTED RIGHTS," as defined in Federal Acquisition Regulation ("FAR") 52.227-19(c)(2), and DFAR 252.227-7013 to 7019, as applicable. Use, duplication or disclosure of the Software and Documentation by the U.S. Government and parties acting on its behalf is governed by and subject to the restrictions set forth in FAR 52.227-19(c)(1) and (2) or DFAR 252.227-7013 to 7019, as applicable.

8. **TRANSFER RIGHTS**

   Customer may transfer the Software, and this license to another party if the other party agrees to accept the terms and conditions of this Agreement. If Customer transfers the Software, it must at the same time either transfer all copies whether in printed or machine-readable form, together with the computer hardware machine on which Software was intended to operate to the same party or destroy any copies not transferred; this includes all derivative works of the Software. FOR THE AVOIDANCE OF DOUBT, IF CUSTOMER TRANSFERS POSSESSION OF ANY COPY OF THE SOFTWARE TO ANOTHER PARTY, EXCEPT AS PROVIDED IN THIS SECTION 8, CUSTOMER'S LICENSE IS AUTOMATICALLY TERMINATED.

9. **GOVERNING LAW AND VENUE** This License Agreement shall be construed, interpreted and governed by the laws of England and Wales without regard to conflicts of laws and provisions thereof or in the event that the Software was delivered in the United States, Latin America or Canada, the laws of the State of Florida. The exclusive forum for any disputes arising out of or relating to this EULA shall be an appropriate court sitting in England, United Kingdom or in the event that the Software was delivered in the United States, Latin America or Canada, the courts of Florida, United States.

.

Chapter 1 - Introduction

General

The HSM 8000 (Host Security Module) series of equipment provides cryptographic functions to support network and point-to-point data security, therefore it is imperative that the HSM itself is secure. The HSM is made physically secure by locks, electronic switches and tamper-detection circuits, and must be located in a secure area with controlled access. See Appendix A - Security Recommendations.

HSM software security is provided by a combination of several security features including:

- Two front-panel locks with separate keys.
- Personalised Smartcards issued to several Security Officers.
- Personal Identification Numbers (PINs) issued to Security Officers.
- A Secure mode which requires the presence of two officers holding separate physical keys to the front panel locks.
- An Authorised mode, requiring the presence of two Authorising Officers with encrypted Smartcards and (optionally) PINs.
- A configurable alarm system.
- Configurable security parameters.
- Error and Audit logs.

Security commands, and operations involving plain text data, are entered by the user via the associated HSM Console, or via the HSM Manager.

About this Manual

This manual contains instructions for the security operations which must be performed on the HSM console. For other HSM information, see the following manuals:

- HSM 8000 Console Reference Manual
- HSM 8000 Installation Manual
- HSM 8000 Image Loader User Manual
- HSM 8000 Host Programmers Manual
- HSM 8000 Host Command Reference Manual
- HSM 8000 Local HSM Manager User's Guide
- HSM 8000 Remote HSM Manager User's Guide

Chapter 2 - Configuration

General

This chapter describes the security and alarm configuration of the HSM.

Entry of commands and data at the Console is not case sensitive (i.e., A has the same effect as a). Additional spaces can be inserted between characters to ease legibility during entry; they are ignored by the HSM. However they cannot be used between command characters (e.g. the LK command cannot be successfully entered as L K).

When entering sensitive (clear text) data, use the Inhibit Echo Back facility to ensure that the HSM does not echo the data to the Console screen. This is set at configuration using the "Echo" parameter in the CS (Configure Security) command. Instead of displaying the data, the HSM displays a star for each character entered. Thus:

```
0123456789ABCDEF
```

is shown on the screen as:

```
****************
```

To exit from a command during data entry, press <Control> and C simultaneously. The HSM responds with:

```
TERMINATED
```

Configure the Alarms

The HSM alarm circuitry should be turned on when the HSM is put into service. The alarms typically need to be turned off if the HSM is to be moved.

The HSM must be in the secure state to configure the alarms.

Enter CL <Return> to initiate the following example in which both the temperature alarm and the motion alarm are turned on. User input is shown underlined. The option to save the alarm settings to Smartcard is selected.

Example:

```
Secure> CL <Return>
LMKs must be erased before proceeding.
Erase LMKs? [Y/N]: Y <Return>
Temperature Alarm [oN/ofF]: F <Return>
Motion Alarm [oN/ofF]: F <Return>
Save ALARM settings to smart card? [Y/N]: Y <Return>
Insert card and press ENTER: <Return>
ALARM settings saved to the smart card.
Secure>
```

Configure Security

The security configuration of the HSM and some processing parameters are set by the CS (Configure Security) console command. The settings can be examined by the QS (Query Security) console command. The HSM must be offline. See the HSM 8000 Console Reference Manual for details of these commands.

The parameters that can be set are:

Parameter	Default value
PIN length: 4..12 *This is the length of the PIN to be stored as an encrypted PIN under the LMK.* *Note: The "encrypted PIN" is one character longer than the length specified for the PIN by this parameter.*	4
Echo: On or Off *If the answer to this question is 'On' then passwords and other secret values are displayed on the console as entered. Characters can be hidden by using '^' prior to entering the component or key.* *Note: Enabling Echo is a security hazard and should not be used in a live system.*	Off
Atalla ZMK variant support: On or Off *For interoperation with Atalla systems. This enables the optional Atalla variants within commands. Any console command providing key support will prompt for an Atalla variant.* *Note: Selection has no effect on host commands - Atalla variants can be supplied with any appropriate command regardless of this setting.*	Off
Transaction key scheme: Racal, Australian or None *Transaction key schemes are techniques whereby data-encrypting keys change with each transaction in a manner that cannot be followed by a third party. The HSM supports three variants of transaction key schemes: Racal, Australian (AS2805) and DUKPT. There are command conflicts between the Racal and Australian scheme so only one can be selected. The use of the DUKPT commands is not affected by this setting.* *Note: The default value has changed to 'None'. In this case, none of the Racal or Australian transaction key scheme commands are available to the host.*	None
User storage key length: Single, Double or Triple *This is the length of the keys stored in user storage; it can be single, double or triple length. The number of keys that can be stored depends upon this setting.*	Single
Select clear PINs: Yes or No *This enables the clear PIN support via host commands 'NG' and 'BA'. Authorised state is a requirement for these commands to be processed by a host application.* *Note: This is a security risk unless precautions are taken at the host.*	No
Enable ZMK translate command: Yes or No *This enables the 'BY' command that allows the translation of Zone Master Keys from under another Zone Master Key. Authorised state is required for this command to process within a host application.* *Note: The availability of this command is a significant security risk.*	No

Parameter	Default value
Enable X9.17 for import: Yes or No *This enables support for the ANSI X9.17 mechanism for key import. When being imported, each key of double or triple length is encrypted separately using the Electronic Code Book (ECB) mode of encryption. This is a lower security option. It is strongly recommended that the X9 TR-31 keyblock is used instead of X9.17.*	No
Enable X9.17 for export: Yes or No *Similar to the previous item, but used when exporting keys.*	No
Solicitation batch size: 1..1024 *A method supported by the HSM to enable customers to self-select their own PINs is to use Solicitation mailers. This is a turnaround form that is sent to the cardholder. The cardholder records the PIN selection on the form and returns it to the issuer. The mailer data consists of the cardholder name and address and a reference number (an encrypted account number). As a security measure, the form returned to the issuer contains only the reference number and the PIN selection. A batch process is used to process these requests when returned.*	1024
Enable single-DES: Yes or No *This parameter is only valid if ZMK length is double. If enabled, it permits the use of single-length DES keys.* *Note: The default value has been changed to 'No'.*	No
Prevent Single-DES keys masquerading as double or triple-length key: Yes or No *When set to Yes, all HSM commands that import double or triple-length DES keys will ensure that the imported key is not simply a single-length key masquerading as a double or triple-length key.*	Yes
ZMK length: Single or Double *The length of the Zone Master Key: single or double. This is a backwards-compatible mode to enable the switching between 16H and 32H for ZMKs.* *Note: The default value of this parameter has been changed to 'Double'.*	Double
Decimalisation table Encrypted/Plaintext: Encrypted or Plaintext *This option determines if the decimalisation table will be encrypted or in plain text. The default setting is encrypted, however, to allow for backward compatibility plaintext decimalisation tables can be selected. It is recommended that encrypted decimalisation tables are used to protect against decimalisation table manipulation attacks.*	Encrypted
Enable decimalisation table checks: Yes or No *The values in the decimalisation tables, used for deriving and verifying PIN offset values, are normally restricted to provide additional security by rejecting values which are potentially insecure. This can cause problems where existing tables fail the checks, so for backward compatibility this parameter allows the restrictions to be disabled.*	Yes

Parameter	Default value
PIN encryption algorithm: A (Visa method) or B (Racal method) *This selects the PIN encryption algorithm to be used when encrypted PINs are stored by the card issuer. The Racal algorithm is the best choice for a new installation; it is the stronger of the two methods. The Visa algorithm is offered for compatibility with older HSMs and for customers who already have a database of encrypted PINs.* *When the Racal method is used, the output of the encryption is hex characters whereas the Visa method produces numeric digits. Commands that use encrypted PINs describe them as 'LN or LH'.*	A (Visa method)
Card/password authorisation: Card or Password *This option selects the method of authenticating security officers requesting a security state change. The Authorised State is a mode that the HSM can be placed in for sensitive data processing. This authorised mode is required when input commands at the console or host use clear text data such as key components or unencrypted pins. Authorised mode can be used in both Online and Offline host states and requires the authorising officers to invoke the higher security level. Before the authorised state can be set the authorising officers need to be verified by the HSM. Officer verification is done by checking either a smartcard and PIN or a password (16 alphanumeric characters.) If the Password option is not set when the LMK is created, the password option will not be available as no password is created and stored with the LMK components.*	Card
Card issuer password: 8 characters *This option enables Thales to change the card issuer password for LMK and authorising officer Smartcards. If the password has been changed you will be advised when new cards are delivered. Special care must be taken that no key is inadvertently struck, placing a character in this field. If this setting is changed, it will not be possible to format the Smartcards using the 'FC' command.*	
Authorised state required when importing DES key under RSA Key: Yes or No *This setting determines whether Authorised State is mandatory for the import of DES keys using RSA keys (host command GI). When set to Yes, the GI command always requires Authorised State (and the use of the signature field is optional). When set to 'No', the GI command does not require Authorised State.*	Yes
Minimum HMAC verification length in bytes: Yes or No *This setting determines the minimum and maximum lengths of HMAC keys that the HSM can generate. HMAC keys must satisfy the equation L/2 <= key length, where L = is the size of the hash function output. For SHA-1 HMAC keys, L=20, and therefore the key length must be at least 10.*	10
Enable PKCS#11 import and export for HMAC keys: Yes or No *This setting determines whether the host commands LU and LW can import or export HMAC keys in PKCS#11 format.*	No
Enable ANSI X9.17 import and export for HMAC keys: Yes or No This setting determines whether the host commands LU and LW can import or export HMAC keys in ANSI X9.17 format.	No

Parameter	Default value
Enable ZEK encryption of all printable ASCII chars[1]: Yes or No *This setting determines whether the 'Message Encryption' host commands M0, M2 and M4 can encrypt/decrypt/translate messages (using a ZEK) where the plaintext contains only printable ASCII characters.*	No
Enable ZEK encryption of "Base94" ASCII chars: Yes or No *This setting determines whether the 'Message Encryption' host commands M0, M2 and M4 can encrypt/decrypt/translate messages (using a ZEK) where the plaintext contains only Base94 characters.*	No
Enable ZEK encryption of "Base64" ASCII chars: Yes or No *This setting determines whether the 'Message Encryption' host commands M0, M2 and M4 can encrypt/decrypt/translate messages (using a ZEK) where the plaintext contains only Base64 characters.*	No
Enable ZEK encryption of "Hex-only" ASCII chars: Yes or No *This setting determines whether the 'Message Encryption' host commands M0, M2 and M4 can encrypt/decrypt/translate messages (using a ZEK) where the plaintext contains only hexadecimal ASCII characters.*	No
Restrict Key Check Value to 6 hex chars: Yes or No *This setting determines whether Key Check Values (KCVs) should be restricted to consist of only 6 hex characters. The overall length of the KCV field will remain the same, regardless of this setting. However, when set to 'Yes', only the first 6 characters will contain the KCV: any remaining characters will be ignored (when input to the HSM) or set to '0' (when returned from the HSM).*	Yes
Enable Multiple Authorised Activities: Yes or No *If enabled, will allow precise selection of authorised activities (including timeout period if required). If disabled HSM reverts to global Authorised state.*	Yes
Enable Persistent Authorised Activities: Yes or No *If enabled, will allow "persistent" authorised activities to be automatically restored when the HSM restarts following a power failure.*	Yes
Enable variable length PIN offset: Yes or No *If enabled, this will allow the IBM 3624 PIN Offset commands to return an Offset whose length matches the PIN, rather than being restricted to the Check Length parameter.*	No
Enable weak PIN checking: Yes or No *If enabled, the HSM's PIN generation/derivation host commands will check to ensure that the PIN does not match one of the entries in the appropriate global 'Excluded PIN Table'. If a match is found in the list, then the command fails, returning error code 86.*	No
Enable PIN Block format 34 as output format for PIN translations to ZPK: Yes or No *If enabled, the HSM will permit PIN block format 34 to be used as the output format of PIN translation commands. In previous versions of HSM software, translations to this format were not possible.*	No

[1] Refer to Appendix H for details of ASCII reduced character sets.

Parameter	Default value
Default LMK identifier: 00..99 *Identifies the Default LMK, which the HSM will use if it receives a command that does not explicitly state which LMK is to be used. The use of the Default LMK provides a "backward-compatible" mode, even when multiple LMKs are loaded in the HSM.*	00
Management LMK identifier: 00..99 *Identifies the Management LMK, which will be used for authorising certain management functions (e.g. setting the HSM's date/time), and for encrypting the audit MAC key.*	00
Use HSM clock for date/time validation: Yes or No *If enabled, the HSM uses its integral real-time clock to validate check the start/end date/time optional header blocks of keyblocks (when present).*	Yes
Additional padding to disguise key length: Yes or No *If enabled, the HSM disguises the length of single or double length keys within a keyblock by adding 8 or 16 extra padding bytes, such that single, double and triple length DES keys all appear to be triple length keys.*	No
Key export and import in trusted format only: Yes or No *If enabled, the HSM will only import/export keys using a keyblock format. In this case, any export/import process using keys in variant format (including X9.17 format) will be prohibited.*	Yes
Secure Link password: 8 characters *This setting allows the user to configure the password which is to be used to protect the HSM Manager – HSM communications. The HSM Manager will be made available at some future date.*	password

Example

```
Secure> CS <Return>
PIN length [4-12]: 4 <Return>
Echo [oN/ofF]: F <Return>
Atalla ZMK variant support [oN/ofF]: F <Return>
Transaction key scheme Racal or Australian or None? [R/A/N]: R <Return>
User storage key length [S/D/T]: T <Return>

LMKs must be erased before remaining parameters can be set.

Erase LMKs? [Y/N]: Y <Return>

Select clear PINs? [Y/N]: N <Return>
Enable ZMK translate command? [Y/N]: N <Return>
Enable X9.17 for import? [Y/N]: N <Return>
Enable X9.17 for export? [Y/N]: N <Return>
Solicitation batch size [1-1024]: 1024 <Return>

Enable Single DES? [Y/N]: Y <Return>
Prevent single-DES keys masquerading as double or triple-length key? [Y/N]: Y Y
<Return>
Making default length for ZMKs: [S/D]: D <Return>
Decimalisation table Encrypted/Plaintext [E/P]: E <Return>
Enable Decimalisation Table Checks? [Y/N]: Y <Return>

PIN encryption algorithm [A/B]: A <Return>
Card/password authorisation (local) [C/P]: C <Return>
Card issuer password (local) [Enter = no change]: <Return>
Authorised state required when importing DES key under RSA key [Y/N]: Y <Return>
```

```
Minimum HMAC verification length in bytes? [5-64]: 10 <Return>
Enable PKCS#11 import and export for HMAC keys? [Y/N]: N <Return>
Enable ANSI X9.17 import and export for HMAC keys? [Y/N]: N <Return>
Enable ZEK encryption of all printable ASCII chars? [Y/N]: N <Return>
Enable ZEK encryption of "Base94" ASCII chars? [Y/N]: N <Return>
Enable ZEK encryption of "Base64" ASCII chars? [Y/N]: Y <Return>

Restrict Key Check Value to 6 hex chars? [Y/N]: Y <Return>
Enable multiple authorised activities? [Y/N]: Y <Return>
Enable persistent authorised activities? [Y/N]: Y <Return>
Enable variable length PIN offset? [Y/N]: N <Return>
Enable weak PIN checking? [Y/N]: N <Return>
Enable PIN Block format 34 as output format for PIN translations to ZPK? [Y/N]:
N <Return>

Default LMK identifier? [00-99]: 00 <Return>
Management LMK identifier? [00-99]: 00 <Return>
Use HSM clock for date/time validation? [Y/N]: N <Return>
Additional padding to disguise key length? [Y/N]: N <Return>
Key export and import in trusted format only? [Y/N]: Y <Return>
Secure Link password (local) [Enter = no change]: <Return>

Save SECURITY settings to smartcard? [Y/N]: Y <Return>
Insert card and press ENTER: <Return>
SECURITY settings saved to the smartcard.
Secure>
```

Chapter 3 - Local Master Keys

Types of LMKs

A **Variant LMK** is a set of 40 DES keys, arranged in pairs, with different pairs (and variants of those pairs) being used to encrypt different types of keys. This is the standard LMK format supported in all versions of Racal/Thales HSM firmware.

Note: The term "Variant LMK" refers to the 'variant' method of encrypting keys; a Variant LMK is not itself a variant of any other key.

A **Keyblock LMK** is a triple-length DES key, and is used to encrypt keys in a keyblock format. It is not compatible with a Variant LMK, and it can only be used to encrypt keys in keyblock form.

Note: The term "Keyblock LMK" refers to the 'keyblock' method of encrypting keys; a Keyblock LMK is not itself stored in keyblock form.

Multiple LMKs

With version 3.0 (and later) software, it is possible to install multiple LMKs within a single HSM 8000. The precise details of the number and type of installed LMKs are controlled via the HSM's licence file:

Licence	Description
HSM8-LIC001v3 (standard v3.0 licence)	Two concurrent LMKs can be installed; however, one must be a Variant LMK, and the other a Keyblock LMK.
HSM8-LIC012 LMK x 2 (optional licence)	Two concurrent LMKs can be installed; they can be any combination of Variant and Keyblock LMKs.
HSM8-LIC013 LMK x 5 (optional licence)	Five concurrent LMKs can be installed; they can be any combination of Variant and Keyblock LMKs.

LMK Table

LMKs are stored in a table within the secure memory of the HSM, with each LMK occupying a different 'slot' within the table. Each slot has the following attributes:

Attribute	Description
LMK ID	A 2-digit number which uniquely indicates the location of each LMK within the table. All references to LMKs are made by specifying the LMK Identifier.
Key Scheme	• "Variant" for traditional Racal/Thales LMK – key encryption performed using the *variant* method. • "Keyblock" for v3.0 and later software – key encryption performed using the *keyblock* method.
Algorithm	• "3DES (2key)" is used by Variant LMKs. • "3DES (3key)" is used by Keyblock LMKs. Other algorithm types may be supported in future software releases.
Status	• "Test" indicates that the LMK is used for testing purposes. • "Live" indicates that the LMK is used for live production purposes. When installing LMKs, the HSM will prevent any mixing of Test and Live LMKs within the same slot (i.e. LMK Value and Old LMK Value must have

	the same status).
Comments	User-entered text, which can be used to help identify LMKs.
Authorisation	Indicates the authorisation status of the HSM for this particular LMK – either a flag (for Authorised State) or a list of authorised activities.
LMK Check Value	The check value of the LMK.
Old LMK Check Value	The check value of the 'old' LMK (in Key Change Storage).

Use the console command VT (View LMK Tables) to view the contents of the HSM's LMK table.

Local Master Keys are normally generated in component form, and recorded on Smartcards. All of an LMK's components are loaded into the HSM to recreate that LMK when required.

Variant LMKs

A Variant LMK is a set of 40 DES keys, arranged in pairs, with different pairs (and variants of those pairs) being used to encrypt different types of keys. This is the standard LMK format supported in all versions of Racal/Thales HSM firmware.

Note: The term "Variant LMK" refers to the 'variant' method of encrypting keys; a Variant LMK is not itself a variant of any other key.

LMK Pair	Function
00 - 01	Contains the two Smartcard "keys" (Passwords if the HSM is configured for Password mode) required for setting the HSM into the Authorised 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 & Card Verification Keys.
16 - 17	Encrypts Terminal Authentication Keys.
18 - 19	Encrypts reference numbers for Solicitation Mailers, decimalisation Tables, and Issuer Proprietary Bitmaps.
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.

LMK Pair	Function
26 - 27	Encrypts Zone Authentication Keys.
28 - 29	Encrypts Terminal Derivation Keys, EMV Master Keys, and Contactless Master Keys.
30 - 31	Encrypts Zone Encryption Keys.
32 - 33	Encrypts Terminal Encryption Keys.
34 - 35	Encrypts RSA & HMAC Keys.
36 - 39	Reserved for future use.
There are Variants of some keys to suit particular requirements.	

Keyblock LMKs

A Keyblock LMK is a triple-length DES key, and is used to encrypt keys in a keyblock format. It is not compatible with a Variant LMK, and it can only be used to encrypt keys in keyblock form.
Note: The term "Keyblock LMK" refers to the 'keyblock' method of encrypting keys; a Keyblock LMK is not itself stored in keyblock form.

Support for Thales Key Blocks

The HSM 8000 now includes support for the Thales keyblock scheme, for the encryption and authentication of keys.

Key Block Format

The Thales keyblock is denoted by key scheme "S" and has the following format:

Tag ("S")	Header	Optional Header Blocks	Encrypted Key Data	Key Block Authenticator
(1 byte)	(16 ASCII characters)	(ASCII characters, variable length)	(variable length, ASCII encoded)	(8 ASCII characters)

The entire keyblock will be ASCII encoded.

Refer to 1270A351 for more details on Thales Keyblocks.

LMK Management

To generate and load an LMK, at least three "Component Holders" (two Authorising Officers and at least one other person) are required.

The first Authorising Officer creates a number of Secret Values (and a Password, if the HSM is configured in Password mode), and enters this data at the Console. The HSM uses these secret values to produce a Component Set. This set of values is then recorded on a Smartcard.

Using the same procedure, the second Authorising Officer creates another set of Secret Values (and if necessary, a Password), generates a Component Set and records it on a second Smartcard.

Each additional Component Holder creates another set of Secret Values, generates a Component Set and records it on an additional Smartcard.

The above procedures result in a number of Smartcards, each containing one Component Set. The first and second Smartcards also contain Authorising data. Each Component Holder makes copies of their Smartcard so that it is stored on a number of Smartcards. At least two copies should be made, one for storage onsite and one offsite. Serious consideration should be given to the creation of extra copies to provide a greater level of resilience against the failure of any one Smartcard. Copies made for resilience against failure can be kept together.

NOTE: AT NO TIME SHOULD ANY ONE PERSON HAVE GAINED ACCESS TO MORE THAN ONE COMPONENT SETS.

The data contained in the Smartcards is loaded to LMK storage. The load function stores Authorising data (Passwords, if this mode is used), and mathematically combines each Component Set with the previous contents of the LMK storage to form the remaining LMK pairs. The Smartcards must then be separately and securely stored (e.g., in safe deposit boxes).

When new LMKs are generated (for example, if existing keys are known to be compromised), it is usually necessary to use the old LMK so that existing encrypted data can be translated from encryption under the old keys to encryption under the new keys. To translate between LMKs, , first load the new LMK, then load the old LMK in to a special memory area known as "key change storage". After this process, use Host commands to translate the old encrypted data.

LMKs in the unit can be verified and the LMK Component Sets on the Smartcards can be checked. It is recommended that:

- LMKs in the HSM are verified at 6-month intervals.
- LMKs on Smartcards (including all the spare copies) are checked at 12-month intervals.
- LMKs are changed at 2 year intervals. This ensures that the procedures required for the change are regularly exercised and updated where necessary.

Generate an LMK Component Set

The following are required:

- The three (or more) Component Holders (two Authorising Officers plus at least one other Component Holder), who are to generate the three (or more) sets of components. (The two Authorising Officers must be present whenever the HSM is to be set into the Authorise Activity state.)
- The HSM Console.
- Access to a single HSM.
- At least 6 formatted blank Smartcards (up to 12 can be used). 6 cards provide two copies of three sets of components, 12 cards provide four copies of three sets. Note that new cards are supplied un-formatted. Use the FC command to format or re-format the cards.
- Labels for identifying the Smartcards.
- A log to record the LMK check values that are used to verify the contents of each Smartcard at a later date. If the HSM is configured in Password mode and the two Passwords are entered by the Authorising Officers (i.e., not automatically created by the HSM and stored electronically), the two Passwords must be also recorded in the log.
- The two keys for the cam locks.

The results of the process with three Component Holders and two copies of the Smartcards are three Smartcard sets as follows:

- Smartcard set 1, consisting of one original Smartcard plus one duplicate (contains Component Set 1 (and, if applicable, Password 1)).
- Smartcard set 2, consisting of one original Smartcard plus one duplicate (contains Component Set 2 (and, if applicable, Password 2)).
- Smartcard set 3, consisting of one original Smartcard plus one duplicate (contains Component Set 3).

The Secret Values must each be 16 random characters, and can contain any hexadecimal characters (0-9, A-F).

Note that during the process of creating an LMK component set a number of values (A, B and C) can be either entered manually or randomly generated by the HSM – which is the recommended approach; if the values are entered manually and written down for storage, it is possible to subsequently re-create the LMK components even if the Smartcards are not available. Therefore the recorded values must be MORE SECURELY STORED than the Smartcards.

Note: When generating Component Sets for a Variant LMK, values A and B contain 16-digit Secret Values, whilst value C contains an 8-digit value. However, when generating Component Sets for a Keyblock LMK, values A, B and C each contain 16-digit Secret Values.

Generating Component Set 1

In the description that follows, user entries at the Console are shown underlined. Characters returned by the HSM that depend on the values entered by the user (and therefore cannot be predicted) are shown as X.

It is assumed that the HSM has been set for Smartcard mode and Echo On at security configuration (CS command).

1. Set the HSM into the Secure state: insert the keys in both of the key switches on the HSM front panel and rotate them both fully. The Console displays:

```
HSM going OFFLINE, press Reset to go Online.
Master Key loading facilities now available.
Secure>
```

2. Initiate the LMK generation and storage procedure. Use the GK command. The HSM responds with a series of prompts to ensure that the initial starting conditions are achieved.

```
Secure> GK <Return>
```

The HSM responds with:

```
Variant scheme or key block scheme? [V/K]: V or K <Return>
Key status? [L/T]: L <Return>
```

3. The HSM prompts for the number to identify this component set:

```
LMK component set [1-9]: 1 <Return>
```

4. The HSM prompts for the first (16-character hexadecimal) secret value:

```
Enter secret value A: aaaaaaaaaaaaaaaa <Return>
```

If Echo off has been configured, the characters are replaced by stars *
If only <Return> is entered, the HSM generates a random number for use as the secret value. This is the recommended way of generating the value.
Note: The random number created by the HSM is not displayed.

5. The HSM prompts for the second (16 character hexadecimal) secret value:

```
Enter secret value B: aaaaaaaaaaaaaaaa <Return>
```

As in Step 4, just <Return> can be entered, and the HSM will generate a random value. This is the recommended way of generating the value.

6. The HSM prompts for the third value. When generating a Variant LMK, the third value consists of 8-hex characters; when generating a Keyblock LMK, the third value, C, is a secret value consisting of 16-hex characters. For example:

Variant LMK	**Keyblock LMK**
`Enter value C: 18022008 <Return>`	`Enter secret value C: aaaaaaaaaaaaaaaa <Return>`

As in Step 4, just <Return> can be entered, and the HSM will generate a random value. This is the recommended way of generating the value.

7. The HSM is now ready to copy the LMKs onto Smartcards. It prompts:

```
Insert blank card and enter PIN:  ***** <Return>
```

Insert the Smartcard in the reader and enter its PIN. PIN entry should not be overlooked.

If there is a fault on the card or it already has data on it, either allow the HSM to write over the old data or reject the card and use another, as applicable, in reply to prompts from the HSM.

8. The HSM displays:

```
Writing keys
Checking keys
Device write complete, check: XXXXXX
```

Remove the Smartcard and store it securely. If a failure has occurred, the Smartcard is ejected: return to Step 7.

Make a note of the check value for future reference. (It is subsequently used to ensure that the contents of the Smartcard are correct, and should be recorded so that the correct use of LMKs can be reliably audited later.)

The HSM prompts:

```
Make another copy? [Y/N]: Y <Return>
```

9. Make another copy: repeat Steps 8 and 9 until the required number of copies have been made, then terminate the command in response to the prompt:

```
Make another copy? [Y/N]: N <Return>
X copies made
```

Generating Component Set 2

The procedure of generating Component Set 2 is almost the same as the procedure for generating Component Set 1. Different secret values should be used; and if the secret values are entered at the console, their entry must not be observed.

1. In Step (3), enter 2 (for Component Set 2) instead of 1.

Generating Additional Components - Set 3, etc.

The procedure for generating Component Set 3 (and 4 to 9, as required) is almost the same as the procedure for generating Component Set 1. Again, different secret values should be used; and if the secret values are entered at the console, their entry must not be observed.

1. In Step (3) enter 3 (or 4, etc.) instead of 1.
2. When all component sets have been generated, to return the HSM to normal use, load the LMKs and lock the cam locks on the front panel, and remove the keys.

Password Mode

The HSM may be configured for password Mode authorisation using the CS (Configure Security) console command.

This mode is provided for backward compatibility.

The process is similar to generating component set 1 & 2, except there is an extra step before (5) where the HSM prompts twice for the (16- character alphanumeric) Password.

Loading the LMKs

The HSM's Local Master Key(s) must have been loaded before an HSM can be put into service. Also, because LMKs are erased whenever the HSM is in an alarmed condition or when any security configuration changes are to be made, the LMKs are likely to need to be reloaded at some point. The procedure for loading from Smartcards is described below.

The following are required:

- One Smartcard from each of the Component Sets.
- The Component Holders responsible for Smartcard custody (no one person should have access to all Smartcards).

In the description that follows, user entries at the Console are shown underlined. Characters returned by the HSM that depend on the values entered by the user (and therefore cannot be predicted) are shown as X.

The order in which the Smartcards are loaded into the HSM is not important, but, for convenience, they are referred to as the first, second and third (etc.) Smartcards.

1. Set the HSM into the Secure state: insert the keys in both of the key switches on the HSM front panel and rotate them both fully. The Console displays:

   ```
   HSM going OFFLINE, press Reset to go Online.
   Master Key loading facilities now available.
   Secure>
   ```

2. Initiate the LMK loading. Use the LK command. The HSM responds with a series of prompts to ensure that the initial starting conditions are achieved.

   ```
   Secure> LK <Return>
   ```

   The HSM responds with:

   ```
   Enter LMK id: 00 <Return>
   Enter comments: Live LMK for ABC Bank <Return>
   LMK in selected location must be erased before proceeding
   Erase LMK? Y <Return>
   ```

3. The HSM prompts for the components:

   ```
   Load LMK from components.
   Insert card and enter PIN: <Return>
   ```

   Insert the first Smartcard into the card reader on the front of the panel of the HSM.

4. When the Smartcard is inserted enter the PIN:

   ```
   ***** <Return>
   ```

5. The HSM reads the Smartcard then displays:

   ```
   CHECK: XXXXXX
   Load more components? [Y/N]: Y <Return>
   ```

   If it displays an error message, rectify the fault and repeat the operation as necessary. When successful, remove the Smartcard.

6. Insert the next Smartcard and repeat the loading procedure, Steps 3 to 5.

7. Repeat Step 6 for the third (and any subsequent) set of components. When all have been loaded and the HSM displays the check value, RECORD THE CHECK VALUE (it is the check on the final LMK pairs and is subsequently used to verify that the LMK pairs are correct), then press N to terminate the loading procedure:

   ```
   CHECK: XXXXXX
   Load more components? [Y/N]: N <Return>
   Use the LO command to load LMKs into key change storage
   ```

8. It is now possible to go to step 3 of the procedure for Moving 'Old' LMKs Into Key Change Storage, if required. Otherwise lock the cam locks on the front panel and remove the keys.

9. Ensure that the HSM can be set into the Authorised state by inserting the Smartcards or entering the Passwords (as applicable). Use the A command, and insert the Smartcards and enter the PINs (or enter the Passwords), in response to prompts. If used, the Passwords must be entered in the correct order (i.e., the first should be the Password loaded with Component Set 1).

   ```
   Online> A <Return>
   ```

   Enter the first PIN (or the Password), as applicable:

   ```
   First Officer:
   Insert card and enter PIN: ***** <Return>
   ```

   or

   ```
   Password: ********** <Return>
   ```

   Enter the second PIN (or the Password), as applicable:

```
Second Officer:
Insert card and enter PIN: ***** <Return>
```

or

```
Password: ********** <Return>
```

When successful the HSM displays:

```
AUTHORISED
Online-AUTH>
```

If one of the PINs (or Passwords) does not have the correct number of characters (excluding spaces), the HSM re-prompts, and, if one was incorrect it returns NOT AUTHORISED. In either case, press <Delete> and re-enter the PINs (or Passwords).

10. To reset the HSM and set it online to the Host, press the RESET button on the front panel. This also removes the HSM from the Authorise Activity state.
11. Check that the yellow Secure LED on the front panel is illuminated.

Moving 'Old' LMKs Into Key Change Storage

When new LMKs have been loaded into the HSM, using the LK command, the HSM prompts whether a set of old LMKs needs to be loaded into Key Change Storage for use in translations from old to new keys. If so, proceed as follows:

1. Ensure that the HSM is in the Secure state (see Step 1 of procedure "Loading the LMKs").
2. Ensure that the HSM is in authorise activity state (see Step 9 of procedure "Loading the LMKs").
3. Initiate moving 'Old' keys into key change storage. Use the LO command:

   ```
   Secure-AUTH> LO <Return>
   Load Old LMK from components.
   Insert card and enter PIN:
   ```

4. Insert the first (old) Smartcard.
5. When the Smartcard is inserted enter the PIN:

   ```
   ***** <Return>
   ```

6. The HSM reads the Smartcard then displays:

   ```
   CHECK: XXXXXX
   Load more components? [Y/N]: Y <Return>
   ```

   If it displays an error message, rectify the fault and repeat the operation as necessary.

   When successful, remove the Smartcard.

7. Insert the next Smartcard and repeat steps 5 and 6.
8. Repeat Step 7 as necessary until all old component sets have been combined in the key change storage area. When all components have been loaded and the HSM displays the correct check value, press N to terminate the procedure:

   ```
   CHECK: XXXXXX
   Load more components? [Y/N]: N <Return>
   ```

9. Return the HSM to normal use by locking the cam locks on the front panel and removing the keys.

Translating Encrypted Data

When the HSM is ready to translate data from encryption under the old LMKs to encryption under the new LMKs (i.e., it has the new keys loaded and the old keys in key change storage), it requires the Host to send the correct sequence of commands for each encrypted set of data that needs translating (see the HSM 8000 Host Programmers Manual).

On completion, ensure that all the HSMs fitted with the old LMKs are updated and that all the units are secure with the yellow Secure LED illuminated.

Verifying the Contents of the LMK Store

The LMKs installed in the HSM should be checked periodically. Using the V command, confirm that the check value is identical to the value that was recorded when the LMK set was installed.

```
Online> V <Return>
```

The HSM responds with a prompt to enter the LMK's 2-digit identifier:

```
Enter LMK id: 00 <Return>
```

The HSM then responds with:

```
Check: XXXXXX
```

Confirm that the check value is the same as the one logged when the LMKs were first loaded.

If the contents of LMK storage in the HSM have been corrupted, the HSM responds with:

```
MASTER KEY PARITY ERROR
```

(LMK storage can also be verified by host command NC.)

The original and duplicate LMK Smartcards should be checked periodically.

Duplicating LMK Component Sets

The LMK component set on a Smartcard can be copied onto another Smartcard using the DC command.

1. The HSM must be in the Secure state (see "Generating Component Set 1", Step 1).
2. Initiate the copying procedure:

   ```
   Secure> DC <Return>

   LMKs must be erased before proceeding Erase LMKs [Y/N]: Y
   <Return>
   ```

3. The HSM prompts:

   ```
   Insert card to be duplicated and enter PIN: ***** <Return>
   ```

   Insert the original card, enter its PIN. Confirm the check value and remove the card.

4. The HSM prompts:

   ```
   Insert blank card and enter PIN: ***** <Return>
   ```

   Insert a new formatted card and enter its PIN.

   If the HSM displays:

   ```
   WARNING CARD CONTAINS LMK SET, OVERWRITE? [Y/N]:
   ```

   Either press Y <Return> if the old data is to be overwritten (for example, an old Smartcard being reused), or, if necessary (for example if the wrong Smartcard has been inserted), press N <Return> to terminate the command.

5. When the Smartcard has been successfully created, the HSM displays:

   ```
   Device write complete, check: XXXXXX
   Make another copy? [Y/N]:
   ```

   Confirm the check value and remove the card.

   If another copy is required press Y <Return> and repeat Steps 3 to 5. Otherwise, lock the cam locks on the front panel and remove the keys to return the HSM to normal use.

Loading the Test Keys

It is good security practice to ensure that the LMK pairs used in the operational system are not used during test operations. It is useful to have a set of known Test LMKs to simplify cryptographic fault-finding. It also helps the manufacturer to diagnose cryptographic problems if they know the LMK pairs. Therefore, all customers are provided with an identical "Test Key Smartcard". To load this device, use the LK command, with the Smartcard in the reader in the normal way.

Test Variant LMK

The values of the LMK pairs contained in the "Test LMK" Smartcard are shown in Figure 1. The two Passwords are also held in this device, and their values are also shown in Figure 1.

The PIN for the Test Key Smartcard is:

1 2 3 4

LMK	Contents	LMK	Contents
00	01 01 01 01 01 01 01 01	01	79 02 CD 1F D3 6E F8 BA
02	20 20 20 20 20 20 20 20	03	31 31 31 31 31 31 31 31
04	40 40 40 40 40 40 40 40	05	51 51 51 51 51 51 51 51
06	61 61 61 61 61 61 61 61	07	70 70 70 70 70 70 70 70
08	80 80 80 80 80 80 80 80	09	91 91 91 91 91 91 91 91
10	A1 A1 A1 A1 A1 A1 A1 A1	11	B0 B0 B0 B0 B0 B0 B0 B0
12	C1 C1 01 01 01 01 01 01	13	D0 D0 01 01 01 01 01 01
14	E0 E0 01 01 01 01 01 01	15	F1 F1 01 01 01 01 01 01
16	1C 58 7F 1C 13 92 4F EF	17	01 01 01 01 01 01 01 01
18	01 01 01 01 01 01 01 01	19	01 01 01 01 01 01 01 01
20	02 02 02 02 02 02 02 02	21	04 04 04 04 04 04 04 04
22	07 07 07 07 07 07 07 07	23	10 10 10 10 10 10 10 10
24	13 13 13 13 13 13 13 13	25	15 15 15 15 15 15 15 15
26	16 16 16 16 16 16 16 16	27	19 19 19 19 19 19 19 19
28	1A 1A 1A 1A 1A 1A 1A 1A	29	1C 1C 1C 1C 1C 1C 1C 1C
30	23 23 23 23 23 23 23 23	31	25 25 25 25 25 25 25 25
32	26 26 26 26 26 26 26 26	33	29 29 29 29 29 29 29 29
34	2A 2A 2A 2A 2A 2A 2A 2A	35	2C 2C 2C 2C 2C 2C 2C 2C
36	2F 2F 2F 2F 2F 2F 2F 2F	37	31 31 31 31 31 31 31 31
38	01 01 01 01 01 01 01 01	39	01 01 01 01 01 01 01 01
Password 1	01 01 01 01 01 01 01 01		
Password 2	NOWISTHETIMEFORA		

Figure 1 – LMK Pairs (and Passwords) on the "Test LMK" Smartcard

The check value is 268604

Test Keyblock LMK

The values of the LMK contained in the Test Keyblock LMK Smartcard are shown in Figure 2. The two Passwords are also held in this device, and their values are also shown in Figure 2.

The PIN for the Test Key Smartcard is:

1 2 3 4

LMK	01 23 45 67 89 AB CD EF 80 80 80 80 80 80 80 80 FE DC BA 98 76 54 32 10
Password 1	89 89 89 89 89 89 89 89
Password 2	THEQUICKBROWNFOX

Figure 2 – LMK Pairs (and Passwords) on the "Test Keyblock LMK" Smartcard

The check value is 165126.

Chapter 4 - Operating Instructions

General

The HSM is normally online to the Host and does not require operator monitoring or intervention. In use, the HSM performs cryptographic processing in response to commands from the Host. Some commands are actioned by the user at the HSM Console terminal. These include commands involving plain text data, system configuration and others that do not concern the Host.

This chapter gives instructions for security operations, with the exception of LMK management, operations which are described in Chapter 3.

Entry of commands and data at the Console is not case sensitive (i.e., A has the same effect as a). Additional spaces can be inserted between characters to ease legibility during entry; they are ignored by the HSM. However they cannot be used between command characters (e.g. the LK command cannot be successfully entered as L K).

When entering sensitive (clear text) data, use the Inhibit Echo Back facility to ensure that the HSM does not echo the data to the Console screen. This is set at configuration using the "Echo" parameter in the CS (Configure Security) command. Instead of displaying the data, the HSM displays a star for each character entered. Thus:

```
0123456789ABCDEF
```

is shown on the screen as:

```
****************
```

To exit from a command during data entry, press <Control> and C simultaneously. The HSM responds with:

```
TERMINATED
```

Viewing HSM Status Information

There are eight 'Query' commands to display various settings in the HSM:

QA :	Query Auxiliary
QC :	Query Console
QH :	Query Host
QL :	Query aLarms
QP :	Query Printer
QS :	Query Security
GETTIME:	Displays the time and date.
VR :	Version

See the HSM 8000 Console Reference Manual for details of these commands.

Secure Mode

The HSM is put into the secure mode by operating both of the key locks on the front panel. Secure mode is required for certain secure commands which affect the security status of the HSM. These are GK, LK, LO, DC, CL, CS, SS, RS, CLEARERR, CLEARAUDIT, AUDITOPTIONS and MODTIME. Any attempt to use these commands without putting the HSM into secure mode will cause an error to be logged.

Authorise Activity State

The Authorise Activity state allows precise specification of authorised activities (including timeout period if required).

Authorise Activity State

The exact method used depends on how the HSM was set up using the CS console command.

The following examples use the menu method of activity selection see 1270A349 Console Reference Manual for full details of this command

If the HSM is set up to use Smartcard mode, with Echo on, proceed as follows:

```
Online> A <Return>
Enter LMK id: 00 <Return>
No activities are authorised for LMK id 00.
List of authorisable activities:
generate    genprint   component   import
export      pin        audit       admin
diagnostic  misc       command
Select category: pin <Return>
clear       mailer
Select sub-category, or <RETURN> for all: mailer <Return>
host        console
Select interface, or <RETURN> for all: <Return>
Enter time limit for pin.mailer, or <RETURN> for permanent: <Return>
Make activity persistent? [Y/N]: n <Return>
Enter additional activities to authorise? [y/N]: n <Return>

The following activities are pending authorisation:
pin.mailer

First Officer:
Insert Card for Security Officer and enter the PIN: **** <Return>
Second Officer:
Insert Card for Security Officer and enter the PIN: **** <Return>

The following activities are authorised for LMK id 00:
pin.mailer
Online-AUTH>
```

If the HSM is set up to use Password mode, with Echo off, proceed as follows:

```
Online> A <Return>
Enter LMK id: 00 <Return>
No activities are authorised for LMK id 00.
List of authorisable activities:
generate    genprint   component    import
export      pin        audit        admin
diagnostic  misc       command
Select category: pin <Return>
clear       mailer
Select sub-category, or <RETURN> for all: mailer <Return>
host        console
Select interface, or <RETURN> for all: <Return>
Enter time limit for pin.mailer, or <RETURN> for permanent: <Return>
Make activity persistent? [Y/N]: n <Return>
Enter additional activities to authorise? [y/N]: n <Return>

The following activities are pending authorisation:
pin.mailer
Password: ************ <Return>
```

```
Second Officer:
Password: ************ <Return>
AUTHORISED
Online-AUTH>
```

Cancelling Authorised Activity

The C (Cancel) command is used to cancel the Authorise activity state. An HSM reset (performed by pressing the RESET button on the front panel) also cancels all Authorised activities.

Proceed as follows:

```
Online Auth> C <Return>
Enter LMK id: 00 <Return>
Cancel pin.mailer? [y/N] y <Return>
No activities are authorised.
Online>
```

View Authorised Activities

The VA (View Authorised Activities) command allows the operator to view all currently authorised activities.

Proceed as follows:

```
Online Auth> VA <Return>
Enter LMK id: 00 <Return>
The following activities are authorised:
pin.mailer
Online Auth>
```

Smartcards

The HSM provides Console commands to support the use of Smartcards:

- FC : Format a Smartcard.
- CO : Create an Authorising Officer Smartcard.
- VC : Verify the contents of a Smartcard.
- NP : Change a Smartcard PIN.
- RS : Restore HSM settings from a Smartcard.
- RC : Read Smartcard Details (unidentifiable card).
- SS : Save HSM settings to a Smartcard.
- EJECT : Ejects the Smartcard.

See the HSM 8000 Console Reference Manual for details of these commands.

Logging Functions

An Error Log and an Audit Log are provided, each with a command to display the log and a command to clear the log. There is also a command to enable the user to set their timezone, so that the correct time is displayed in audit journal reports.

The Audit Log and Error Log are not retained if an alarm event occurs, as they can no longer be trusted.

See the HSM 8000 Console Reference Manual for details of the logging commands.

The Error Log

An Error Log and an Audit Log are provided, each with a command to display the log and a command to clear the log. There is also a command to enable the user to set their timezone, so that the correct time is displayed in audit log reports.

The Error log stores fault information for use by Thales e-Security support personnel. It contains 100 slots for error codes and sub-codes entries. After 100 entries the HSM will overwrite existing entries i.e. event 101 will overwrite the 1st entry. The error log is used to log unexpected software errors, hardware failures and alarm events. Whenever an error occurs, that error code is stored, along with the time, date and severity level. Additional errors that have the same error code cause the time and date of that code to be updated. In this way, each error type remains in the log (with the most recent time and date) and is not lost. The severity levels are:

- Informative (0) Something abnormal happened, but was not important.
- Recoverable (1) Something abnormal happened, but the unit recovered from it without rebooting or losing data.
- Major (2) Something abnormal happened, but the unit recovered from it but may have lost data/information due to restarting a process or re-initialising hardware. The unit may not function in a full capacity.
- Catastrophic (3) Something abnormal happened, and the unit had to reboot to recover.

Only catastrophic errors cause the HSM to reboot. New errors cause the Fault LED on the front panel to flash.

The Audit Journal

The Audit Log contains 2000 entries for audit records. Whenever the HSM state is altered through power-up, key-lock changes or console commands, the Audit log is updated with the action and the time and date. The Audit log can also be configured to record execution of almost any console or host command. The Audit Log records state changes until it is 100% full and for each subsequent state change the earliest (i.e. oldest) record in the log is deleted to make room for the new record. A number of host commands are provided which allow the host computer to extract and archive (print) audit records from the HSM.

Management of the Audit Log is performed from the console using the command 'AUDITOPTIONS', whilst 'AUDITLOG' is used to retrieve the log and 'CLEARAUDIT' to clear the log. The HSM must be put into the secure-authorised state in order to execute the 'AUDITOPTIONS' and 'CLEARAUDIT' console commands.

Note: Auditing host or console commands may impact HSM performance.

The SETTIME command can be used to set the internal clock to compensate for time zone difference so that local time can be recorded in the audit journal. The date and time can be checked using the GETTIME command.

Appendix A - Security Recommendations

Introduction

This appendix to the HSM Security Operations Manual is provided as guidance for the development of policies and systems, including countermeasures to threats and the mitigation of risks. These must exist in order to provide an appropriate environment for HSM devices. In some cases these are related to the functionality provided by the HSM itself.

This appendix is not intended to provide a definitive list of requirements for HSM operation. It should be read in conjunction with audit requirements and mandates from organisations and authorities relevant to the specific application and environment in which an HSM is being used.

This appendix uses the terms:

- MUST This word means that the definition is an absolute requirement to achieve an acceptable overall level of risk;
- MUST NOT This phrase means that the definition is an absolute prohibition of the specification to achieve an acceptable overall level of risk;
- SHOULD This word means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course;
- SHOULD NOT This phrase means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before being implemented.

Procedural Security

A system employing an HSM can only operate securely if the HSM's environment provides the procedural security that it requires, and if the HSM's security enforcing functions are utilised appropriately.

Note the requirements for procedural security are likely to extend beyond the Secure Area within which the HSM is used operationally (see the section "Measures to Protect Secure Area"), and are likely to include every aspect of an operation that contributes to the continuous secure management of HSMs and the mitigation of associated risks.

Recommendations for procedural security are as follows:

1. A management process MUST be in place for the system, to enable corrective action to be taken if any security elements, including procedures, are e.g. not being observed, failing their objectives, or could be efficiently improved.
2. An incident management process MUST be in place for the system, e.g. to enable action to be taken if any compromise to the security of the system is detected or suspected, or if any security elements of the system is in an unplanned or uncontrolled state.
3. The system MUST be audited regularly to help ensure that the intended overall level of risk is being achieved, by checking that the chosen security elements of the system (e.g. satisfying the requirements laid down in this appendix) are in place and are being used correctly.
4. The auditor MUST be independent of the operators of the security elements within the system.

Audit and records

Audits are required to help determine whether or not HSMs are being used appropriately. In this context, an audit is a review of records and procedures.

1. Audits MUST NOT themselves necessitate the recording of any sensitive information, (e.g. key material).
2. Whenever a maintenance function or authorised function is used, this fact MUST be recorded, with details of the function used, and the reason for its use.
3. Whenever the product is put into a new operating state this MUST be recorded.
4. It MUST always be possible to determine the current operating state of the HSM by viewing the records.
5. Every movement of an HSM from one location to another MUST be recorded, together with reason for movement.
6. Every access to the HSM Secure Area or PIN printing areas MUST be recorded, including details of damaged and destroyed PIN mailer material.
7. Every access to an authorising smartcard, LMK or HSM settings smartcard MUST be recorded and include the name of every officer involved and the reason for access.
8. Where key material or smartcard PINs are written down, every access MUST be recorded and include the name of every officer involved and the reason for access.
9. Every access to physical (cam) keys MUST be recorded and include the name of every officer involved.
10. The records MUST be regularly reviewed to aid discovery of any hostile action that may have occurred.
11. Incident management procedures MUST exist to react to and counter hostile actions however discovered.
12. The records SHOULD be easy to understand and organised in such a way as to make analysis both straightforward and useful.
13. Records SHOULD be regularly backed up and copies stored off-site in such a way that they can be easily restored if necessary.
14. All record entries MUST include a time and date.
15. All record entries MUST include a traceable signature. Where an entry involves more than one individual, e.g. the granting of access, all the individuals MUST sign the entry.
16. Sufficient resource MUST be available to allow complete records to be created.
17. The records MUST be protected against unauthorised modification.
18. There MUST be a record of all training activities relevant to the security system, and including any training exercises involving the facilities and equipment of the HSM Secure Area.
19. Before any deletions are made from the HSM's electronic log (e.g. using the CLEARAUDIT command from the Console to empty the Audit Log) the log MUST be correlated with the other record(s) of that HSM, and any differences fully investigated.

Note it will be important to check that the first entries in the AUDITLOG correspond exactly with the last time the AUDITLOG was cleared. This also implies that the AUDITLOG is not configured to wrap – where the oldest entries are automatically overwritten once it becomes full. It is also important to check that each change to the Secure state was authorised.

Identification and Authentication

The following requirements will be applied when a change of state is affected for an HSM with an online connection to the host. A more stringent process would be applicable in situations where the overall design or configuration of the system is being altered. However, the following requirements should be adequate to cover the day-to-day aspects of key management and both the planned and unplanned physical replacement of an HSM.

1. The persistent state (i.e. Online, Offline, Secure and/or Authorised) and physical condition of every HSM within the system MUST always be determinable from the records.
2. Necessary transitory states can be assumed but MUST be recorded if they are to be utilised in addition to their role in the transition to other operating states.
3. If an individual is no longer an authorised officer, procedures MUST be put in place to prevent him from acting subsequently as an authorised officer e.g. by changing or replacing the sensitive items to which the officer was exposed e.g. LMK key components, smartcards and PINS/passwords.

Use of Authorised State (and the Security Officer role of the HSM Manager)

The Security Officer role utilised by the (Local or Remote) HSM Manager requires equivalent controls to the Authorised State accessed via the Console terminal.

1. At least 2 separate authorised officers MUST be required to put the HSM into Authorised state.
2. Before the HSM is put into the Authorised state, the identities and authority of both authorised officers MUST be checked and logged, with audit entries signed by both authorised officers.
3. Before either one or both authorised officers leave the HSM Secure Area (even temporarily), the HSM MUST be taken out of Authorised state.

Use of Secure State

1. At least 2 separate operators MUST be required to switch the HSM into Secure state.
2. Before the HSM is switched into Secure state, the identities of both operators MUST be checked and logged, with audit entries signed by both operators.
3. Before either one or both operators leave the HSM Secure Area (even temporarily), the HSM MUST be switched out of Secure state.

Use of Offline State

1. Before the HSM is switched into the Offline state, the identity of the operator(s) MUST be checked and logged.
2. Before the operator(s) leave the HSM Secure Area (even temporarily), any key under their control MUST be removed from its HSM and secured.

Use of the Operator role of the HSM Manager

1. Before any HSM is put into the Operator role, the identity and authority of the authorised officer MUST be checked and logged, with audit entries signed by the authorised officer.
2. Before the authorised officer leaves the HSM Secure Area (even temporarily), the HSM MUST be taken out of the Operator role.

Use of the Guest role of the HSM Manager

The use of the HSM Manager requires knowledge of the password used in the encryption of the communication traffic to the specific HSM.

1. If an individual is no longer authorised to work on HSMs, in the Secure Area, procedures SHOULD be put in place to prevent him (or her) from accessing any HSM via the HSM Manager, e.g. by changing the password(s) known to them.

Command Security

There are a number of standard features provided by the HSM 8000 that can help "lock down" the HSM to perform only the functions that are required by the host application.

1. Use ConfigCmds to disable all unused host and console commands.
2. Use ConfigPB to disable all unused PIN block formats.
3. Use Multiple Authorised Activities instead of the global Authorised state, thus permitting specific authorised commands, rather than all authorised commands.
4. Use the auditing capabilities to record and detect unexpected commands or events:
   - All HSM commands that require the HSM to be in the Authorised or Secure state must be audited by the HSM itself. This is achieved using the console command AUDITOPTIONS.
   - The host system must extract the audit records from inside the HSM, and store them securely. The audit records can be extracted from the HSM using the host command 'Q2'.
   - Prior to viewing the extracted audit records, they should be validated by the HSM. This is achieved using the host command 'Q8'.

Measures to Protect HSM Secure Area

Figure A.1 below shows an HSM, printer & console in a "secure area with limited access". The Host Computer and HSM are on a secure private network – separate from any user-orientated network and any connection to the Internet, even via a firewall and DMZ, etc. When necessary, the Console terminal is connected directly to the HSM e.g. via a suitable RS232 serial cable.

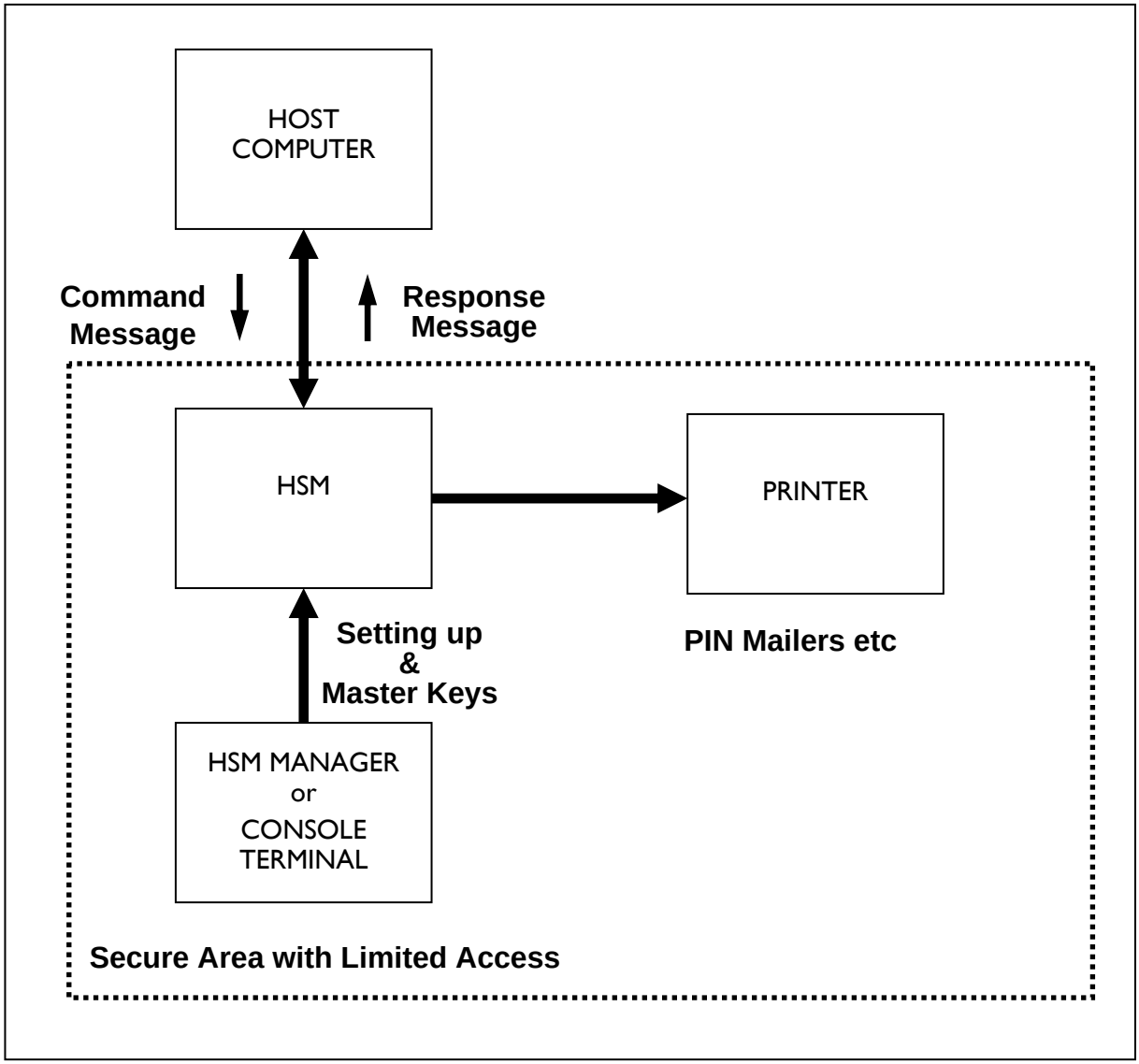

Figure A.1 - HSM in a Secure Area

Recommendations for the HSM secure area are as follows:

1. The operating procedures associated with the HSM Secure Area plus all the equipment and the interconnections between them MUST be subject to a management process that will deliver the required system functionality and achieve an acceptable level of overall risk.

   The HSM, HSM Manager, Console terminal and printer (if attached) MUST be located in a physically secure area during all operational use.

2. Access to the HSM Secure Area MUST only be provided when necessary.

3. Access to the HSM Secure Area MUST be recorded.
4. The HSM Secure Area MUST NOT ever be occupied by a lone individual.
5. The HSM Secure Area MUST be subject to protection against electromagnetic emanation if this is deemed to be a threat.
6. HSM peripherals (e.g. printer) MUST only be attached when required.
7. An HSM MUST be inspected, or subject to equivalent checks on its identity and integrity, when it enters or leaves the HSM Secure Area.
8. All staff associated with the security system MUST be instructed in their responsibilities and adequately trained in the use of relevant equipment, processes and procedures.

In the case of a HSM attached to a host via an Ethernet network, the following note applies:

Important Note: In order to ensure that an HSM only processes commands on behalf of the legitimate host computer, it is strongly recommended that a private Ethernet network segment is used. The only devices on this network should be the host and its associated HSM(s).

Host Application Functions

1. The host application MUST be written such that cryptographic requests are made as appropriate to the HSM.
2. The host application MUST be written such that cryptographic responses from the HSM are acted on as appropriate.
3. The host application MUST react appropriately in the event that an error is received from the HSM.
4. There MUST be procedures in place to detect if the host application is operating incorrectly.

Local HSM Manager Functions

The Local HSM Manager runs on a standard computer and is an alternative to managing an HSM from a Console terminal.

Refer to the relevant User Manual for more details of the preferred Security Environment for the HSM Manager.

1. The user MUST define and implement suitable management procedures.
2. The user's management procedures MUST mandate the use of the correct software - to reduce the possibility of intercepting PINs or passwords.
3. Efforts to operate the HSM Manager securely SHOULD be enhanced by minimising the presence of unnecessary hardware and other software.
4. All hardware and software within the computer hosting the HSM Manager MUST be operated and maintained according to the vendor's recommendations.

Cryptographic Key Management

In some cases key management requirements are dictated by card schemes or other authorities such as a central bank. Also some aspects of key management, such as the replacement of terminal keys, may be automated within an application.

1. The user MUST define and implement suitable key management procedures.
2. For every cryptographic key, a suitable lifetime and key length MUST be chosen, as appropriate given:
   - card scheme mandates or other requirements relevant to the application and environment in which the key is used;
   - the effective strength of the associated cryptographic algorithm;
   - the function of the key (e.g. key encryption, data encryption, data authentication);
   - the volume of use;
   - the propensity to attack or unauthorised disclosure;
   - the full implications of actual or possible compromise both during and after active use.
3. All cryptographic keys used within the system MUST be updated on a regular basis in an appropriate manner.
4. When a cryptographic key (in particular the LMK) is updated, data protected by that key might need to be translated from the 'old' key to the 'new' key. Once this translation process is complete, the 'old' key SHOULD be removed from the HSM.

Cryptographic Key Generation

1. When generating an LMK component for use in the HSM, the secret values SHOULD be generated randomly by the HSM rather than entered manually.
2. Keys that are not generated by the HSM MUST be generated using a good random number generator.
3. The random number generator used for external key generation MUST be subject to statistical testing.

Protection of Cryptographic Key Material

Protection of keys is critical to the security of the system in which the HSM operates.

1. Keys and key components MUST NOT be disclosed to unauthorised individuals. This is particularly important for the LMK.
2. The management of key components MUST fully and continuously support the requirements of the "split knowledge" approach, helping to protect the system and its staff.
3. Untrusted keys MUST NOT be loaded or used. This is particularly important for the LMK.
4. Key material MUST NOT be loaded or used with untrusted equipment.
5. Unencrypted key material (such as ZMK components) MUST be distributed in a physically secure manner.
6. The secure management of each unencrypted key used in an HSM system MUST be the responsibility of a trusted individual.
7. Key material SHOULD NOT be written down.

8. Encryption of key material that is not subsequently subject to physical protection MUST be performed using an appropriately secure algorithm with a sufficiently large key length.
9. Encryption of key material that is not subsequently subject to physical protection MUST be performed using a physically secure key or one that is itself encrypted.
10. Procedures MUST exist such that in the event of key material compromise, keys are replaced as necessary.
11. The utilisation of each key component MUST be controlled by separate authorised officers.
12. Where keys or key components are stored on smartcards, the smartcards MUST be treated with an adequate degree of physical security to prevent unauthorised access.

Key Material Usage

1. Test key material MUST NOT be used in the live operation.
2. Keys MUST only be used for their defined purpose.

HSM PIN and Password Security

1. The user MUST define and implement suitable management procedures.
2. The PIN associated with each smartcard MUST be created securely e.g. created at random. Obvious, common, predictable or previously used values MUST NOT be used intentionally.
3. Strong passwords SHOULD be used. Good properties for strong passwords are that they:
    - Contain upper and lower case characters
    - Contain numbers, letters and punctuation characters
    - Contain at least 8 random characters
    - Don't contain dictionary words
    - Don't use spouse's/children's names
    - Don't intentionally re-use old passwords
4. The frequency for changing passwords SHOULD be stated and be sufficient for the role.
5. Passwords SHOULD NOT be disclosed to others.
6. The process for managing forgotten passwords SHOULD be set out in the user's security management procedures.
7. If the PINs or passwords are written down, they MUST be stored securely and separately.
8. If a PIN or password is compromised (including a previously authorised individual becoming unauthorised), it MUST be invalidated and a replacement issued.
9. Everyone, and especially operators and authorised officers, MUST have no unauthorised knowledge of any PIN or password.

Smartcard Security

Smartcards are used for storing three distinct types of sensitive information:

- storage of key components – particularly the LMK;
- storage of authorising officer credentials;
- storage of HSM alarm, security and host settings.

Security precautions for the cards are as follows:

1. The user MUST define and implement suitable management procedures.
2. All smartcards containing sensitive information MUST be stored securely.
3. Smartcards containing sensitive information MUST be stored separately from each other.
4. Access to any smartcard containing sensitive information MUST be recorded.
5. Smartcards containing LMK components MUST only be made available to authorised officers, and only when necessary.
6. If a smartcard containing sensitive information is compromised (including a previously authorised individual becoming unauthorised), suitable measures MUST be taken to re-establish adequate security for the system e.g. by changing the LMK.
7. Copies of the smartcards containing sensitive information SHOULD be kept separately, off-site. These copies MUST be subject to equivalent access controls as the original smartcards.
8. All smartcards containing sensitive information SHOULD be periodically checked to ensure that they are functional and have not been corrupted.
9. There MUST NOT be any unauthorised access to smartcards containing sensitive information – especially by operators and authorised officers.
10. Only limited reliance MUST be placed on the security afforded by a smartcard's PIN in controlling access to its contents.

    Note that the individual components of a cryptographic key (such as the LMK), each of which is normally stored on a separate smartcard, are not equivalent to each other.

Physical Key Security

The HSM is supplied with two physical keys for the front panel. These have three functions:

- Both locks must be opened in order to remove the HSM from the cabinet.
- Both locks must be opened to put the HSM into the Secure state.
- One lock (either one) must be opened to put the HSM into the Offline state.

Security precautions for the keys are as follows:

1. The user MUST define and implement suitable key management procedures.
2. The physical (cam) keys MUST be stored securely.
3. The physical key MUST only be made available when necessary.
4. If a previously authorised individual becomes unauthorised, measures MUST be taken to ensure that the individual no longer has access to the key.
5. Each use of the physical key on an HSM in operational use MUST be recorded.
6. There MUST NOT be any unauthorised access to a physical key – especially by operators and authorised officers.

HSM Integrity

HSM Traceability

1. Procedures MUST exist so that movement of HSM devices from one location to another is controlled and recorded.
2. This record SHOULD be verified periodically to provide a high level of confidence in the location of all HSMs in the system.
3. If records show any discrepancy in the location of HSMs, this MUST be investigated, and immediate consideration SHOULD be given to withdrawing the HSM from service.

HSM Physical Integrity

1. When in use by the host application, the HSM MUST be in a secure environment.
2. When being transported to or from a user's premises, trusted couriers MUST be used.
3. If integrity of transport procedures is in doubt (for example if the HSM arrives substantially late without explanation), this MUST be investigated.
4. On arrival at a secure location, the HSM and its packaging MUST be inspected for signs of tampering prior to installation.
5. Anything, such as additional labels, that would alter the external appearance of the HSM SHOULD be discouraged.
6. In normal usage, the HSM MUST periodically have a routine inspection for signs of tampering.
7. Any HSM that appears to have been tampered with MUST NOT be loaded with keys or connected to the host application.
8. Any HSM that appears to have been tampered whilst connected to the host application MUST be withdrawn from service as soon as possible; and the system MUST become subject to the incident management process.

HSM Maintenance

1. HSM maintenance MUST only be performed by trusted personnel.
2. Before an HSM is given to the maintenance authority it SHOULD be given a routine inspection.
3. The HSM SHOULD be removed from the Secure Area for maintenance.
4. All maintenance operations MUST be recorded.
5. If the HSM is left unattended during maintenance, measures MUST be taken to ensure that no one else has access to it.
6. Before an HSM is given to the maintenance authority, the LMKs MUST be erased.
7. Before an HSM is given to the maintenance authority, the Test LMK MUST be loaded in place of each live LMK (i.e. a non-Test LMK).
8. Before an HSM is given to the maintenance authority it MUST be put into the Offline state as described in the manual.
9. When an HSM is returned by the maintenance authority, it MUST be subject to the inspection procedures.
10. The return of faulty HSMs to the manufacturer MUST take place under the control of the incident management process.

Note that this approach is designed to help ensure that a faulty HSM, e.g. one on which the deletion of all LMKs cannot be confirmed or from which the AUDITLOG cannot be inspected, is handled appropriately and within an acceptable level of risk. The necessary decisions are likely to be more appropriate to the incident management process than to normal operations – as these might not be suitable for handling unusual risks and issues.

Normal Operations

These measures are applicable whilst the HSM is being held or used within the user's Secure Area. If a functional HSM is to leave the Secure Area this is considered to be a maintenance activity e.g. the LMK would be replaced by the Test LMK.

The HSM contains an intrusion detection mechanism that is always armed.

1. When the HSM is to have an online connection to the host application it MUST be locked in position by the action of being put into the Online state.
2. When the HSM contains an LMK, the motion detector MUST be enabled.
3. When the HSM contains an LMK, the temperature sensor MUST be enabled.
4. The HSM's diagnostic tests MUST be run on a regular basis. (These tests exercise the HSM's cryptographic functions as well as the general operational correctness of the device).
5. Any HSM that develops a fault whilst it contains an LMK MUST become subject to the incident management process if deletion of the LMK cannot be confirmed or the Audit Log cannot be inspected.
6. A faulty HSM MUST NOT be given an online connection to the host application.
7. The system design SHOULD include adequate contingencies for system failures, e.g. specific, isolated, localised, geographical or systemic.
8. Where the system design implies continuous availability of an HSM, in the event of failure of an HSM, a means of quickly switching operation to another HSM SHOULD be available at all times. (An automated load-balancing mechanism may be useful for this purpose.)
9. At least two authorised officers MUST control the initialisation of a new HSM.
10. All online HSMs MUST be subject to regular monitoring, particularly with respect to the management of any HSM where the "Error" LED or "Alarm" LED has become illuminated.

    Note that normal operations can only continue with an HSM if a benign explanation can be established for a resettable error or alarm condition.

Timely Return to the Online State

1. The device MUST NOT remain in Authorised state or Secure state inadvertently. If either state is active when it is not required to be active, the HSM MUST immediately either be switched off or returned to the Online state.

   Note that the Secure state is not indicated by the state of the HSM's "Secure" LED. The Secure state is achieved by using both physical keys to open both locks. The "Secure" LED is illuminated to indicate that the HSM contains an LMK.

Inspection Procedures

This section describes procedures that are carried out to confirm that the HSM has not been subject to accidental or deliberate tampering that may lead to insecure operation.

1. The inspection procedures MUST be performed by trusted personnel.
2. Details of the personnel performing the inspection procedures MUST be recorded.
3. The results of each step of the inspection procedures MUST be recorded.

Frequency of Inspection

Both the "Initial Inspection Procedure" and the "Routine Inspection Procedure" MUST be carried out whenever the HSM is received from an external source. That is:

- on initial receipt of the HSM;
- at any time after the HSM has travelled outside of the HSM Secure Area.

Additionally, the "Routine Inspection Procedure" SHOULD be carried out:

- after any known unauthorised entry to the HSM Secure Area;
- periodically, e.g. on a three-monthly basis, to confirm continued secure operation of the device in case of unknown unauthorised entry into the HSM Secure Area or accidental damage to the HSM.

Initial Inspection Procedure

The initial inspection procedure is as follows:

1. The arrival of the HSM MUST match expectations in respect of model type and delivery timing.
2. The delivery details MUST correspond to information provided by the originator e.g. with respect to courier used and the delivery tracking number.
3. Any opening of the HSM delivery packaging other than by the intended addressee MUST be traceable to an acceptable source e.g. the result of a customs check.
4. A detailed record of the HSM MUST be established for reference during audits and routine inspections.

   Note that this record is meant to establish the authenticity of the HSM and aid the checks on its continuous integrity. It MUST include details of all serial numbers i.e. of the HSM and its tamper-evident seals, plus the physical keys. It SHOULD also include a record of the condition of the exterior of the HSM. Where possible all details SHOULD be verified with their originator(s). This record formalises an inspector's knowledge of the general design of the HSM and its accessible security features, plus their knowledge of this particular HSM. In this respect, an active comparison with existing equipment can also be of value.

Routine Inspection Procedure

The inspection procedure is as follows:

1. The serial number of the HSM, as stated on the label on the back of the HSM, MUST correspond correctly with the record created during the initial inspection.
2. The operational mode of the HSM MUST be as expected. This MUST include verification of the HSM's operating state (Authorised state, Secure state or Online state) and the condition of the Secure LED.
3. The identification numbers of the physical keys MUST correspond correctly with the record created during the initial inspection.
4. All physical keys associated with the HSM MUST operate correctly.
5. The HSM MUST NOT report any permanent, significant or unexplained faults i.e. it is only acceptable for the "Error" LED to be illuminated, either permanently or flashing if there is a known benign explanation.
6. The HSM's diagnostic test console DT command, as described in the HSM 8000 Console Reference Manual, MUST demonstrate the correct basic operation of the HSM. The result of each test MUST be "OK". The final test MUST be followed by the phrase:

   ```
   Diagnostics complete
   ```

   Note that use of the DT command requires the HSM to be in the Secure state.
7. The HSM VR console command, as described in the HSM 8000 Console Reference Manual, MUST confirm that the version number reported agrees with the record created during the initial inspection.
8. Any cables connected to the HSM MUST terminate at the expected location/equipment; and there MUST be no signs of physical damage to the cables themselves.
9. The HSM MUST have no unrecorded physical changes or damage.
10. Any HSM whose authenticity and integrity cannot be adequately established MUST become subject to the incident management process.

Appendix B - Remote HSM Manager Recommendations

Background

The Thales e-Security Remote HSM Manager is a PC-based product that allows communication with, and management of, an HSM 8000 Host Security Module over a wide area network. As such, it permits "remote" users to perform almost all console activity (see HSM 8000 Console Reference Manual) without requiring physical access to the HSM.

In order to provide secure communication between a remote user and an HSM, all communication will be encrypted using a 3-DES session key, exchanged between the relevant parties and encrypted under the RSA public key of the user and signed using the RSA private key of the HSM.

Remote Management Smart Cards

Two types of smart card, with slightly different applications, are issued to users of the Remote HSM Manager. They are known as *administrator cards* and *operator cards*.

Comment on Terminology

The terms "administrator" and "operator" are generic terms used in Remote HSM Manager documentation. Users with administrator cards are permitted to carry out a variety of (largely) administrative tasks (for example, the same state changes that are possible with the physical front panel keys of the HSM 8000) whereas users with operator cards carry out sensitive activities, usually involving management of cryptographic keys.

Administrator cards are analogous to the physical front panel keys of the HSM 8000, in that there is a "left" administrator card, and a "right" administrator card. In order to put the HSM into the secure state (which traditionally requires both front panel keys to be turned), the Remote HSM Manager requires both a "left" and a "right" administrator card (and the cards' corresponding PINs).

Operator cards are analogous to the regular HSM cards that contain either LMK components or LMK Authorising Officer passwords.

Organisations using the Remote HSM Manager may well use different names to describe the above roles and so must ensure that the relationship between Thales terminology and their own personnel structure is properly understood.

Certificate Authority

Each administrator and operator smart card contains an RSA public/private key pair and, similarly, each HSM is initialised with a public/private key pair. In order to have confidence in the authenticity of the various public keys, each such key will be held in the form of a certificate, signed by the private key of a (trusted) *Certificate Authority* (CA). The corresponding CA public key (used to verify the certificates) is stored in each smart card and HSM.

The CA functionality is standard in all HSM 8000s that support the remote management solution. All user interaction with the CA functionality is via the HSM's console interface.

Security Group

The term "security group" is used to describe a set of administrator and operator smart cards and a single HSM, such that (secure) remote communication between the cards and the HSM in the group is permitted. Communication requires both the card and the HSM to have prior knowledge of each other.

A necessary condition for a card and an HSM to communicate is that their RSA public keys are both signed by the same CA. However, this is not a sufficient condition, and it is quite possible to have non-overlapping security groups created via the same CA.

Recovery

One concern relating to the HSMs used in the remote management solution is that if an HSM is tampered then it will lose its public and private keys from memory and it will be necessary to generate a new key pair. This could involve considerable operational inconvenience.

Therefore, a mechanism involving a 3-DES Recovery Master Key (RMK) has been defined and allows a public/private key pair to be restored into the HSM's secure memory following a tamper.

HSM Base Firmware

All HSM 8000s used in the remote management solution have base firmware v3.1 or above, as specified in HSM 8000 Console Reference Manual and HSM 8000 Host Reference Manual, and in particular support multiple Local Master Keys (LMKs) in both variant and key block format.

Purpose of this Appendix

This appendix provides guidelines for the secure operation of the Remote HSM Manager. It is not intended as an Installation Manual (see HSM 8000 Remote HSM Manager Installation Guide) or as a User Guide (see HSM 8000 Remote HSM Manager User's Guide), but instead it provides "security best practice" advice for organisations that are using the Remote HSM Manager.

This appendix does not replace the recommendations in Appendix A - Security Recommendations, but simply extends them to include the use of the Remote HSM Manager.

Assumptions

This appendix assumes that the reader is familiar with the operation of the HSM (including console functionality) and the Remote HSM Manager.

Terminology

In accordance with Appendix A - Security Recommendations, the terms "MUST", "MUST NOT", "SHOULD" and "SHOULD NOT" will have the following meanings in this appendix:

- MUST: this indicates an absolute requirement to achieve an acceptable overall level of risk;
- MUST NOT: this indicates an absolute prohibition of the specified activity in order to achieve an acceptable overall level of risk;
- SHOULD: this means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully evaluated before choosing a different course;
- SHOULD NOT: this means that there may exist valid reasons in particular circumstances when the specified activity is acceptable or even useful, but the full implications must be understood and evaluated before the activity is implemented.

Remote HSM Manager Best Practice

Introduction

The following security guidelines should be used to complement Appendix A - Security Recommendations. Both appendices should be read in conjunction with existing security policies and procedures, audit requirements and mandates from organisations and authorities relevant to the specific application and environment in which the HSMs are being used.

Personnel

Two types of Remote HSM Manager user are defined, namely *Administrators* and *Operators*. Specifically, an Administrator is a user with an administrator smart card and an Operator has an operator smart card. Administrators are generally responsible for the day-to-day operations of the Remote HSM Manager, whereas Operators are involved in more sensitive activities, such as key management.

In addition, someone responsible for the overall operation and security of the Remote HSM Manager needs to be identified. For the purposes of this appendix, this person will be designated as the *Security Manager*.

1. The Security Manager MUST have access to a secure area (such as a safe) for the storage of Remote HSM Manager documentation, procedures, audit records and other sensitive items. Other Remote HSM Manager users MUST NOT have access to this area.

2. Users of the Remote HSM Manager SHOULD NOT have more than one of the Administrator, Operator or Security Manager roles.

3. Written justification SHOULD be provided by the Security Manager if it is deemed necessary for a user to carry out more than one of the roles.

4. An Administrator with a left administrator smart card MUST NOT be allowed to possess (even temporarily) a right administrator smart card, and vice versa.

5. Every Remote HSM Manager user, including the Security Manager, MUST have a named deputy, with the same level of access and responsibility.

6. All users MUST be given adequate training to allow them to carry out their roles.

7. All users MUST be made fully aware of their responsibilities regarding the security of the Remote HSM Manager.

8. All users SHOULD sign affidavits stating that they understand their roles and responsibilities with respect to the Remote HSM Manager and that they will carry out their duties to the best of their abilities.

9. Administrators and Operators who no longer need access to the Remote HSM Manager (e.g. have left the organisation, have been assigned to a new department or are on extended leave, etc) MUST be deleted immediately from the system and their smart cards MUST have all contents deleted, using the functionality of either the HSM console, the Remote HSM Manager or by physically destroying the card.

Procedures

All Remote HSM Manager processes and procedures must be fully documented.

1. All procedures relating to the security and operation of the Remote HSM Manager MUST be fully documented; the Security Manager SHOULD be responsible for the creation, maintenance and security of such documents.

2. Documentation regarding the security and operation of the Remote HSM Manager SHOULD be distributed on a "need-to-know" basis.

3. Documentation regarding the security and operation of the Remote HSM Manager MUST be reviewed and updated regularly.

4. The Security Manager MUST ensure that all procedures relating to the security and operation of the Remote HSM Manager are followed correctly.

5. Processes and procedures for the investigation of error conditions and security incidents relating to the Remote HSM Manager MUST be fully documented; the Security Manager SHOULD be responsible for the creation, maintenance and security of such documents.

6. The Security Manager MUST ensure that all processes and procedures relating to the investigation of error conditions and security incidents are followed correctly.

7. Documentation regarding the investigation of error conditions and security incidents MUST be reviewed and updated regularly, especially following an incident.

Audit

Detailed audit logs of all activity relating to the Remote HSM Manager must be maintained. These will include HSM audit logs, access logs, activity logs and error logs and may be held in electronic or paper form. The following guidelines should be read in conjunction with the more general guidelines in Appendix A - Security Recommendations.

1. A detailed audit policy for the Remote HSM Manager MUST be documented; the Security Manager SHOULD be responsible for the creation, maintenance and security of this policy document.

2. The Security Manager MUST be responsible for ensuring adherence to the audit policy.

3. Records of all Remote HSM Manager activity MUST be made; this MUST include:
   - HSM management and user events (see, for example, Chapter 3 of HSM 8000 Remote HSM Manager User's Guide);
   - personnel;
   - security incidents;
   - details of all personalised smart cards and HSMs;
   - access to the Remote HSM Manager operations room (access logs and CCTV images);
   - access to the safe in the operations room;
   - access to various smart cards and PINs (administrator cards, operator cards, CA private key share cards, RMK component cards, etc);
   - access to documents relating to the Remote HSM Manager, including audit and error logs.

4. Audit logs MUST be stored securely by the Security Manager.

5. Back-up copies of all logs MUST be made and SHOULD be stored in a separate location from the primary logs.

6. Audit logs MUST only be accessible on a "need-to-know" basis.

7. A log of all "unexpected" incidents (including errors) during the operation of the Remote HSM Manager MUST be kept.

8. All audit records MUST include, as a minimum, a date/time stamp and a brief description of the event that is being recorded.

9. Paper-based logs MUST also include the name and signature of the person making the log entry.

10. In so far as is practical, audit records SHOULD be protected from tampering.

11. Audit logs SHOULD be retained for inspection for a period of not less than 2 years.

12. HSM audit logs MUST be copied to file or printed before the first records are overwritten (i.e. before 2000 auditable events are recorded, see HSM 8000 Remote HSM Manager User's Guide).

13. The Security Manager SHOULD review the audit logs on a regular basis and all anomalies MUST be investigated.

14. An independent review of all audit logs SHOULD be conducted annually (say).

Physical Security

Many Remote HSM Manager activities are extremely sensitive and need to be carried out in a secure environment.

1. The Remote HSM Manager MUST be operated in an Operations Room, which is a physically secure environment.

2. Access to the Operations Room MUST be controlled and personnel who do not need access MUST NOT be given access.

3. Users who previously had access to the Operations Room but no longer need access MUST be revoked on the access control system.

4. Access to the Operations Room SHOULD require a 2-factor mechanism (i.e. "something you have", such as a physical token, and "something you know" or "something you are", such as a PIN/password or a biometric).

5. If the Operations Room is occupied, there SHOULD be a minimum of 2 personnel present.

6. The loss or theft of a Operations Room physical access token MUST be reported immediately to the Security Manager and the token revoked on the access control system; the circumstances of the loss/theft MUST be investigated.

7. It MUST NOT be possible to leave the door to the Operations Room open for longer than a specified period of time without an alarm being raised; such an alarm MUST be investigated immediately.

8. All access to the Operations Room MUST be logged; each record MUST contain, as a minimum, a date/time stamp and a user identifier.

9. Exit from the Operations Room SHOULD be recorded by the access control system.

10. All failed access to the Operations Room MUST be recorded in the access log.

11. Failed access attempts MUST be investigated.

12. The door to the Operations Room SHOULD be covered by a CCTV camera.

13. Authorised users of the Operations Room SHOULD NOT have access to the access logs or CCTV images.

14. Access logs and CCTV images MUST be retained for inspection for a period of time that is compatible with organisational policies, but SHOULD be at least 6 months.

15. The Operations Room SHOULD be alarmed outside "normal" operating hours.

16. CCTV MUST NOT be used inside the Operations Room.

17. All cabling inside the Operations Room MUST be clearly visible.

18. There SHOULD be no network access to the Operations Room, except as necessary to allow communication with the HSMs.

19. The Operations Room MUST contain a "dual access" safe for the storage of sensitive items; dual access could be (for example) a physical key and a PIN/password.

20. Access to the safe MUST require two people.

21. All access to the safe MUST be logged and MUST include, as a minimum, a date/time stamp, user name and the reason for access.

22. The Remote HSM Manager Linux boot CD MUST be stored in the safe when not in use; ideally it SHOULD be stored in a uniquely-numbered tamper-evident container, with a procedure in place to check the container number on each access.

23. Smart card readers SHOULD be stored in the safe when not in use.

24. If a laptop is used to run the Remote HSM Manager then it SHOULD be stored in the safe when not in use.

25. If a desktop PC is used to run the Remote HSM Manager then it SHOULD be locked to prevent access to the internal circuitry.

26. The software environment of the Remote HSM Manager PC/laptop MUST not be modified (for example, by installing software after the laptop has started). Additionally, the Remote HSM Manager Linux boot CD must not be loaded in a virtual operating system environment.

27. The PC/laptop, smart card readers and all cabling MUST be checked for signs of tampering before each Remote HSM Manager session.

28. Equipment that is not required for the operation of the Remote HSM Manager MUST NOT be brought into the Operations Room; such equipment includes data analysers, cameras, etc.

29. Loss or theft of any Remote HSM Manager equipment MUST be investigated by the Security Manager and any necessary remedial action MUST be immediately instigated.

30. The network communications link between the Operations Room and the secure area housing the physical HSM MUST be secured to provide further protection for the system. Examples of such protection include virtual private networks, firewalls, encrypted links, etc.

HSM Security Configuration

HSM configuration is described in HSM 8000 Remote HSM Manager User's Guide, and includes a number of security related activities.

1. Security configuration, via the "Initial Settings" menu item, SHOULD retain the default settings unless there is a good operational reason to do otherwise. Special consideration MUST be given to configuration settings involving:
   - authorised state;
   - decimalisation tables;
   - key import and export.
2. Non-default security configuration settings MUST be approved, in writing, by the Security Manager. Such approval SHOULD include a justification for the decision.
3. The temperature alarm and the movement alarm SHOULD be enabled, via the "Advanced Settings" menu item.
4. Fraud detection SHOULD be enabled, via the Advanced Settings menu item. The fraud detection parameters SHOULD be monitored to ensure that they are, and continue to be, appropriate for the HSM environment.
5. A decision to disable the temperature or movement alarm or to disable fraud detection MUST be approved, in writing, by the Security Manager. Such approval SHOULD include a justification for the decision.
6. Host commands that are not required for operations MUST be disabled, via the "Host Commands" menu item.
7. PIN block formats that are not required for operations SHOULD be disabled, via the "PIN Blocks" menu item. In particular, PIN block formats that do not involve an account number MUST be disabled unless needed.
8. A decision to enable (i.e. not disable) a host command or a PIN block format that is not an operational requirement MUST be approved, in writing, by the Security Manager. Such approval SHOULD include a justification for the decision.
9. All Remote HSM Manager activities and User Events SHOULD be audited by the HSM. These are enabled via the "Auditing" menu item. As noted in HSM 8000 Remote HSM Manager User's Guide, this may impact HSM performance and so the extent of auditable activity SHOULD be reviewed from time to time.
10. Decisions regarding those Remote HSM Manager activities and User Events that are not to be audited by the HSM MUST be approved, in writing, by the Security Manager. Such approval SHOULD include a justification for the decision.
11. All configuration selections SHOULD be saved to files, via the "Save Settings" menu item. Back-up copies of such files SHOULD be made.

Certificate Authority

The *Certificate Authority* (CA) is critical to the security of the Remote HSM Manager, although its functions are not part of the Remote HSM Manager! All HSMs and all administrator and operator smart cards used in the remote management solution must possess an RSA public/private key pair, with the public key held in the form of a certificate signed by the CA's private key.

A one-off process to generate the CA public/private key pair is required, involving any HSM whose firmware supports the remote management solution. This is achieved via the "RI" console command and is described in detail in Chapter 3 of HSM 8000 Remote HSM Manager Installation Guide.

Thereafter, individual HSMs generate an RSA public/private key pair and the public key is signed using the CA private key. The "RH" console command is used to generate an HSM key pair and is described in detail in Chapter 4 of HSM 8000 Remote HSM Manager Installation Guide. Similarly, any of the HSMs can be used to generate public/private key pairs for smart cards (with the public keys signed by the CA private key) and the results written to the smart cards. This uses the "RR" console command and is described in detail in Chapter 5 of HSM 8000 Remote HSM Manager Installation Guide.

The CA public key, in the form of a self-signed certificate, is loaded into each HSM and onto each smart card as part of the above processes. A "transport PIN" is set for each smart card (administrator and operator) as part of the "RR" command processing.

The use of the various public/private keys allows the creation of the Security Group and forms the basis of secure communication between the Remote HSM Manager and the HSM(s).

The CA private key is stored on various smart cards (different from the administrator/operator cards) via a (k, n)-threshold scheme[2]. The only restrictions on the values of the parameters "k" and "n" that are enforced by the HSM are that $3 \leq k \leq n \leq 9$. The people responsible for the CA private key shares are called "shareholders".

Remote HSM Manager Administrators and Operators may act as shareholders, but there is no requirement for them to do so. In general, the choice of shareholders will depend on the organisational structure.

1. CA-related activities SHOULD take place in a secure area.

2. The Security Manager MUST take overall responsibility for all CA activities and MUST ensure that all CA-related procedures are followed correctly.

3. The Security Manager MUST maintain a log of shareholder names and the corresponding card number and share number; the log SHOULD be stored securely.

4. Shareholders MUST be fully briefed by the Security Manager with regard to their roles and responsibilities.

5. Shareholders SHOULD sign affidavits stating that they understand their roles and responsibilities with respect to their CA private key shares and that they will carry out their duties to the best of their abilities.

6. The number of CA private key "shares" (the parameter "n") MUST be such that adequate contingency is provided in the event of a share card being lost or damaged. The parameters "k" and

[2] A threshold scheme (also known as a "secret sharing scheme") is a mechanism that allows a "secret" to be broken into "shares", so that the secret can be recovered provided a defined number of shares are available, yet no information about the secret can be obtained if fewer than the required number of shares are presented. Threshold schemes provide a flexible management solution for sensitive data, whilst at the same time providing an automatic back-up facility. In the case of the Remote HSM Manager solution, the "secret" is the CA private key. A "(k, n)-threshold scheme" means that the secret is broken into n shares and that the secret can be recovered provided k (different) shares are presented.

"n" SHOULD satisfy $2k \leq n$ and there may be operational benefit in requiring that k divides n, thus allowing "teams" of shareholders to be established.

7. When creating the CA, the CA parameters that provide the highest level of security SHOULD be used.
   Remark: Where a choice exists, the default selection provides the highest level security.

8. Shareholders MUST NOT have access to more than one CA private key share.

9. All shareholder smart cards MUST be protected by strong PINs. For example:
   - PINs MUST be at least 8 digits in length;
   - "random" PINs SHOULD be chosen;
   - "obvious" PINs MUST NOT be chosen (e.g. "12345678" or "99999999");
   - shareholders MUST NOT choose PINs that may be easily guessed by somebody else (e.g. date of birth, telephone number, etc).

10. Shareholders MUST NOT divulge their smart card PINs to any other party.

11. Shareholders SHOULD change their PINs on a regular basis.

12. New shareholders who take ownership of an existing shareholder card MUST change the shareholder card's PIN as soon as is practical.

13. All shareholder cards MUST be clearly labelled; as a minimum, the label MUST identify the card as a shareholder card and the share number.

14. All shareholder cards MUST be stored securely when not in use.

15. Shareholder card PINs MUST be written down and stored securely, separate from the cards, and separate from other shareholder card PINs.

16. The Security Manager MUST log all access to shareholder cards and PINs.

17. The Security Manager MUST know the location of all shareholder cards and the corresponding PINs but MUST NOT have access to any of these items (unless, of course, he or she is a shareholder).
    Remark: Once the CA private key shares are created there is no facility to create extra shares. Should a shareholder leave the organisation, the existing shares can continue to be used if this is deemed to be an acceptable risk. However, the new shareholder MUST change the shareholder card PIN as soon as is practical.

18. A person who ceases to hold the role of shareholder MUST have their access rights to the share card revoked immediately.

19. Shareholder cards MUST be tested regularly to ensure that they still function correctly.

20. A shareholder card that is no longer usable MUST be destroyed in a secure manner and a record of such destruction MUST be retained by the Security Manager.

21. Administrator and operator cards that are created via the "RR" console command MUST be distributed securely to the relevant Administrators and Operators and the recipients MUST acknowledge receipt of the cards.

22. The transport PIN for the administrator and operator smart cards SHOULD be distributed separately from the cards and, ideally, SHOULD NOT be sent until card receipt has been acknowledged.

23. The Security Manager MUST retain a record of all HSMs and administrator and operator cards that have been issued (i.e. a public/private key pair has been generated and the public key signed by the CA private key).

Recovery Master Key (RMK)

In the event that an HSM should tamper and lose its RSA keys (and the public keys of smart cards in the Security Group), it would be a major operational headache to re-initialise the HSM and generate a new RSA key pair. Hence, a supplementary (and entirely optional) mechanism has been devised to allow a relatively simple means of recovering the situation. This involves the use of a 3-DES *Recovery Master Key* (RMK).

The RMK is generated as three components, using the "RG" console command, and is loaded into each HSM using the "RL" console command. Each component is held on a smart card. If the HSM is tampered then it is necessary only to reload the RMK (using the "RL" command) to recover the situation.

Note that the recovery mechanism stores an encrypted copy of the HSM's unique private key in persistent storage within the HSM, and this is not erased if the HSM is tampered. It is therefore essential to ensure that the RMK components are kept separate to prevent compromise of the RMK, and (if internal HSM access is possible) compromise of the HSM's private key.

Further details of the RMK and its use are given in Chapter 4 of HSM 8000 Remote HSM Manager Installation Guide.

Note: The RMK can only be generated and loaded via the HSM's console interface. No Remote HSM Manager function exists to manage the RMK.

1. RMK-related activities SHOULD take place in a secure area.

2. The Security Manager MUST take overall responsibility for all RMK activities and MUST ensure that all RMK-related procedures are followed correctly.

3. The Security Manager MUST maintain a log of the names of the RMK component holders and the corresponding card and component number; the log SHOULD be stored securely.

4. RMK component holders MUST be fully briefed by the Security Manager with regard to their roles and responsibilities.

5. All RMK component holders SHOULD sign affidavits stating that they understand their roles and responsibilities with respect to their RMK components and that they will carry out their duties to the best of their abilities.

6. At least one back-up copy of each RMK component card MUST be created at the time the RMK is generated.

7. RMK component holders MUST NOT ever have access to more than one RMK component.

8. All RMK component smart cards MUST be protected by strong PINs. For example:
   - PINs MUST be at least 8 digits in length;
   - "random" PINs SHOULD be chosen;
   - "obvious" PINs MUST NOT be chosen (e.g. "12345678" or "99999999");
   - shareholders MUST NOT choose PINs that may be easily guessed by somebody else (e.g. date of birth, telephone number, etc).

9. RMK component holders MUST NOT divulge their smart card PINs to any other party.

10. RMK component holders SHOULD change their PINs on a regular basis.

11. All RMK component cards MUST be clearly labelled; as a minimum, the label MUST identify the card as an RMK component card and the component number.

12. All RMK component cards MUST be stored securely when not in use.

13. RMK component card PINs MUST be written down and stored securely, separate from the cards.

14. The Security Manager MUST log all access to RMK component cards and PINs.

15. The Security Manager MUST know the location of all RMK component cards and the corresponding PINs but MUST NOT have access to any of these items (unless, of course, he or she is an RMK component holder).

16. If an RMK component holder leaves the organisation, the Security Manager MUST arrange for a new RMK to be created and installed into the relevant HSMs, in order to replace the existing RMK.

17. A person who ceases to hold the role of RMK component holder MUST have their access rights to the component card revoked immediately, and the Security Manager MUST arrange for a new RMK to be created and installed into the relevant HSMs, in order to replace the existing RMK.

18. RMK component cards MUST be tested regularly to ensure that they still function correctly.

19. An RMK component card that is no longer usable MUST be destroyed in a secure manner and a record of such destruction MUST be retained by the Security Manager.

Administrator and Operator Smart Card Security

Remote HSM Manager Administrators and Operators each have a smart card, protected by a PIN. Initially the PIN is the transport PIN created when the card was issued to them. Users are forced to change the PIN before subsequent use of the card.

1. Administrator and operator smart cards MUST be stored securely when not in use.

2. Administrator and operator card PINs SHOULD be written down and stored securely, separate from the cards.

3. The Security Manager SHOULD NOT need to know the secure storage location of administrator and operator cards and the corresponding PINs and MUST NOT have access to any of these items (unless, of course, he or she is an Administrator or Operator).

   Remark: Unlike the situation with CA private key share cards, additional administrator and/or operator cards can be created in the event that an existing cardholder leaves the organisation or if a card becomes unusable.

4. A person who ceases to hold the role of Administrator or Operator MUST surrender their cards immediately, and have their access rights to both their card and to the relevant secure areas revoked immediately.

5. All administrator and operator cards MUST be clearly labelled; as a minimum, the label MUST identify the card as an administrator card (left or right) or an operator card.

6. Administrator and operator smart cards MUST be protected by strong PINs. For example:

   - PINs MUST be at least 8 digits in length;
   - "random" PINs SHOULD be chosen;
   - "obvious" PINs MUST NOT be chosen (e.g. "12345678" or "99999999");
   - shareholders MUST NOT choose PINs that may be easily guessed by somebody else (e.g. date of birth, telephone number, etc).

7. Administrators and Operators MUST NOT divulge their smart card PINs to any other party.

8. Administrators and Operators SHOULD change their PINs on a regular basis.

9. All access to administrator and operator cards and PINs SHOULD be recorded by the Security Manager.

10. Administrator and operator cards SHOULD be tested regularly to ensure that they still function correctly.

11. An administrator or operator card that is no longer usable MUST be destroyed in a secure manner and a record of such destruction MUST be retained by the Security Manager.

Operator Cards

Operators of the Remote HSM Manager carry out a range of sensitive functions, including key management activities and functions that require the HSM to be in Authorised State. Operator cards typically store Local Master Key (LMK) components and/or authorisation passwords. As such, the security of the operator cards is critical to the security of the Remote HSM Manager.

In addition to the general security guidelines relating to administrator and operator cards, the following guidelines apply specifically to operator cards:

1. LMK cards MUST be clearly labelled; as a minimum, the label MUST identify the LMK and the component number.

2. Authorising password cards SHOULD be created and used for day-to-day operations; LMK cards SHOULD NOT be used for day-to-day operations.

3. Authorising password cards MUST be clearly labelled; as a minimum, the label MUST indicate LMK identifier and password number.

Remark: LMK and authorising password cards are specific to a particular LMK and so when multiple LMKs are used, the labelling of the cards is crucial.

Security Group

The term "Security Group" describes a set of (administrator and operator) smart cards and a set of HSMs, such that (secure) remote communication between a card in the group and an HSM in the group is permitted. A necessary pre-requisite for a card and an HSM to be in the same Security Group is that both must possess an RSA key pair, with the public key signed by the same CA private key.

As cards are added to the Security Group, their details (including public key certificates) are loaded into the HSMs in the Security Group. Similarly, as HSMs are added to the Security Group, their details (serial numbers and IP addresses) are stored on the cards. If a card does not contain details of a particular HSM then communication between the two devices is not possible. The same applies if an HSM does not contain the public key certificate for a card.

Details of the initialisation and management of the Security Group can be found in Chapter 8 of HSM 8000 Remote HSM Manager Installation Guide and Chapter 7 of HSM 8000 Remote HSM Manager User's Guide.

1. The Security Manager MUST keep a record of all administrator and operator cards and HSMs that belong to a particular Security Group; the record MUST be updated as new devices are added to, or deleted from, the Security Group.

2. If an HSM's Security Group no longer exists, then to prevent confusion, the HSM's details SHOULD be deleted from all the cards in that Security Group as soon as possible.

3. Details of a lost or stolen card MUST be deleted from all the HSMs in the card's Security Groups as soon as possible.

Back-Up

All equipment, documentation and audit records relating to the Remote HSM Manager must be backed-up.

1. All LMK component smart cards and corresponding PINs MUST be backed-up and stored securely, separate from the primary cards; at least one back-up copy of each component SHOULD be stored off-site.

2. All RMK component smart cards and corresponding PINs MUST be backed-up and stored securely, separate from the primary cards; at least one back-up copy of each component SHOULD be stored off-site.

3. At least one set of CA private key share cards that can be used to re-generate the CA private key (i.e. "k" such cards) and the corresponding PINs SHOULD be stored securely off-site and at different locations.

4. All documentation and audit records relating to the Remote HSM Manager MUST be backed-up and at least one copy SHOULD be stored off-site.

5. Access control relating to all back-up equipment, documentation and audit records MUST be equivalent in strength to the controls surrounding the primary items.

Operational Security

Details of Remote HSM Manager operations are given in HSM 8000 Remote HSM Manager User's Guide. These should be complemented by an organisational security and operations document (see, for example, the earlier section on "Procedures"). The following guidelines should be used in conjunction with other guidelines in this document.

Remark: The "key" guidelines listed below do not attempt to define a key management policy (e.g. key generation, distribution, update, archive, destruction, etc). Such a policy should already exist within the organisation and so any of the particular guidelines below that relate to keys should be used to complement this policy.

1. Administrators and Operators MUST be fully aware of, and follow, security procedures relating to the operation of the Remote HSM Manager.

2. The Security Manager MUST ensure that all security procedures relating to the operation of the Remote HSM Manager are followed correctly.

3. Users MUST take their smart cards with them if they exit the Operations Room.

4. Users MUST ensure that nobody else can observe the entry of a PIN at a smart card reader.

5. HSMs MUST NOT be placed in the off-line state or in secure mode for any longer than is absolutely necessary to complete the required activity.

6. Users MUST NOT be logged into HSMs at the "Security Officer" level for any longer than is absolutely necessary.

7. A time-out for user sessions SHOULD be specified.

8. HSMs MUST NOT be placed in Authorised State for any longer than is absolutely necessary to complete the required activity.

9. A time-out for Authorised State SHOULD be specified.

10. If Multiple Authorised Activities has been configured for the HSMs (see, for example, the earlier section on "HSM Security Configuration"), then activities that are not being used MUST NOT be authorised.

11. LMKs (in particular, "old LMKs") MUST be deleted from the HSM when no longer required.

12. Key block header values MUST be chosen with care.

13. Key block header values SHOULD be chosen to be as restrictive as possible for the particular key type and key usage; special attention SHOULD be given to:

    - key usage;
    - mode of use;
    - exportability.

    Remark: Some changes to key block header values are permitted (via a host command), but only to restrict key usage further. For example, a key initially designated as a "MAC generate and verify" key can later have its header changed to make it a "MAC generate only" key, but the reverse change is not permitted. Similarly, if a key is designated as "non-exportable" then it cannot later be changed to "exportable".

14. A plaintext key component displayed on the PC/laptop screen MUST NOT be viewed by anybody other then the operator who generated the component.

15. Plaintext key components SHOULD NOT be saved to file, except for the purpose of printing the components, after which the file MUST be deleted.

16. The "half" or "third" method of forming a key from components SHOULD NOT be used.

17. All error conditions and other "incidents" relating to any aspect of Remote HSM Manager operations MUST be recorded in a paper-based incident log (see also the earlier section on "Audit"), and passed to an incident management process for further investigation

18. The network communications link between the Operations Room and the secure area housing the physical HSM MUST be regularly inspected and tested to ensure that it provides sufficient protection against intrusion and unauthorised access.