THALES

cpl.thalesgroup.com

payShield 9000 v3.5

Security Operations Manual

1270A545-038

26 July 2021

Contents

End User License Agreement

Use of this product is subject to the Thales Cloud Protection & Licensing *End User License Agreement* found at:

https://cpl.thalesgroup.com/legal

Revision Status

Document No.	Manual Set	Software Version	Release Date
1270A545-038	Issue 38	payShield 9000 v3.5	July 2120

Chapter 1 – Introduction

General

The payShield 9000 hardware security module (HSM) provides cryptographic functions to support network and point-to-point data security, therefore it is imperative that the HSM itself is secure. The payShield 9000 is made physically secure by locks, electronic switches and tamper-detection circuits, and must be located in a secure area with controlled access.

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

- Two front-panel locks with separate keys.
- Personalized smartcards issued to several Security Officers.
- Personal Identification Numbers (PINs) issued to Security Officers.
- A Secure mode which requires the presence of two operators holding separate physical keys to the front panel locks. (An equivalent card-controlled mode can be achieved via payShield Manager.)
- An Authorized mode, requiring the presence of two Authorizing 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 payShield Manager.

About this Manual

This manual includes instructions for the security operations which must be performed on the HSM console or via the equivalent facilities of payShield Manager. For other information, see the following manuals:

- payShield 9000 Console Reference Manual
- payShield 9000 Installation Manual
- payShield 9000 Host Programmer's Manual
- payShield 9000 Host Command Reference Manual
- payShield Manager User's Guide

This manual also includes appendices containing guidance for the development of policies and systems employing HSMs and payShield Manager.

Chapter 2 – Configuration

General

This chapter describes the security and alarm configuration of the payShield 9000 HSM using the Console interface. (Users of payShield Manager should refer to the payShield Manager manuals to perform the equivalent configuration functions.)

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 motion alarm circuitry should be turned on when the HSM is put into service. The motion alarm will need to be turned off if the HSM is to be moved. The **CL** console command allows the user to view and modify the current alarm settings (Users of PayShield Manager should use the ***General Settings*** section of the ***Configuration*** tab to perform the equivalent configuration functions.)

The HSM must be in the Secure state to configure the motion alarm.

Note that from payShield 9000 v2.2 software onwards, the temperature alarm is permanently enabled.

Configure the Self-Tests

Self tests are run during the HSM boot-up. Diagnostic tests can be run upon user request via the **DT** console command.

PCI HSM requires the HSM self tests are run automatically at least once every 24 hours. By default the HSM will run the self tests at 09:00 daily. The **ST** console command allows the user to view and modify the current self test settings. (Users of PayShield Manager should use the ***Health Statistics/Diagnostics*** section of the ***Status*** tab to perform the equivalent configuration functions.)

The HSM must be in the Offline or Secure state to configure the self tests.

Should any of the self tests fail an error log message shall be created as per the following example.

Example:

```
1: May 06 13:55:00  ERROR: [Power Supply:    FAILED (PSU 2 Failed) ]
(Severity: 3, Code = 0x00000001, Sub-Code = 0x0000000E)
```

An audit log message will also be generated upon the failure of a self test as shown in the following example.

Example:

```
000008F1  13:55:00  06/May/2011  Diagnostic self test failure: Power
```

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 payShield 9000 Console Reference Manual for details of these commands. (Users of PayShield Manager should use the items from the ***Security Settings*** section of the ***Configuration*** tab to perform the equivalent configuration functions.)

The parameters that can be set are:

Parameter	Default value
PIN length: 4..12 *This value is used by the HSM to define the length of encrypted PINs, symbolized as "L" in the Host Command manuals in the "Length & Type" column. The value of L is one more than the value entered for the PIN length in the CS command. Cleartext PINs (as entered into the BA host command) must have a length of L: shorter PINs can be entered, but must be padded to the right with hexadecimal F digits.* *For example, if the PIN Length in CS has been set to 6 (i.e. L = 7), and the 4-digit PIN "1234" is to be entered into the BA host command, the value that is included in the command is "1234FFF".* *All LMK-encrypted PINs will have a length of L.* *Where a PIN is generated (e.g. JA host command) and the PIN length specified in the command is less than L, the generated PIN will be padded to the right with hexadecimal F characters to a length of L digits.* *When an LMK-encrypted PIN is decrypted using the NG host command, any F-padding used to expand a shorter PIN is presented in the decrypted PIN and will need to be stripped off to derive the shorter PIN.* *Note: Once the length is set, it cannot be easily altered. If it has to be changed to accommodate longer PINs, all the existing encrypted PINs will have to be translated. This requires two operations: the old PINs are first translated to encryption under, for example, a ZPK; the HSM is then re-configured for the longer PIN length; the PINs are then translated back from the ZPK to the LMK.* *The above information applies to the following host commands: BA, BC, BE, BG, BQ, CE, CQ, DE, DG, EE, G2, G4, GA, GU, JA, JC, JE, JG, NG, PE, PG, QC, QK, QW, XK, XM, ZM.*	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

Parameter	Default value
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 payShield 9000 supports three variants of transaction key schemes: Racal (i.e. Thales), 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.* *Notes:* *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.* *Use of this setting may modify the functionality associated with some Host commands. See Chapter 13 of the payShield 9000 General information Manual for further information.*	None
User storage key length: Single, Double, Triple or Variable *This is the length of the keys stored in user storage; it can be 'Single', 'Double', 'Triple' or 'Variable' length. The number of keys that can be stored depends upon this setting.*	Single
Display general information on payShield Manager landing page: Yes or No *When set to 'Yes', the landing (initial) page displayed by payShield Manager will contain basic information about the HSM.*	No
Default LMK identifier: 0..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. The upper limit (99) is determined by the number of LMKs that can be installed concurrently.*	0
Management LMK identifier: 0..99 *Identifies the Management LMK, which will be used for authorizing certain management functions (e.g. setting the HSM's date/time), and for encrypting the audit MAC key. The upper limit (99) is determined by the number of LMKs that can be installed concurrently.*	0
CHANGING THE FOLLOWING PARAMETERS REQUIRES THE LMK(S) TO BE ERASED	
Enforce Atalla variant match to Thales key type: Yes or No *This parameter is only valid if 'Atalla ZMK variant support' is 'Yes'.* *If enabled, a defined match between Atalla variant and Thales variant key types will be enforced. Note that this parameter only is displayed in the 'QS' command if the "Atalla ZMK variant support" was previously set to 'ON'.*	No
Select clear PINs: Yes or No *This enables the clear PIN support via host commands 'NG' and 'BA'. Authorized 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. Authorized state is required for this command to process within a host application.* *Note: The availability of this command is a significant security risk.*	No
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, and is included for backward compatibility reasons only. 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

Parameter	Default value
Solicitation batch size: 1..1024 *A method supported by the payShield 9000 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. Small batch sizes must be avoided to prevent matching of reference numbers with account numbers.*	1024
Prevent single-DES keys masquerading as double or triple-length keys: 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
Single/Double length ZMKs: 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.*	Double
Decimalization table Encrypted/Plaintext: Encrypted or Plaintext *This option determines if the decimalization table will be encrypted or in plain text. The default setting is encrypted, however, to allow for backward compatibility plaintext decimalization tables can be selected. It is recommended that encrypted decimalization tables are used to protect against decimalization table manipulation attacks.*	Encrypted
Enable Decimalization Table Checks: Enabled or Disabled *The values in the decimalization 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.*	Enabled
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 decimal digits. Commands that use encrypted PINs describe them as 'LN or LH'.*	A (Visa method)
Use default card issuer password: Yes or No *This option determines whether the default Card Issuer Password is user or not.* *Note: this item should only be changed where customized HSM smartcards are being used. The original value must not be changed if standard Thales smartcards are in use.* *See the row below for details on setting a non-default card issuer password.*	Yes
Card issuer password (local): 8 characters *This parameter is only valid if 'Use default card issuer password' is 'No'.* *This option provides a method for users to set the password that the HSM sends to a smartcard prior to formatting the card. Most users will not need to change this value. If this setting is changed to a value that doesn't match the password on the smartcard, it will not be possible to format the smartcards using the 'FC' command. This setting is only relevant to standard HSM smartcards – not to payShield Manager smartcards.*	n/a
Authorized State required when importing a key under an RSA Key: Yes or No *This setting determines whether Authorized State is mandatory for the import of a key using RSA keys (host command GI). When set to Yes, the GI command always requires Authorized State (and the use of the signature field is optional). When set to 'No', the GI command does not require Authorized State.*	Yes
Minimum HMAC key length in bytes: 5..64 *This setting determines the minimum length of HMAC keys that the HSM can generate. HMAC keys must satisfy the equation L/2 <= key length, where L = 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

Parameter	Default value
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
Enable ZEK encryption of ASCII data or Binary data or None: ASCII or Binary or None *This setting determines the type of messages that can be encrypted/decrypted/translated (using a ZEK) using the 'Message Encryption' host commands M0, M2 and M4:* *ASCII: the plaintext message must contain only ASCII (0x20-0x7F) characters;* *Binary: no restrictions on the contents of the plaintext message;* *None: encryption using a ZEK is not permitted.*	None
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 authorized activities: Yes or No *If enabled, will allow precise selection of authorized activities (including timeout period if required). If disabled HSM reverts to global Authorized state.*	Yes
Allow persistent authorized activities: Yes or No *If enabled, will allow "persistent" authorized activities to be automatically restored when the HSM restarts following a power failure. This option is only presented if the response to the previous option is "Yes". Even where persistent authorized activities are allowed, there will be a maximum limit of 12 hours for the time that any Console command may remain authorized.*	Yes
Enable support for 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 new PIN is not considered weak. The precise method used to determine a PIN's strength is selected in one of the three settings, below.*	No
Check new PINs using global list of weak PINs: Yes or No *Note: This setting is only available if "Enable weak PIN checking" = "Yes".* *If enabled, the HSM's PIN generation/derivation host commands will check to ensure that the new PIN does not match one of the entries in the appropriate global 'Excluded PIN Table' (loaded into the HSM via the 'BM' host command). If a match is found in the list, then the command fails, returning error code 86.* *If disabled, the HSM will not perform any weak PIN checking using the 'global' list of weak PINs.*	No
Check new PINs using local list of weak PINs: Yes or No *Note: This setting is only available if "Enable weak PIN checking" = "Yes".* *If enabled, the HSM's PIN generation/derivation host commands will check to ensure that the new PIN does not match one of the entries in the 'Excluded PIN Table' (supplied with the host command). If a match is found in the list, then the command fails, returning error code 86.* *If disabled, the HSM will not perform any weak PIN checking using the 'local' list of weak PINs.*	No
Check new PINs using rules: Yes or No *Note: This setting is only available if "Enable weak PIN checking" = "Yes".* *If enabled, the HSM's PIN generation/derivation host commands will check to ensure that the new PIN is not considered weak using the rules defined below.* *A PIN is considered weak if any of the following are TRUE:* • *>50% of the PIN's digits have the same value. (e.g. 1111, 0111, 1101, etc. are all weak);* • *The PIN consists entirely of ascending or descending digits (e.g. 1234, 2345, etc. are all weak).*	No

Parameter	Default value
Enable PIN Block Format 34 as output format for PIN translations to ZPK: Yes or No *If enabled, the HSM will permit translations from Thales PIN block formats 2, 3 & 5 to Thales PIN block format 34 in the CA, CC & G0 PIN translation commands.*	No
Enable translation of account number for LMK encrypted PINs: Yes or No *If enabled, allows the account number (PAN) for an LMK-encrypted PIN to be changed without the customer PIN itself being changed, using the QK host command.*	No
Enable 2DES LMK encryption of 3DES/2048-bit RSA keys: Yes or No *If enabled, allows the encryption of triple-length DES keys and >1024 bit RSA keys using a double-length Variant LMK.*	Yes
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 key blocks (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 key block 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 key block format. In this case, any export/import process using keys in variant format (including X9.17 format) will be prohibited.*	Yes
Protect MULTOS Cipher Data Checksums: Yes or No *This setting is used to control whether checksums generated over sensitive data will require encryption. {Only relevant if optional license HSM9-LIC023 is installed.)*	Yes
Enable Key Scheme Tag 'X' (X9.17) for storing keys under LMK: Yes or No *If enabled, keys encrypted under a Variant LMK will be permitted to use the key scheme tag 'X'. This is a lower security option, and is included for backward compatibility reasons only.* *If enabled, the following host commands will support LMK-encrypted keys using key scheme 'X': B0, EA, FA, IA, CK, G0, EC, CI, CM, GQ, CC, GO, M0, M2, A0, and A6.*	No
Enable use of Tokens in PIN Translation: Yes or No *This option determines whether PIN Translation commands will support the use of Tokens, in the Account Number field for Source PIN Blocks, by providing a second Account Number field for the Destination PIN Block.* *If enabled, allows the account number (PAN) for a ZMK-encrypted PIN to be changed without the customer PIN itself being changed, using the CC host command.*	No
Enable use of Tokens in PIN Verification: Yes or No *This option determines whether PIN Verification commands will support the use of different Account Numbers/Tokens, for the PIN Block and reference value generation process.*	No
Allow Error light to be extinguished when viewing Error Log: Yes or No *When set to No, the error light will remain lit (not flashing) when the error log has been read. When set to Yes, the error light will be extinguished once the user has confirmed that the error log has been read.*	No
Ensure LMK Identifier in command corresponds with host port: Yes or No *When using multiple Variant LMKs, there are two ways to specify which LMK a host command should use: by using a specific TCP port, or by specifying the LMK Id within the command. Conflicts may arise if both methods are used at once. When this option is set to 'No', an LMK Id field within a host command has priority over the TCP port used; when set to 'Yes', an LMK Id field within a host command must match the LMK Id implied by the TCP port used.*	No
Ignore LMK ID in Key Block Header: Yes or No *When set to 'Yes', the LMK ID inside the header (bytes 14-15) of Thales Key Blocks will be ignored. Instead, the HSM will use the same mechanisms for deducing the LMK ID as used with Variant LMKs: i.e. by host port, or by specifying the LMK ID within the command.* *When set to 'No', the LMK ID inside the header of Thales Key Blocks will be used to identify which LMK to use with a command.*	No

Parameter	Default value
Enforce NIST recommendations when encrypting AES keys using RSA: Yes or No *When set to 'Yes', the HSM will not permit a lower strength RSA key to encrypt a higher strength AES key – using the NIST SP800-57 recommended definitions of relative key strength.*	Yes
Enable import and export of RSA Private keys: Yes or No *If enabled, host commands 'L6' and 'L8' will be available (if the appropriate license is installed), permitting the import and export of RSA private keys. Otherwise, host commands 'L6' and 'L8' will be disabled, and immediately return error code '03'.*	No
Enable import of a ZMK: Yes or No *If enabled, console command 'IK' and host commands 'A6' and 'GI' will be able to import a ZMK by translating it from encryption under a (supplied) ZMK, to encryption under the LMK.*	No
Enable export of a ZMK: Yes or No *If enabled, console command 'KE' and host commands 'A8' and 'GK' will be able to export a ZMK by translating it from encryption under the LMK, to encryption under a (supplied) ZMK.*	No
THE FOLLOWING PARAMETERS AFFECT PCI HSM COMPLIANCE	
Enable single-DES: Yes or No *If enabled, it permits the use of single-length DES keys. This is a lower security option, and is included for backward compatibility reasons only.*	No
To operate in PCI HSM compliant mode, the HSM software must be PCI HSM certified and this option must be set to 'No'.	
If this option is set to 'No' and all other PCI HSM-relevant settings have PCI HSM compliant values then it will not be possible to change any of these options without performing a factory reset and reloading the LMKs.	

Parameter	Default value
Card/password authorization: Card or Password *This option selects the method of authenticating security officers requesting a security state change. The Authorized state is a mode that the HSM can be placed in for sensitive data processing. This authorized mode is required when input commands at the console or host use clear text data such as key components or unencrypted PINs. Authorized mode can be used in both Online and Offline host states and requires the Authorizing Officers to invoke the higher security level. Before the Authorized state can be set the Authorizing 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. (Only relevant to standard HSM smartcards – not to PayShield Manager smartcards.)* *To operate in PCI HSM compliant mode, the HSM software must be PCI HSM certified and this option must be set to 'Card'.* *If this option is set to 'Card' and all other PCI HSM-relevant settings have PCI HSM compliant values then it will not be possible to change any of these options without performing a factory reset and reloading the LMKs.*	Card
Restrict PIN block usage for PCI HSM compliance: Yes or No *If enabled, the HSM will prevent translations from ISO PIN block formats 0, 1, 3 and 4 (Thales PIN block formats 01, 05, 47 and 48 respectively) to any non-ISO format. The HSM will also prevent translation of PIN block formats that include the PAN to PIN block formats that do not include the PAN. Translations between PIN block formats that both include the PAN shall not allow a change in the PAN.* *The HSM will also restrict the calculation of values derived from the PIN and PAN such as PIN offsets and PIN Verification Values to ISO PIN block formats 0, 3 and 4 only (Thales PIN block formats 01, 47 and 48).* *Refer to Chapter 10 of the General Information Manual for the allowed PIN Block translations within the HSM.* *To operate in PCI HSM compliant mode, the HSM software must be PCI HSM certified and this option must be set to 'Yes'.* *If this option is set to 'Yes' and all other PCI HSM-relevant settings have PCI HSM compliant values then it will not be possible to change any of these options without performing a factory reset and reloading the LMKs.*	No
Enforce key type 002 separation for PCI HSM compliance: Yes or No *If enabled, the HSM will separate the keys currently encrypted under LMK 14-15 (key type 002).* *Refer to Chapter 10 of the General Information Manual for a list of the key type changes this will implement. The complete Key Type Tables for each setting of this parameter can be found in Chapter 4 of the General Information Manual.* *If this option is enabled the following Host commands are disabled: AA, AE, FC, FE, FG, HC, KA, OE.* *To operate in PCI HSM compliant mode, the HSM software must be PCI HSM certified and this option must be set to 'Yes'.* *If this option is set to 'Yes' and all other PCI HSM-relevant settings have PCI HSM compliant values then it will not be possible to change any of these options without performing a factory reset and reloading the LMKs.*	No

Parameter	Default value
Enforce Authorization Time Limit: Yes or No *If enabled, the maximum authorization time limit for console commands is set to 720 minutes.* *If disabled, the maximum authorization time limit for console commands is unlimited.* *To operate in PCI HSM compliant mode, the HSM software must be PCI HSM certified and this option must be set to 'Yes'.* *If this option is enabled and all other PCI HSM-relevant settings have PCI HSM compliant values then it will not be possible to change any of these options without performing a factory reset and reloading the LMKs.*	Yes
Enforce Multiple Key Components: Yes or No *If enabled, all LMK and keys formed in the HSM must be formed from at least 2 different components.* *To operate in PCI HSM compliant mode, the HSM software must be PCI HSM certified and this option must be set to 'Yes'.* *If this option is set to 'Yes' and all other PCI HSM-relevant settings have PCI HSM compliant values then it will not be possible to change any of these options without performing a factory reset and reloading the LMKs.*	No

Chapter 3 – Local Master Keys (LMKs)

LMK Overview

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 previous versions of Thales (Racal) HSM firmware.

Note: The term "Variant LMK" refers to the fact that variants are applied to the LMK prior to using the LMK; a Variant LMK is not itself a variant of any other key.

A **Keyblock LMK** is either a triple-length DES key, or a 256-bit AES key, and is used to encrypt keys in a keyblock format. A Keyblock LMK is not compatible with a Variant LMK, and it can only be used to encrypt keys in the keyblock format.

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

LMK Management

At least two copies should be made, one for storage onsite and one for 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 of the same card made for resilience against card failure can be kept together.

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

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.

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

Generate an LMK Component Set

(Users of payShield Manager should refer to the payShield Manager manuals to perform the equivalent configuration functions.)

The following are required (Users of payShield Manager have different requirements e.g. the metal keys are replaced by a card-based authentication scheme.):

- The two (or more) Component Holders (two Authorizing Officers), who are to generate the two (or more) sets of components. (Two Authorizing Officers must be present whenever the HSM is to be set into the Authorize Activity state.)
- The HSM Console terminal (or payShield Manager).

- Access to a single HSM.
- At least 4 formatted blank smartcards (up to 12 can be used). 4 cards provide two copies of two sets of components, 8 cards provide four copies of two 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 Authorizing Officers (i.e., not automatically created by the HSM and stored electronically), each must be also be recorded by the Authorizing Officer who enters the password and who will also be responsible for keeping that password a secret.
- The two metal keys for the HSM's locks.

Note that during the process of creating each Variant or triple-length DES keyblock LMK Component, its seed values (A, B, C, D) are either entered manually or randomly generated in secret by the HSM (which is the recommended approach). If the seed values are entered manually, they must be unique values for each component card and written down for storage, as it is possible to subsequently re-create that LMK Component even if its smartcards are not available. Therefore the recorded values must be MORE SECURELY STORED than the Smartcards.

Keyblock header values MUST be chosen with care. They SHOULD also 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 keyblock 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".

Password Mode

The HSM may be configured for Password Mode authorization using the CS (Configure Security) Console command.

This mode is provided for backward compatibility.

Note: AES keyblock LMKs do not support Password Mode.

The process is similar to generating Component Set 1 & 2, except there is an extra step 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 a 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:

- The HSM Console or payShield Manager.
- Access to the HSM – unless payShield Manager is being used.
- One smartcard from each of the required Component Sets.
- The Component Holders responsible for smartcard custody (no one person should have access to more than one Component Set).

Verifying the Contents of the LMK Store

The LMKs installed in the HSM should be checked periodically. Using the V Console command, confirm that the check value is identical to the value that was recorded when the LMK set was installed. (Users of payShield Manager will always see the HSM's LMK details once connected to it.)

```
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 Component Set smartcards should be individually checked periodically – to confirm that they work correctly with an HSM and produce the same check values.

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 three test LMK cards – one containing a Test Variant LMK, another containing a Test triple-length DES keyblock LMK and another containing a Test AES keyblock LMK. To load a test LMK, use the LK command, with the appropriate smartcard in the reader in the normal way.

Chapter 4 – Operating Instructions

General

(Users of payShield Manager should refer to the payShield Manager manuals to perform the equivalent functions.)

The payShield 9000 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.

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 (Ctrl-C). The HSM responds with:

```
TERMINATED
```

Viewing HSM Status Information

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

- 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 payShield 9000 Console Reference Manual for details of these commands.

Users of payShield Manager should refer to the payShield Manager manuals to perform the equivalent functions.

Secure Mode

Secure mode is required for certain secure Console commands which affect the security status of the HSM. These include GK, LK, LO, LN, DC, CL, CS, SS, RS, CLEARERR, CLEARAUDIT, AUDITOPTIONS and SETTIME. The HSM is put into the Secure mode by operating both of the key locks on the front panel or by presenting authorized smartcards to the payShield Manager.

Users of payShield Manager should refer to the payShield Manager manuals to perform the equivalent functions.

Authorize Activity State

The Authorize Activity state allows precise specification of authorized activities (including configurable timeout period).

Users of payShield Manager should refer to the payShield Manager manuals to perform the equivalent functions.

Note: Console authorizations will be limited to (and default to) 12 hours. This is designed to coincide with an employee's shift pattern. Host authorizations will continue to allow (and default to) being indefinitely authorized.

Note: Whenever a PIN entry is requested by the HSM or payShield Manager in order to authenticate a user, the PIN entry process must be completed within 60 Seconds otherwise the process which requested the PIN entry will be automatically terminated. Note that this does not require the correct PIN to be entered within 60 seconds: if an incorrect PIN is entered and the software offers another opportunity to enter the PIN, the timeout timer re-starts from zero.

The C (Cancel) command is used to cancel one or more Authorize activities. Power cycling the HSM, or resetting the HSM (performed by pressing the RESET button on the front panel) cancels all non-persistent Authorized activities.

Smartcards

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

- FC : Format a smartcard.
- CO : Create an Authorizing 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 payShield 9000 Console Reference Manual for details of these commands.

The payShield Manager manuals describe the equivalent menu items for performing these functions.

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.

See the payShield 9000 Console Reference Manual for details of the logging commands.

The Error Log

The Error log stores fault information for use by Thales e-Security support personnel. It contains a circular buffer to store internally generated error messages. 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-initializing 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

As of v1.4a the Audit Log contains 50000 (previously 2000) entries for audit records. Whenever an auditable event occurs, the Audit log is updated with the action and the time and date, and the serial number(s) of any smartcards involved. The Audit Log can also be configured to record execution of almost any console or host command.

Use of smartcards to authenticate users and successful execution of a number of sensitive actions that involve key or component entry are always recorded in the Audit Log to provide traceability to the smartcard that authorized their execution.

Example:

```
000008ED  13:42:43  06/May/2011  Activity admin..console:720 was authorized for LMK id 0
000008EF  13:45:05  06/May/2011  Authorized activity admin..console:720 was cancelled
000008F0  13:45:07  06/May/2011  Authorized activity admin..host was cancelled for LMK id 0
000007DD  15:08:48  19/Apr/2011  Smartcard activated: 20025132
000007F6  15:14:02  19/Apr/2011  Key I/O command BK executed.
000008F1  13:55:00  06/May/2011  Diagnostic self test failure: Power
```

The Audit Log records auditable events until it is 100% full and for each subsequent audit event 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-Authorized state in order to execute the

'AUDITOPTIONS' and 'CLEARAUDIT' Console commands. Users of payShield Manager should refer to the payShield Manager manuals to perform the equivalent functions.

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

Archiving of the Audit Log should be managed in a way, and with a timeliness, that ensures that no audit record is unintentionally omitted from the archive e.g. by erasure or by virtue of the Audit Log becoming full.

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.

Users of payShield Manager should refer to the payShield Manager manuals to perform the equivalent functions.

Appendix A – Security Recommendations

Introduction

This appendix to the payShield 9000 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 organizations and authorities relevant to the specific application and environment in which a 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 behavior 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 a 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 utilized appropriately. Careful consideration needs to be given to the tasks for which individual HSMs are configured and used to ensure that contradictory security requirements are avoided.

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 overall management and configuration of HSMs to define the acceptable configuration settings and enabled commands for each device – mainly to ensure that the risk-exposure of cryptographic keys and secret data is always within acceptable limits.

Remark: Particular care must be taken when an HSM is required to have multiple or changing roles within a system, or for compatibility with legacy systems, or system elements that are not capable of supporting the full range of security features – such as longer cryptographic keys or stronger PIN block formats.

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

3. 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.

4. Procedures regarding the security and operation of the system MUST be regularly reviewed and updated when necessary.

5. 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.

6. 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.

7. 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. A management process MUST be in place to define the scope and on-going management of audit records i.e. to define the nature of all auditable events, to define the form or method for capturing audit information (including their storage and transfer arrangements), the system for reviewing and reconciling audit records, plus their backup and retention periods.

2. Audits MUST NOT themselves necessitate the recording of any sensitive information, (e.g. key material).

3. Whenever a maintenance function or authorized function is used, this fact MUST be recorded, with details of the function used, and the reason for its use.

4. Whenever the product is put into a new operating state this MUST be recorded.

5. It MUST always be possible to determine the current operating state of the HSM by viewing the records.

6. Every movement of a HSM from one location to another MUST be recorded, together with reason for movement.

7. Every access to the HSM Secure Area or PIN printing areas MUST be recorded, including details of damaged and destroyed PIN mailer material.

Remark: Particular care must be taken when using the HSM in a PIN issuing operation so that the physical security of the printer and its cable connections is given equivalent consideration to that of the HSM.

1. Every access to an authorizing smartcard, LMK or HSM settings smartcard MUST be recorded and include the name of every officer involved and the reason for access.

2. 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.

3. Every access to metal keys MUST be recorded and include the name of every officer involved.

4. The records MUST be regularly reviewed to aid discovery of any hostile action that may have occurred.

5. Incident management procedures MUST exist to react to and counter hostile actions however discovered.

6. The records SHOULD be easy to understand and organized in such a way as to make analysis both straightforward and useful.

7. Records SHOULD be regularly backed up and copies stored off-site in such a way that they can be easily restored if necessary.

8. All record entries MUST include a time and date.

9. 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.

10. Sufficient resource MUST be available to allow complete records to be created.

11. The records MUST be protected against unauthorized modification.

12. 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.

13. 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 in support of a legitimate activity.

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 a HSM.

1. The persistent state (i.e. Online, Offline, Secure and/or Authorized) 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 utilized in addition to their role in the transition to other operating states.

3. If an individual is no longer an Authorizing Officer, procedures MUST be put in place to prevent him from acting subsequently as an Authorizing 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.

Remark: The HSM is capable of uniquely identifying any smartcard whose format includes a serial number; and it is recommended that this feature be used to support the goal of managing authorized activities. The serial numbers of cards must therefore be recorded as they are issued to individuals.

Use of Authorized State

1. At least 2 separate Authorizing Officers MUST be required to put the HSM into Authorized state.

2. Before the HSM is put into the Authorized state, the identities and authority of both Authorizing Officers MUST be checked and logged, with audit entries signed by both Authorizing Officers.

3. Before either one or both Authorizing Officers leave the HSM Secure Area (even temporarily) or the payShield Manager application, the HSM MUST be taken out of Authorized state and the appropriate payShield Manager smartcard logged out.

4. HSMs MUST NOT be placed in Authorized state for any longer than is absolutely necessary to complete the required activity.

5. A time-out for Authorized state SHOULD be specified.

6. If Multiple Authorized 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 authorized.

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) or the payShield Manager application, the HSM MUST be switched out of Secure state and the appropriate payShield Manager smartcard logged out.

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) or the payShield Manager application, any key/smartcard under their control MUST be removed/logged out from the HSM and secured.

Use of the restricted role of the payShield Manager

1. The use of the payShield Manager in the restricted role requires an authorized smartcard allowed to communicate with the specific HSM.
2. If an individual is no longer authorized to work an HSM, procedures SHOULD be put in place to prevent him (or her) from accessing that HSM via the payShield Manager, e.g. by revoking their smartcards' authorization to communicate with that HSM.
3. Before any individual(s) leave the payShield Manager application, they MUST log their smartcard out of the application.

Command Security

There are a number of standard features provided by the payShield 9000 that can help "lock down" the HSM to perform only the functions that are required by the host application.

Users of payShield Manager should refer to the payShield Manager manuals to perform the equivalent functions.

1. Use `ConfigCmds` Console command to disable all unused host and Console commands.
2. Use `ConfigPB` Console command to disable all unused PIN block formats.
3. Use Multiple Authorized Activities instead of the global Authorized state, thus permitting specific authorized commands, rather than all authorized commands.
4. All Authorized Activities should be time limited to reduce the risk of abuse.

5. Use the auditing capabilities to record and detect unexpected commands or events:

   - All HSM commands that require the HSM to be in the Authorized 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 audit records extracted by the host, they should be validated by the HSM. This is achieved using the host command '`Q8`'.

Measures to Protect HSM Secure Area

The figure below shows a 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 USB-to-serial cable (supplied by Thales).

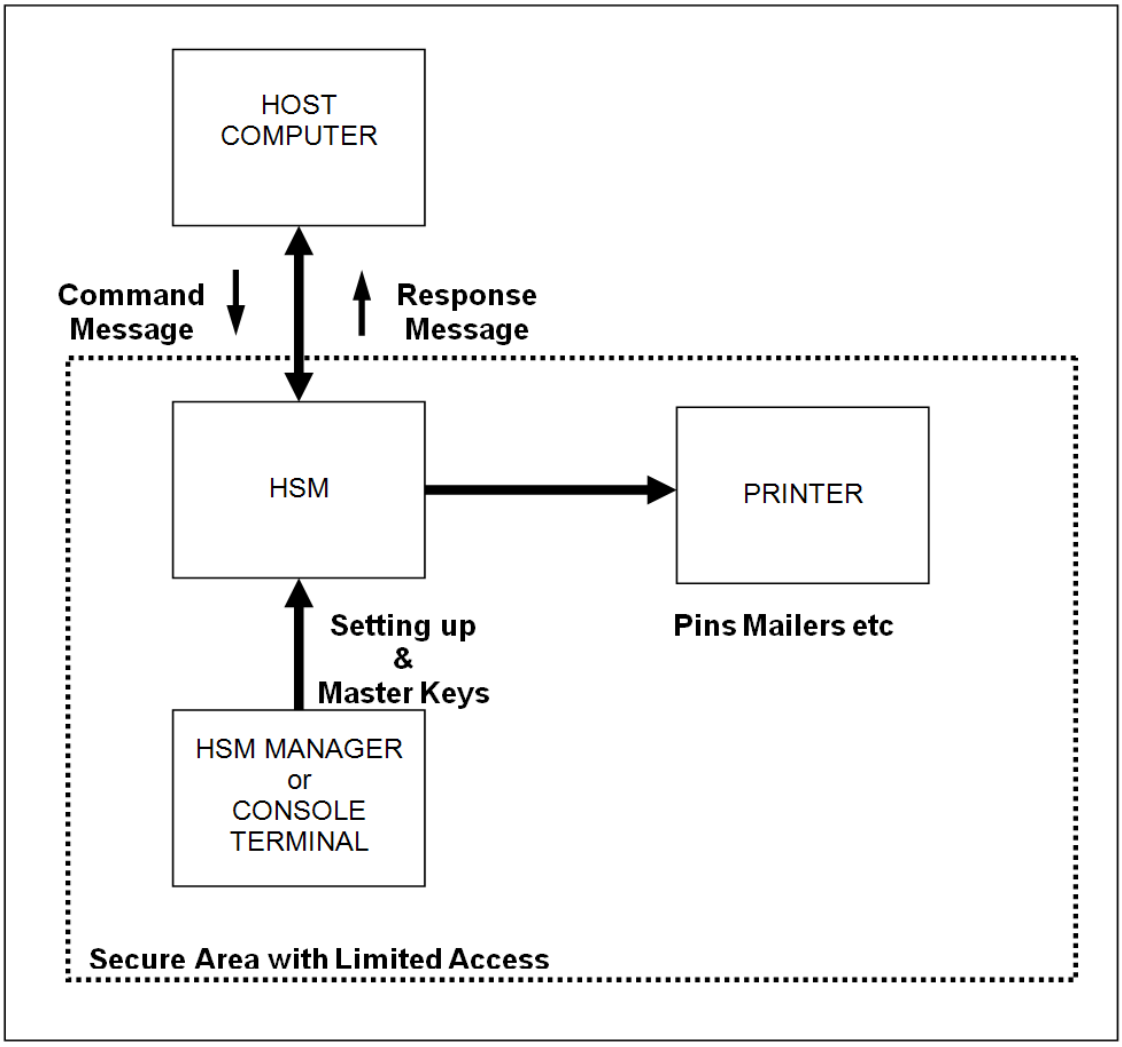

Figure A.1 - HSM in a Secure Area

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.

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

3. The HSM's Host and Management ports SHOULD be configured to communicate over separate subnets. This recommendation supports the electrical separation of networks by function i.e. operational, or managerial.

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

5. Access to the HSM Secure Area MUST be recorded.
6. The HSM Secure Area MUST NOT ever be occupied by a lone individual.
7. The HSM Secure Area MUST be subject to protection against electromagnetic emanation if this is deemed to be a threat.
8. The use of non-CRT monitors MUST be used to prevent the monitoring of electromagnetic emanation.
9. HSM peripherals (e.g. printer) MUST only be attached when required.
10. A HSM MUST be inspected, or subject to equivalent checks on its identity and integrity, when it enters or leaves the HSM Secure Area.
11. 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 a 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).

HSM Configuration Functions

1. Appropriate network protection mechanisms SHOULD be in place and the associated risks understood before enabling Dynamic Host Configuration Protocol (DHCP) on any of the HSM interfaces.

2. Access Control Lists SHOULD be configured, for each of the HSM interfaces. This will restrict the IP addresses that can access each of the HSM's interfaces.

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 payShield Manager Functions

Users of payShield Manager will need to refer to payShield Manager Installation Guide, payShield Manager User's Guide and Appendix B – payShield Manager Recommendations.

The payShield Manager can be run in local mode on a directly connected, secured computer and is an alternative to managing a HSM from a Console terminal.

Refer to the relevant User Manual for more details of the preferred Security Environment for the payShield 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 payShield Manager securely SHOULD be enhanced by minimizing the presence of unnecessary hardware and other software.

4. All hardware and software within the computer hosting the payShield 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 unauthorized 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 will 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 Set 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 unauthorized 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 a HSM system MUST be the responsibility of a trusted individual.
7. Key material SHOULD NOT be written down.
8. A plaintext key component displayed on the PC/laptop screen MUST NOT be viewed by anybody other than the user who generated the component.
9. Plaintext key components SHOULD NOT be saved to file, except for the purpose of printing the components, after which the file MUST be deleted.
10. 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.
11. 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.
12. Procedures MUST exist such that in the event of key material compromise, keys are replaced as necessary.

Remark: Where a key suspected of compromise is a key encipherment key, then all keys which are hierarchically under it shall be replaced.

1. The utilization of each key component MUST be controlled by separate Authorizing Officers.
2. Where keys or key components are stored on smartcards, the smartcards MUST be treated with an adequate degree of physical security to prevent unauthorized 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. PINs MUST be at least 8 digits in length.

4. 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
5. The frequency for changing passwords SHOULD be stated and be sufficient for the role.
6. Passwords SHOULD NOT be disclosed to others.
7. The process for managing forgotten passwords SHOULD be set out in the user's security management procedures.
8. If the PINs or passwords are written down, they MUST be stored securely and separately.
9. If a PIN or password is compromised (including a previously authorized individual becoming unauthorized), it MUST be invalidated and a replacement issued.
10. Everyone, and especially operators and Authorizing Officers, MUST have no unauthorized 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 Authorizing Officer credentials;
- storage of HSM alarm, security and host settings.

Security precautions for the cards are as follows:

- The user MUST define and implement suitable management procedures.
- All smartcards containing sensitive information MUST be stored securely.
- Smartcards containing sensitive information MUST be stored separately from each other.
- Access to any smartcard containing sensitive information MUST be recorded.
- Smartcards containing LMK Component Sets MUST only be made available to Authorizing Officers, and only when necessary.
- If a smartcard containing sensitive information is compromised (including a previously authorized individual becoming unauthorized), suitable measures MUST be taken to re-establish adequate security for the system e.g. by changing the LMK.
- 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.

- All smartcards containing sensitive information SHOULD be periodically checked to ensure that they are functional and have not been corrupted or compromised.
- There MUST NOT be any unauthorized access to smartcards containing sensitive information – especially by operators and Authorizing Officers.
- 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 payShield 9000 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 metal lock keys MUST be stored securely and separately.
3. Each metal lock key MUST only be made available when necessary.
4. If a previously authorized individual becomes unauthorized, measures MUST be taken to ensure that the individual no longer has access to the key.
5. Each use of the physical key on a HSM in operational use MUST be recorded.
6. There MUST NOT be any unauthorized access to a physical key – especially by operators and Authorizing Officers.

HSM Recovery Key (HRK)

In the event that an HSM erases its secure memory and loses its Secure Host Communications & Remote Management key material, it would be a major operational headache to re-initialize the HSM and generate new key material. Hence, a supplementary mechanism has been devised to allow a relatively simple means of recovering the situation. This involves the use of an AES-256 bit *HSM Recovery Key* (HRK).

The HSM will erase its secure memory upon a tamper event, the user pressing the erase button and a factory reset. Prior to restoring any key material to the HSM after an unexplained tamper event the Routine Inspection Procedure SHOULD be performed to ensure the HSM has not been maliciously tampered with.

Note: Key material protected under the HRK will not be recoverable after a factory reset.

The HRK is generated securely within each HSM using the SK Console command. The HRK is cryptographically protected using a separate key which is protected by two, user-generated passphrases. To restore the HRK both passphrases are required using the SL

Console command; this shall recover the Secure Host Communications and Remote Management trust anchors.

Note that the recovery mechanism stores encrypted copies of the Secure Host Communications and Remote Management key material in persistent storage within the HSM, and that this is not erased if the HSM erases its secure memory. It is therefore essential to ensure that the HRK passphrases are kept secret to prevent a compromise of the HRK and possible recovery of the Secure Host Communications and Remote Management key material.

Further details of the HRK and its use are given in Chapter 14 of the General Information manual.

Note: The HRK can only be generated and restored via the HSM's console interface. No payShield Manager function exists to restore the HRK.

1. HRK-related activities SHOULD take place in a secure area.
2. The Security Manager MUST take overall responsibility for all HRK activities and MUST ensure that all HRK-related procedures are followed correctly.
3. The Security Manager MUST maintain a log of the names of the HRK passphrase holders; the log SHOULD be stored securely.
4. HRK component holders MUST be fully briefed by the Security Manager with regard to their roles and responsibilities.
5. All HRK passphrase holders SHOULD sign affidavits stating that they understand their roles and responsibilities with respect to their HRK passphrases and that they will carry out their duties to the best of their abilities.
6. HRK passphrase holders MUST NOT ever have access to more than one HRK passphrase.
7. HRK passphrase holders MUST NOT divulge their passphrase to any other party.
8. HRK passphrase holders SHOULD change their passphrase on a regular basis.
9. The Security Manager SHOULD perform the Routine Inspection Procedure prior to restoring the HRK if the key material erasure was caused by an unexplained event (i.e. not the erase button or an explainable tamper event).
10. The Security Manager MUST log all usages of the HRK including name of the passphrase holders, the log SHOULD be stored securely.
11. A person who leaves the organisation or ceases to hold the role of HRK passphrase holder MUST have their access rights to the HRK revoked immediately, and the Security Manager MUST arrange for a new HRK passphrase holder to take on the vacant role (this MUST include changing the role's passphrase to a new passphrase), in order to replace the existing HRK.

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 (see Inspection Procedure below).
5. Anything, such as additional labels, that would alter the external appearance of the HSM SHOULD be discouraged.
6. If the HSM is PCI-HSM certified and was delivered to a location that is NOT the initial key loading facility; the HSM MUST be kept under auditable controls that can account for the location of the HSM at every point in time until the initial keys are loaded. This will ensure continued PCI-HSM compliance.
7. If the HSM is PCI-HSM certified and is being transferred between internal departments within the customer’s facilities; an audit record MUST be created to track the transfer of accountability for the HSM between those internal departments.
8. In normal usage, the HSM MUST periodically have a routine inspection for signs of tampering (see Inspection Procedure below).
9. Any HSM that appears to have been tampered with MUST NOT be loaded with keys or connected to the host application.
10. 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

The HSM is not suitable for user maintenance. The HSM has no user-maintainable parts. The HSM contains a long-life battery that can be replaced only by Thales at their premises.

1. HSM maintenance and repair MUST only be performed only by Thales; and if Thales found any evidence of tampering it would be preserved and reported appropriately.
2. Before a HSM is returned to Thales 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. Before a HSM is given to Thales for maintenance, the LMKs MUST be erased e.g. by using the RESET function.
6. Before a HSM is given to Thales for maintenance follow the relevant instructions in the payShield 9000 Decommissioning Guide (PPIF0552).
7. 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 audit log 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 may not be suitable for handling unusual risks and issues.

1. When an HSM is returned by Thales, it MUST be subject to the inspection procedures as described below.

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 deleted or replaced by the Test LMK.

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

2. 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.
3. When the HSM contains an LMK, the motion detector SHOULD be enabled.
4. When the HSM contains an LMK, the temperature sensor MUST be enabled.
5. Fraud detection SHOULD be enabled. The fraud detection parameters SHOULD be monitored to ensure that they are, and continue to be, appropriate for the HSM environment.
6. Host commands that are not required for operations MUST be disabled.

7. PIN block formats that are not required for operations SHOULD be disabled. In particular, PIN block formats that do not involve an account number MUST be disabled unless needed.

8. 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.

9. A faulty HSM MUST NOT be given an online connection to the host application.

10. The system design SHOULD include adequate contingencies for system failures, e.g. specific, isolated, localized, geographical or systemic.

11. Where the system design implies continuous availability of a HSM, in the event of failure of a HSM, a means of quickly switching operation to another HSM SHOULD be available at all times. (An automated load-balancing mechanism or Thales Security Resource Manager software may be useful for this purpose.)

12. At least two Authorizing Officers MUST control the initialization of a new HSM.

13. 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 a 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 Authorized 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.

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.

2. The inspection procedures MUST be performed by trusted personnel.

3. Details of the personnel performing the inspection procedures MUST be recorded.

4. 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 traveled outside of the HSM Secure Area.

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

- after any known unauthorized 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 unauthorized 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, delivery mechanism, 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 visible 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 formalizes 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 labels on the front and back of the HSM, MUST correspond correctly with the record created during the initial inspection.
2. Exceptionally, if the HSM is being inspected within the Secure Area, the operational mode of the HSM MUST be as expected. This MUST include verification of the HSM's operating state (Authorized state, Secure state or Online state) and examination of the "LMK" 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. When looking for evidence of tampering, consideration should be given to the possibility that the tamper-evident seals have been defeated or replaced with counterfeits. Such suspicions may be corroborated by errors or log entries indicating removal of the unit's lid. If the unit reports tampering of the internal cryptographic module this report should be taken seriously regardless of the apparent condition of the HSM external seals.

Remark: The inspection should check that no tamper-evident seals have been cut e.g. along the join between the covers they are intended to protect. Thales uses "voiding" seals, so the surface of the seal should be examined for the word "void" that appears repeatedly across its surface when the seal has been peeled back. Seals that have been peeled off may have lost some of their adhesion, and so may be loose or damaged. Counterfeited or defeated Seal may have been re-applied with adhesive whose traces could be observed at the edges of the seal.

1. The HSM's diagnostic test console DT command, as described in the 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
   ```

   Users of payShield Manager should refer to the payShield Manager manuals to perform the equivalent functions.

2. The HSM's self test console ST command, as described in the Console Reference Manual, MUST confirm that the self tests are running at the expected time.

   Users of payShield Manager should refer to the payShield Manager manuals to perform the equivalent functions.

3. The HSM VR Console command, as described in the Console Reference Manual, MUST confirm that the version number reported agrees with the record created during the initial inspection. If the HSM is required to be operating in a PCI HSM compliant manner the user MUST check that the Revision number is of the format `XXXX-19XX`, that the Revision number appears on the certificate on the PCI website, and that the following phrase is present:

   ```
   PCI HSM Compliance: Refer to the PCI web site
   (https://www.pcisecuritystandards.org/approved_companies_providers/app
   roved_pin_transaction_security.php) for current certification status
   of this version of payShield 9000 software.


   Security settings are consistent with the requirements of PCI HSM.
   ```

   Users of payShield Manager should refer to the payShield Manager manuals to perform the equivalent functions.

4. Exceptionally, if the HSM is being inspected within the Secure Area, 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.

5. The HSM MUST have no unrecorded physical changes or damage.

   Remark: Potential attacks against an HSM can include subtle attempts to create small holes through which bugs or temporary probes may have been passed. Therefore some consideration must be given to the condition of removable fixings such as screws and brackets, in case these have been used as the point of entry. Particular consideration should be given to scratches and marks that may have been caused during unauthorized activities, and therefore cannot be traced in the records of legitimate activities and inspections. There must be no opaque labels on the HSM that could obscure holes or other damage to the casing.

6. Any HSM whose authenticity and integrity cannot be adequately established MUST become subject to the incident management process.

Appendix B – payShield Manager Recommendations

Background

The Thales e-Security payShield Manager is a web-based product that allows communication with, and management of, a payShield 9000 unit over a wide area network. As such, it permits "remote" users to perform almost all console activity (see payShield 9000 Console Reference Manual) without requiring physical access to the HSM.

In order to provide secure communications between a remote user and a HSM:

- All management traffic is protected by a TLS v1.2 server-only authenticated session.
- All critical security parameters are further protected by an end-to-end encrypted channel between the payShield 9000 and the currently authenticated remote management smartcards.

Remote Management States

The payShield Manager allows the same states that exist when managing the payShield locally: Online, Offline and Secure.

Remote Management Roles & Limitations

payShield Manager smartcards can operate in one or more of the following roles:

Role #	Role Name	Role Description
1	Customer Trust Authority (CTA) Card	Card is commissioned by the CTA and contains a component of the CTA which defines the customer security domain of HSMs and associated smartcards.
2	Restricted Remote Access Control Card (RACC)	Card is commissioned by the CTA and is allowed access via the payShield Manager to any HSM that has this card within its whitelist as a 'Guest'.
3a	Left Key RACC	Card is commissioned by the CTA and is allowed access via the payShield Manager to any HSM that has this card within its whitelist as a 'Left key'. Also enables the user to transition the HSM into the 'Offline' state. Can be used in conjunction with role 3b to transition the HSM to 'Secure' state.
3b	Right Key RACC	Card is commissioned by the CTA and is allowed access via the payShield Manager to any HSM that has this card within its whitelist as a 'Left key'. Also enables the user to transition the HSM into the 'Offline' state.

		Can be used in conjunction with role 3a to transition the HSM to 'Secure' state.
4a	Remote LMK (RLMK) Card	Card is commissioned by the CTA and contains a share of the LMK.
4b	Remote LMK (RLMK) 1st Authorizing Card	Card is commissioned by the CTA and may contain a share of the LMK. Can be used in conjunction with role 4c to authorize the HSM for the specific LMK.
4c	Remote LMK (RLMK) 2nd Authorizing Card	Card is commissioned by the CTA and may contain a share of the LMK. Can be used in conjunction with role 4b to authorize the HSM for the specific LMK.

Based on the following restrictions:

- A smartcard can only exist in one customer security domain;
- A smartcard cannot represent both the left and right key RACC (roles 3a and 3b) for the same HSM;
- A smartcard cannot contain more than one LMK share /RLMK role (roles 4a, 4b or 4c);
- A smartcard cannot contain more than one CTA share (role 1).

Comment on Terminology

Organizations using the payShield 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.

Customer Trust Authority

Every commissioned HSM or smartcard contains an ECDSA 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 a private key that is also created by the user on an HSM. This root private key is normally described as a *Customer Trust Authority* (CTA). The CTA is split across a number of CTA cards. The CTA is temporarily loaded into an HSM prior to signing the smartcard or HSM public key certificates. The corresponding CTA public key (used to verify the certificates) is stored in each smartcard and HSM.

The CTA functionality is standard in all payShield 9000s that support the payShield Manager. All user interaction with the CTA functionality is via either the HSM's console interface or the payShield Manager.

Customer Security Domain

The term "customer security domain" is used to describe the set of smartcards and HSMs, such that (secure) remote communication between the cards and the HSM in the group is permitted.

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

In addition to having matching CTAs, whitelists within each HSM define which smartcards can communicate with that HSM and what role they possess.

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 recovery mechanism involving an AES HSM Recovery Key (HRK) is available that simplifies the task of restoring a public/private key pair to the HSM's secure memory and re-establishing the previous security group following a tamper caused by some innocuous event.

Purpose of this Appendix

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

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

Assumptions

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

Terminology

In accordance with Appendix A – Security Recommendations, the terms "MUST", "MUST NOT", "SHOULD" and "SHOULD NOT" 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.

PayShield 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 organizations and authorities relevant to the specific application and environment in which the HSMs are being used.

Personnel

An individual responsible for the overall operation and security of the payShield 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 storage area (such as a safe) for the storage of payShield Manager:

   - Laptop
   - Card reader
   - Smart cards
   - Audit records
   - Other sensitive items as defined in remainder of this appendix.

   Other payShield Manager users MUST NOT have access to this area.

2. The Security Manager SHOULD NOT possess any other role within the system.

3. Users of the payShield Manager SHOULD NOT have more than one smartcard per customer security domain.

4. 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.

5. A user with a left key RACC MUST NOT be allowed to possess (even temporarily) a right key RACC, and vice versa.

6. Every payShield Manager user, including the Security Manager, SHOULD have a named deputy, with the same level of access and responsibility.

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

8. All users MUST be made fully aware of their responsibilities regarding the security of the payShield Manager.

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

10. Users who no longer need access to the payShield Manager (e.g. have left the organization, have been assigned to a new department or are on extended leave, etc) MUST be deleted immediately from the system (and all whitelists) and their smartcards MUST have all contents deleted, using the functionality of either the HSM console, the payShield Manager or by physically destroying the card.

Procedural Security

In addition to the procedural security recommendations in Appendix A, all processes and procedures relating to the security and operation of the payShield Manager MUST be fully documented.

Audit

In addition to the audit recommendations in Appendix A, records of all payShield Manager activity MUST be made; this MUST include:

- HSM management and user events;
- personnel;
- security incidents;
- details of all personalized smartcards and HSMs;
- access to the payShield Manager operations room (access logs and CCTV images);
- access to the safe in the operations room;
- access to various passphrases, smartcards and PINs (e.g. Key RACC smartcards, RLMK smartcards, CTA smartcards, HRK passphrases, etc);
- access to documents relating to the payShield Manager, including audit and error logs.

Physical Security

Many payShield Manager activities are extremely sensitive and need to be carried out in a secure environment. In particular, compromise of a computer from which remote management operations are carried out could lead an authorized user to unwittingly carry out malicious actions.

1. The browser extension MUST only be obtained from genuine Thales sources (i.e. the payShield 9000 itself through the management interface, the Thales website or the installation CD).

2. The obtained browser extension SHOULD be hashed (using SHA-256) and compared to the expected message digest as provided by the Thales website, documentation and/or Support team.

3. When commissioning a payShield 9000 for payShield Manager, to avoid a possible man-in-the-middle attack, the network connection between the payShield 9000 and the management client MUST be trusted;

- The recommended method of achieving this is to connect to the payShield 9000 locally.

NOTE: FAILURE TO SECURE THE INITIAL CONNECTION TO THE HSM COULD LEAD TO COMPROMISE OF THE ENTIRE CUSTOMER SECURITY DOMAIN.

4. Remote access to the payShield Manager interface MUST be performed from an Operations Room, which is a physically secure environment.
5. Access to the Operations Room MUST be controlled and personnel who do not need access MUST NOT be given access.
6. Users who previously had access to the Operations Room but no longer need access MUST be revoked on the access control system.
7. 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).
8. If the Operations Room is occupied, there SHOULD be a minimum of 2 personnel present.
9. The loss or theft of an Operations Room physical access token MUST be reported immediately to the Security Manager and the token revoked on the access control system; and the circumstances of the loss/theft MUST be investigated.
10. 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.
11. All access to the Operations Room MUST be logged; each record MUST contain, as a minimum, a date/time stamp and a user identifier.
12. Exit from the Operations Room SHOULD be recorded by the access control system.
13. All failed access to the Operations Room MUST be recorded in the access log.
14. Failed access attempts MUST be investigated.
15. The door to the Operations Room SHOULD be covered by a CCTV camera.
16. Authorized users of the Operations Room SHOULD NOT have access to the access logs or CCTV images.
17. Access logs and CCTV images MUST be retained for inspection for a period of time that is compatible with organizational policies, but SHOULD be at least 6 months.
18. The Operations Room SHOULD be alarmed outside "normal" operating hours.
19. CCTV MUST NOT be used inside the Operations Room, to avoid compromising user passwords.
20. All cabling inside the Operations Room SHOULD be clearly visible.

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

22. 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.

23. Access to the safe SHOULD require two people.

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

25. Smartcard readers SHOULD be stored in the safe when not in use.

26. The computing equipment used to access the payShield Manager SHOULD be stored in the safe when not in use.

27. If a desktop computer (PC) is used to run the payShield Manager then it SHOULD be locked to prevent access to the internal circuitry.

28. The computer MUST be kept up to date with any applicable security updates (including OS and browser).

29. The computer, smartcard readers and all cabling MUST be checked for signs of tampering before each payShield Manager session.

30. The computer SHOULD NOT be used for any purpose other than remote management of payShield device, to reduce the risk of compromise of the computer.

31. Equipment that is not required for the operation of the payShield Manager MUST NOT be brought into the Operations Room. Such equipment includes, e.g.: data analyzers, cameras, etc.

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

33. 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.

34. 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 unauthorized access.

HSM Security Configuration

1. HSM configuration is described in the payShield Manager User's Guide, and includes a number of security related activities.Security configuration SHOULD retain the default settings unless there is a good operational reason to do otherwise.

2. All payShield Manager activities and User Events SHOULD be audited by the HSM. As noted in payShield Manager User's Guide, this may impact HSM performance and so the extent of auditable activity SHOULD be reviewed from time to time.

3. Decisions regarding those payShield 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.

Customer Trust Authority

The *Customer Trust Authority* (CTA) is critical to the security of the payShield Manager. All HSMs and smartcards used in the remote management solution possess a public/private key pair, with the public key held in the form of a certificate signed by the CTA's private key. If the CTA private key is compromised, an attacker can impersonate any member of the Customer Security Domain.

A one-off process to generate the CTA public/private key pair is performed on an HSM whose firmware supports the remote management solution. This is achieved via the GUI or the XI Console command and is described in detail in the payShield Manager Installation Guide.

Thereafter, individual HSMs generate a public/private key pair and the public key is signed using the CTA private key, this process is known as commissioning Similarly, any of the HSMs can be used to commission smartcards. Commissioning of HSMs and Smartcards uses the GUI, the XH console command (for HSM commissioning), or the XR Console command (for smartcard commissioning) and is described in detail in the payShield Manager Installation Guide.

The CTA public key, in the form of a self-signed certificate, is loaded into each HSM and onto each smartcard as part of the above processes.

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

The CTA private key is stored on a group of smartcards via a (k, n)-threshold scheme[1]. 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 CTA private key shares are called "shareholders".

payShield Manager users may act as shareholders, but there is no requirement for them to do so. In general, the choice of shareholders will depend on the organizational structure.

[1] 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.

1. CTA-related activities SHOULD take place in a secure area.
2. The Security Manager MUST take overall responsibility for all CTA activities and MUST ensure that all CTA-related procedures are followed correctly.
3. The Security Manager MUST maintain a log of shareholder names and the corresponding card number and smartcard fingerprint. 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 CTA private key shares and that they will carry out their duties to the best of their abilities.
6. The number of CTA 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 "n" SHOULD satisfy $2k \leq n$ and there may be operational benefit in allowing "teams" of shareholders to be established.
7. When creating the CTA, the CTA 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 CTA private key share/card.
9. All shareholder smartcards SHOULD be protected by strong PINs. For example:
   - PINs SHOULD be at least 8 digits in length;
   - PINs SHOULD be randomly generated;
   - "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 smartcard 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 labeled; and, as a minimum, the label SHOULD identify the card as a shareholder card.
14. All shareholder cards MUST be stored securely when not in use.
15. Shareholder cards SHOULD NOT be stored in the same location as one-another.

16. Shareholder card PINs SHOULD be written down and stored securely, separate from the cards, and separate from other shareholder card PINs. The Security Manager SHOULD 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 CTA private key shares are created there is no facility to create extra shares. Should a shareholder leave the organization, 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.

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

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

19. 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.

Smartcard Security

payShield Manager users authenticate to the system using smartcards that are protected by PINs. Initially the PIN is the transport PIN created when the card was issued. Users are forced to change the PIN before subsequent use of the card.

1. Smartcards MUST be stored securely when not in use.

2. Smartcard PINs SHOULD be written down and stored securely, separate from the smartcards.

3. The Security Manager SHOULD NOT need to know the secure storage location of smartcards and the corresponding PINs and MUST NOT have access to any of these items.

Remark: Unlike the situation with CTA private key share cards, additional smartcards can be created in the event that an existing cardholder leaves the organization or if a card becomes unusable.

4. A person who ceases to hold their role within the payShield Manager system MUST surrender their cards immediately, and have their access rights to both their card and to the relevant secure areas revoked immediately.

5. Smartcards MUST be removed from the payShield Manager attached smartcard reader as soon as authentication has completed.

6. All smartcards SHOULD be clearly labeled (for example whether the card is a left or right key card or a restricted card).

7. Smart cards SHOULD 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).

8. Users MUST use a tamper-resistant PIN entry device in conjunction with the payShield Manager.
9. Users MUST NOT divulge their smartcard PINs to any other party.
10. Users SHOULD change their PINs on a regular basis.
11. All access to smartcards and PINs SHOULD be recorded by the Security Manager.
12. Smartcards SHOULD be tested regularly to ensure that they still function correctly.
13. A Smartcard 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.
14. Smartcards MUST be distributed securely to the relevant user and the recipients MUST acknowledge receipt of the cards.
15. The transport PIN for the smart cards SHOULD be distributed separately from the cards and, ideally, SHOULD NOT be sent until card receipt has been acknowledged.
16. The Security Manager MUST retain a record of all HSMs and smartcards that have been issued (i.e. a public/private key pair has been generated and the public key signed by the CTA private key).

RLMK Smartcards

RLMK users of the payShield Manager carry out a range of sensitive functions, including key management activities and functions that require the HSM to be in Authorized State. RLMK smartcards store Local Master Key (LMK) shares and/or authorization passwords. As such, the security of the RLMK smartcards is critical to the security of the payShield Manager.

In addition to the general security guidelines relating to smartcards, the following guidelines apply specifically to RLMK cards:

1. RLMK cards MUST be clearly labeled; and, as a minimum, the label MUST identify the LMK.
2. RLMK Authorizing Password smartcards SHOULD be created and used for day-to-day operations; and cards containing LMK shares SHOULD NOT be used for day-to-day operations.
3. RLMK Authorizing Password smartcards MUST be clearly labeled; and, as a minimum, the label MUST identify the LMK and the password number (1 or 2).

Remark: RLMK and RLMK Authorizing Password smartcards are specific to a particular LMK and so when multiple LMKs are used, the labeling of the cards is crucial. It may therefore be convenient if the authorizing password card's label also includes the relevant LMK identifier although this can be changed when the LMK is loaded. The LMK identifying is less likely to change in systems where the same LMK is loaded on to multiple HSMs.

Customer Security Domain

The term "Customer Security Domain" describes a set of smartcards and HSMs, such that (secure) remote communication between a card in the group and the HSM in the group is permitted. A necessary pre-requisite for a card and a HSM to be in the same Security Group is that both must possess their own key pair, with the public key signed by the same CTA private key.

In addition to the Customer Security Domain each HSM maintains its own whitelist, into which smartcard details (including public key certificate and serial number) are loaded and associated with their designated role. If an HSM does not contain details of a particular smartcard then communication between the two devices is not possible.

Details of the initialization and management of the Customer Security Domain can be found in the payShield Manager Installation Guide and the payShield Manager User's Guide.

1. The Security Manager MUST keep a record of all smartcards and HSMs that belong to each Customer Security Domain; the record MUST be updated as new devices are added to, or deleted from any Customer Security Domain.

2. The Security Manager MUST keep a record of all smartcards and their associated roles allowed to communicate to each HSM; the record MUST be updated as new devices are added to, or deleted from the HSM.

3. Details of a lost or stolen card MUST be deleted from all HSM whitelists in the card's Customer Security Domain as soon as possible.

Back-Up

All equipment and audit records relating to the payShield Manager must be backed-up.

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

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

3. All audit records relating to the payShield Manager MUST be backed-up and at least one copy SHOULD be stored off-site.

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

Operational Security

Details of payShield Manager operations are given in payShield Manager User's Guide. These should be complemented by an organizational security and operations document based on this guide. 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 organization and so any of the particular guidelines below that relate to keys should be used to complement this policy.

1. Users MUST be fully aware of, and follow, security procedures relating to the operation of the payShield Manager.
2. The Security Manager MUST ensure that all security procedures relating to the operation of the payShield Manager are followed correctly.
3. Users MUST logout and take their smartcards with them if they exit the Operations Room.
4. Users MUST ensure that nobody else can observe the entry of a PIN at a smartcard reader.
5. HSMs MUST NOT be placed in the Offline state, Secure mode, or Authorized state for any longer than is absolutely necessary to complete the required activity.
6. Users MUST NOT be logged into HSMs for any longer than is absolutely necessary.
7. A time-out for user sessions SHOULD be specified.
8. A Web Application Firewall may be employed to offer additional defense in depth against attacks on the payShield Manager interface.

Appendix C – TLS Security Recommendations

Background

The Thales e-Security payShield 9000 allows for secure host communications via the TLS protocol. These connections are secured using a Public Key Infrastructure (PKI) trust system.

payShield 9000 TLS Server

The payShield 9000 provides the TLS server for secure host communications. To enhance the security of the connections the server has been configured with the following options:

Protocol Support

From software version 3.3a, the TLS server only supports the TLS v1.2 protocol.

Cipher Suite Support

The server will only support connections with one of the following cipher suites; with preference being given in descending order:

Cipher ID	Cipher Suite Name	Protocol version
1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS v1.2
2	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS v1.2
3	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS v1.2
4	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS v1.2
5	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLS v1.2
6	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLS v1.2
7	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS v1.2
8	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS v1.2
9	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS v1.2
10	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS v1.2
11	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS v1.2
12	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS v1.2

Elliptic Curve Cryptography (ECC) asymmetric key pairs SHOULD be preferred over RSA key pairs whenever possible due to the increased security strength they provide.

TLS Configuration Options

The server also has the following options configured:

- When negotiating a cipher, the server's cipher preferences will be used as opposed to the client's cipher preferences.
- Ephemeral key cipher suites are preferred by the server. When selected, every new handshake will require new ephemeral keys be generated; this provides perfect forward secrecy.
- When performing a renegotiation of an existing connection, the server will always force a new session to be negotiated; this protects against a known renegotiation vulnerability.
- Connections will not use data compression, protecting against the CRIME vulnerability.

Man-In-The-Middle Mitigation

The payShield 9000 TLS server implements a client whitelist mechanism to help prevent man-in-the-middle attacks; this prevents any unspecified clients from successfully connecting to the HSM. Any TLS client that wishes to communicate with the server must first have their public key certificate installed in the HSM (performed using the console command SI).

It should be noted that the TLS protocols do not intrinsically provide protection against man-in-the-middle attacks. Therefore clients MUST authenticate the TLS server they are connecting to by checking the information in the server's public key certificate.

To facilitate this validation check, server certificates MUST contain a reference to the entity they belong to; in this case the payShield 9000 Host IP address. This can be achieved through the Subject Alternative Name field of X.509 public key certificates or through an internal PKI and Certificate Authority (CA).

TLS Clients

The payShield 9000 TLS server enforces mutual authentication. This requires the client to authenticate itself to the server as part of the handshake.

To successfully connect to the payShield 9000 clients must have their own asymmetric key pair; the public key of which will be provided to the server during the handshake in the form of a public key certificate.

Thales recommend that industry best practices are followed for the generation, storage and usage of these asymmetric key pairs.

Client Mitigations

The payShield 9000 TLS server includes mitigations for the BEAST attack (CVE-2011-3389), however due to the nature of this attack a TLS session can still be vulnerable if the TLS client does not also implement similar mitigations.

Thales recommend that TLS clients with BEAST mitigations are used to establish secure host communications with the payShield 9000.

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211
E-mail: CPL_Sales_AMS_TG@thalesgroup.com

Asia Pacific
Unit 904-906A, Core D
Cyberport 3, 100 Cyberport Road
Pokfulam, Hong Kong | Tel: +852 3157 7111
Fax: +852 2815 8141 | E-mail: apacsales.cpl@thalesgroup.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: CPL_Sales_EMEA_TG@thalesgroup.com

> cpl.thalesgroup.com <