payShield® 10K

Security Manual

007-001513-005

Date: February 2022

Doc. Number: 007-001513-005

Contents

Revision Status

Document No.	Revision	Date	Changes
PUGD0536-001	001	April 2019	Initial issue
PUGD0536-002	002	July 2019	Update to default settings; update Health LED description Added: Section **2.3.2** NIST SP800-57 and comparable strengths Updated example of VR command output to reflect both PCI compliant output and non-PCI compliant output
PUGD0536-003	003	November 2020	Updated Security Settings to reflect that the import/export of a ZMK encrypted under a ZMK is permitted
PUGD0536-004	004	December 2020	Updated security parameter to include ECC: **Enforce minimum key strength of 2048-bits for RSA and ECC? Yes or No**
PUGD0536-005	005	May 2021	Section 2.1.2 Temperature Alarm updated Section 2. 3 Updated description for security parameters: **Enforce minimum key strength of 2048-bits for RSA and ECC?** Follow this link to page: 22 **Enable import of ZMK:** Follow this link to page: 19 **Enable export of ZMK:** Follow this link to page: 19 **Prevent single-DES keys masquerading as double or triple-length keys:** Follow this link to page: 20
007-001513-005	005	February 2022	New document number Clarification added to the "Select clear PINs" description

1 Introduction

This manual provides regulatory user information for the payShield® 10K product.

The manual identifies the security implications of the security relevant choices available to the user, and provides guidance to assist the user when making those choices.

1.1 General

The payShield 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 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 rack locks with separate physical keys
- Personalized smartcards issued for Security and Authorizing Officers
- Personal Identification Numbers (PINs) issued for Security and Authorizing Officers
- A "SECURE" mode which requires the presence of two Security Officers holding separate physical keys for the front panel locks. (An equivalent card-controlled mode can be achieved via payShield Manager with the two "Administrator" cards.)
- An Authorized mode, requiring the presence of two Authorizing Officers with encrypted smartcards and PINs
- A configurable motion sensor, to detect attempts to move the unit
- Configurable security parameters
- Error and Audit Logs
- Tamper evidence and tamper resistance with fully locked-down lid, and sensors to detect motion, voltage, and temperature anomalies
- Secure by default – Where possible, default settings are the most secure option.

2   Configuration

2.1   Configure Alarm

2.1.1   Motion Alarm

The HSM Motion Alarm should be turned on when the HSM is put into service. Once enabled, the Motion Alarm will need to be turned off if the HSM is to be moved.

To view and modify the current alarm settings using payShield Manager, navigate to **Configuration > General Settings > Alarms**.

The **CL** console can also be used to change alarm settings.

The HSM must be in the Secure state to configure the Motion Alarm.

The Motion Alarm has four security level settings: off, low, medium, and high. Changing the setting to a lower level results in LMKs being erased. (See *Section 3.4, Motion Sensor*, for additional information.)

2.1.2   Temperature Alarm

The Temperature Alarm is permanently enabled and can not be disabled by users.

The alarm is triggered if the temperature inside the HSM exceeds a safe value.

The temperature sensor is active even if the payShield 10K is disconnected from an electrical power supply. The temperature sensing capability is maintained by the payShield 10K's internal battery, and will still initiate LMK deletion and tamper state.

If the temperature falls outside of predefined limits, the temperature sensor will initiate a tamper alarm causing the LMKs to be deleted and the unit will automatically reboot and attempt to clear the tamper state. If the alarm condition persists, the unit will stop attempting to clear the tamper after 2 attempts and will remain powered on with limited functionality such that LMKs cannot be loaded. Deletion of the LMKs prevents the payShield 10K from executing Host commands or console commands which require an LMK to be present.

Once the stimulus that triggered the alarm has ended, the payShield 10K will need to be rebooted to clear the tamper state and allow the LMKs to be reloaded.

An entry will be made in the error log.

2.2   Configure Self-tests

Self-tests are run during the HSM boot-up.

PCI HSM requires that 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.

To change the self-test run time:

ⓘ The payShield is in the Offline or Secure state.

- Navigate to **Status > Health Statistics/Diagnostics > Diagnostics**.
- Click the tools icon (located on the far right of the display).
- Click **Change time**.
- Enter your time preferences in the Enter Time display.
- Select **Apply**.
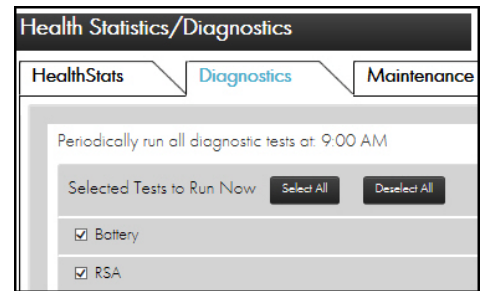
ⓘ The **DT** console command can also be used to change self-test settings.

Failures in the daily self-tests typically generate an Error log entry, reboot immediately. If another failure occurs, the device enters a tamper state.

2.3   Configure Security Settings

By default, the security settings are set to their most secure option with exceptions duly noted.

To configure security settings:

ⓘ The payShield is in the Secure state.

- Navigate to: **Configuration > Security Settings**.
- Review/modify the settings on the **General** display.
- Select **Apply**.
- Select **Initial**.
- Review/modify the settings on the **Initial** display.
- Select **Apply**.
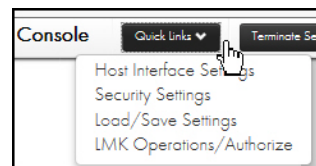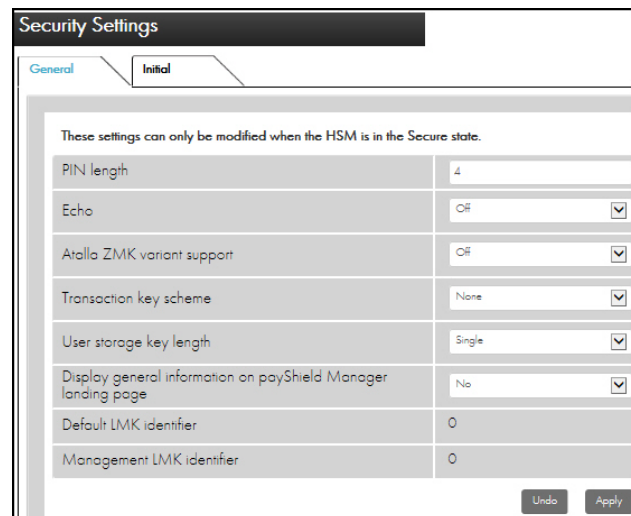
ⓘ The Quick Links tab contains navigational shortcuts.

ⓘ The CS console command can also be used to change security settings. The settings can be examined using the **QS** console command.

2.3.1   Security Parameter Descriptions

Security Parameter Description	Default Value
PIN length: 04..12	04
Encrypted PIN length:	05
This value is used by the HSM to define the length of encrypted PINs, symbolized as "L" in the payShield 10K 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 is 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.	
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.	
Echo: On or Off	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.	
Enabling Echo is a security hazard and should not be used in a live system.	
Atalla ZMK variant support: On or Off	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. ℹ️ Selection has no effect on host commands - Atalla variants can be supplied with any appropriate command regardless of this setting.	
Transaction key support: 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 10K supports three variants of transaction key schemes: Racal (i.e., Thales), Australian (AS2805), and DUKPT. There are command conflicts between the Racal and Australian schemes so only one can be selected. The use of DUKPT commands is not affected by this setting. ℹ️ The default value is '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.	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 contains basic information about the HSM.	NO
Default LMK identifier: 00..99 Identifies the Default LMK, which the HSM will use if it receives a command that does not explicitly state which LMK is to be used. The use of the Default LMK provides a "backward-compatible" mode, even when multiple LMKs are loaded in the HSM. The upper limit (99) is determined by the number of LMKs that can be installed concurrently.	00
Management LMK identifier: 00..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.	00
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. ⓘ This parameter only valid if the "Atalla ZMK variant support" was previously set to 'ON'.	NO
Select clear PINs: Yes or No The BA host command is NOT controlled by this setting. This enables the clear PIN support via the 'NG' host command. Authorized state is a requirement for this command 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
Solicitation batch size: 0001..1024 A method, supported by the payShield 10K, 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

ZMK length: Single or Double The length of the Zone Master Key: 'Single' or 'Double'. This is a backwards-compatible mode to enable the switching between 16H and 32H for ZMKs.	DOUBLE
Decimalization tables: 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
Decimalization table checks: Yes or No 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.	YES
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
Use default card issuer password: Yes or No This option determines whether the default Card Issuer Password is user or not. ℹ 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 does not match the password on the smartcard,	n/a

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.	
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 DES keys 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
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/TEK 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 or TEK) 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 or TEK 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	YES

If enabled, will allow precise selection of authorized activities (including timeout period if required). If disabled HSM reverts to global Authorized state.	
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.	NO
Enable variable length PIN offset: Yes or No If enabled, this will allow the IBM 3624 PIN Offset commands to return an Offset whose length matches the PIN, rather than being restricted to the Check Length parameter.	NO
Enable weak PIN checking: Yes or No If enabled, the HSM's PIN generation/derivation host commands will check to ensure that the 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
If Enable weak PIN Checking is set to YES, the following 3 parameters display:	
Check new PINs using global list of weak PINs: Yes or No *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.*	
Check new PINs using local list of weak PINs: Yes or No *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.*	
Check new PINs using rules: 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 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).*	
Enable PIN Block Format 34 as output format for PIN translations to ZPK: Yes or No If enabled, the HSM will permit PIN block format 34 to be used as the output format of PIN translation commands.	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
Use HSM clock for date/time validation: Yes or No If enabled, the HSM uses its integral real-time clock to validate check the start/end date/time optional header blocks of keyblocks (when present).	YES
Additional padding to disguise key length: Yes or No If enabled, the HSM disguises the length of single or double length keys within a keyblock by adding 8 or 16 extra padding bytes, such that single, double and triple length DES keys all appear to be triple length keys.	NO
Key export and import in trusted format only: Yes or No If enabled, the HSM will only import/export keys using a keyblock format. In this case, any export/import process using keys in variant format (including X9.17 format) will be prohibited.	YES
Protect MULTOS cipher data checksums: Yes or No This setting is used to control whether checksums generated over sensitive data will require encryption.	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
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
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	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.	
ℹ THE FOLLOWING PARAMETERS AFFECT PCI HSM COMPLIANCE	
Prevent single-DES keys masquerading as double or triple-length keys: Yes or No If enabled it will prevent the use of single-length DES keys disguised as a double or triple length key. ℹ 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.	YES
Single-DES: Enabled or Disabled 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. ℹ To operate in PCI HSM compliant mode, the HSM software must be PCI HSM certified and this option must be set to 'Enabled'. If this option is set to 'Disabled' 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.	ENABLED
Card/password authorization (local): C or P 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.)	C

ℹ 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 'C' 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.	
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). ℹ 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). If this option is enabled the following host commands are disabled: AA, AE, FC, FE, FG, HC, KA, OE. ℹ 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 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.	YES

ℹ️ 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.	
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. ℹ️ 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.	YES
Enforce PCI HSMv3 Key Equivalence for Key Wrapping? Yes or No If enabled, the HSM will not permit a lower strength key to encrypt a higher strength key – using the NIST SP800-57 recommended definitions of relative key strength. ℹ️ 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.	YES
Enforce minimum key strength of 1024-bits for RSA signature verification? Yes or No If enabled, the HSM will not permit RSA signature verification using a key smaller than 1024 bits. ℹ️ 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.	YES
Enforce minimum key strength of 2048-bits for RSA and ECC? Yes or No	YES

If enabled, the HSM will enforce the minimum RSA and ECC key sizes mandated by PCI for use with key transport, exchange, or establishment and for data protection in connection with these requirements. It does not enforce the minimum key sizes for non-PCI payment brand relevant transactions (e.g. for Australian AS2805 commands, WebPIN commands, OBKM commands) nor for card issuance commands (including Multos). 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.	

2.3.2   NIST SP800-57 and comparable strengths

When "Enforce PCI HSMv3 Key Equivalence for Key Wrapping" is set to YES, this setting does not allow RSA keys greater in length than 1024 bits to generated with a double length 3DES LMK loaded. This is because NIST SP800-57 specifies that a double length 3DES key is equivalent in strength to a 1024 bit RSA key.

The three settings referenced are:

- Enforce PCI HSMv3 Key Equivalence for Key Wrapping: YES
- Enforce minimum key strength of 1024-bits for RSA signature verification: YES
- Enforce minimum key strength of 2048-bits for RSA: YES

Extract from NIST SP800-57 – Comparable strengths

Security Strength	Symmetric key algorithms	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
≤ 80	2TDEA21	$L = 1024\ N = 160$	$k = 1024$	$f = 160\text{-}223$
112	3TDEA	$L = 2048\ N = 224$	$k = 2048$	$f = 224\text{-}255$
128	AES-128	$L = 3072\ N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680\ N = 384$	$k = 7680$	$f = 384\text{-}511$

2.4   Configure Commands

payShield 10K provides over 80 console and over 400 host commands. Typically, host applications use just 10% of these commands, depending on the payments functionality they are serving. Unused commands left enabled could present a security risk, so all commands except the console **CONFIGCMDS** command are disabled at the factory.

Thales recommends that customers enable just those commands which are required. Note that disabled commands are not available until they are re-enabled.

To enable or disable commands, navigate to the **Configuration** tab in payShield Manager and then select **Configure Commands**.
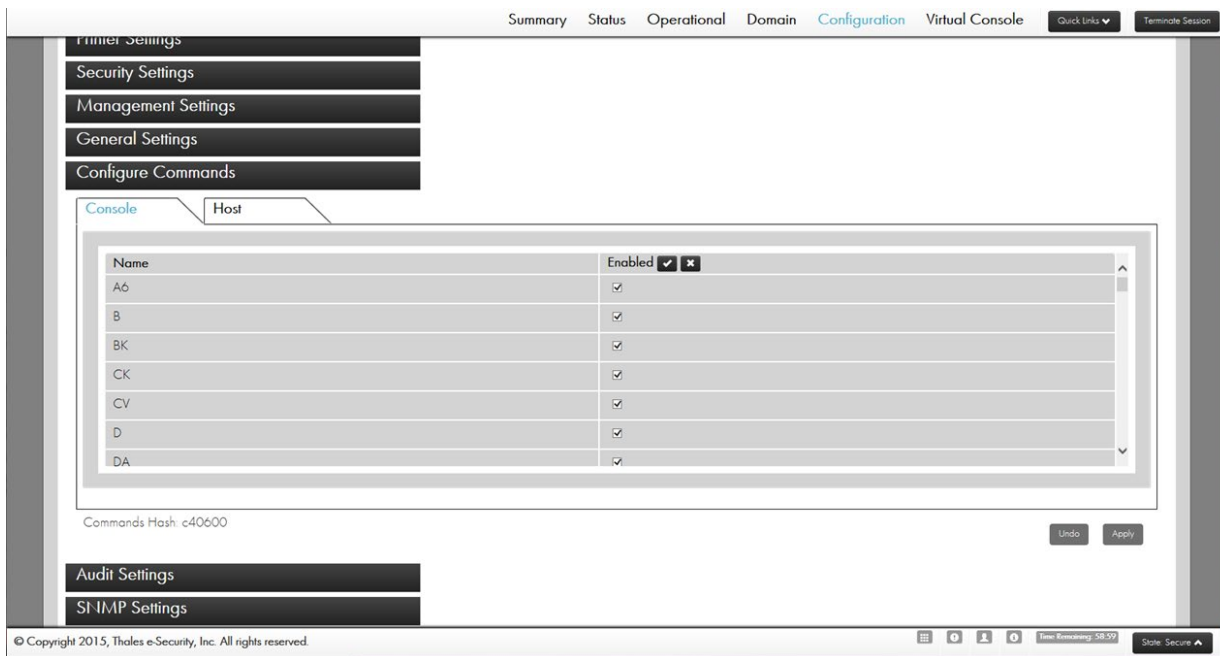
ℹ Note that disabled console commands return a "Function Disabled" error and host commands return an Error Code 68.

ℹ To view the list of enabled host and console commands, and (if in Secure state) to enable or disable host and console commands, you can also use the console **CONFIGCMDS** command.

ℹ All available commands are disable by default, except **CONFIGCMDS**.

2.5   Configure PIN Block

A PIN Block is a cryptographic transformation of a PIN. It is a PCI requirement that the account number or a related number is included in the PIN Block transformation. There are several methods for PIN Blocks, not all of them are compliant with standards.

To enable or disable PIN Blocks, navigate to the **Configuration** tab in payShield Manager and select **General Settings;** from the general settings, select **PIN Blocks**.
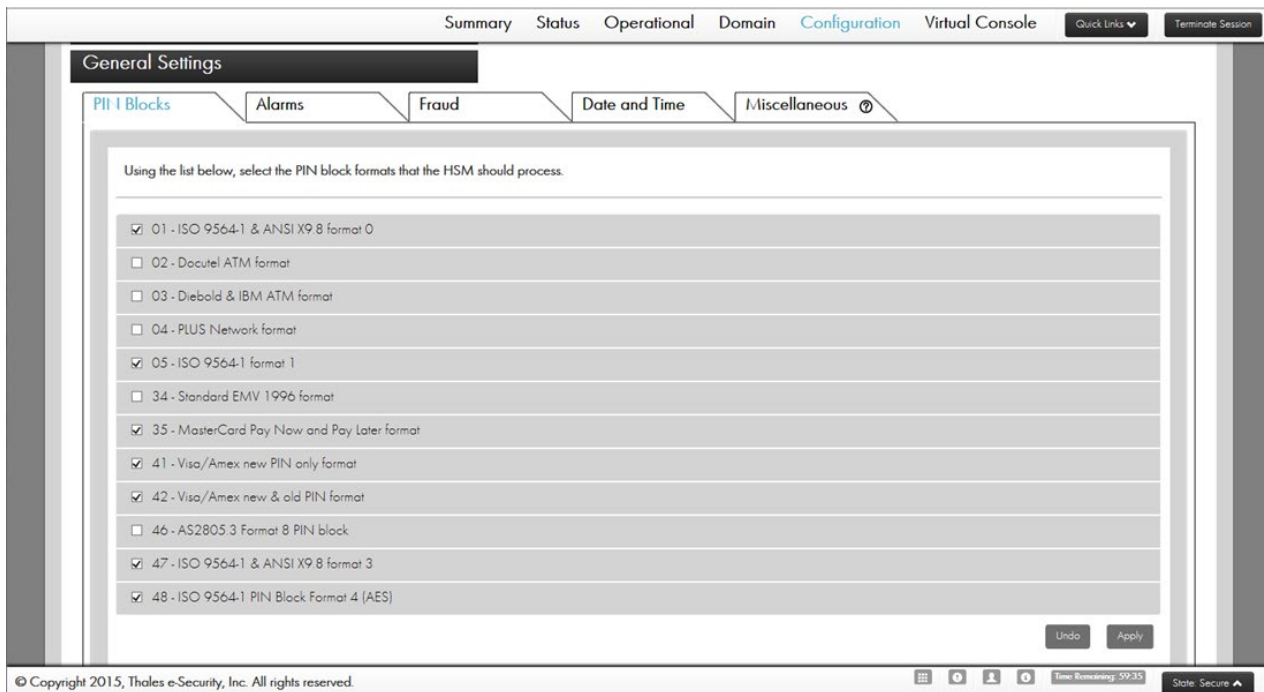
To view the list of enabled PIN Blocks, and (if in Secure state) to enable or disable PIN Blocks, you can use the console command **CONFIGPB**.

ℹ️ Note that by default, the "weakest" PIN block formats are disabled: Formats 02, 03, 04 & 34.

For additional information about PIN Blocks, see the *payShield 10K Programmer's Manual* and the *payShield 10K Installation and User Guide*, Appendix A.

2.6   Configure Fraud Detection

The payShield 10K's fraud detection functions are designed to detect and prevent "brute force" attacks, where, for example, large numbers of PINs are submitted until the correct PIN is discovered.

The detection works by counting the number of failed PIN verifies detected in one minute and in one hour. Each time that these counts exceed specified limits, the PIN Attack Counter is incremented. If the PIN Attack Counter exceeds the specified PIN Attack Limit, then a PIN Attack is assumed.

The fraud detection configuration also determines how the HSM will react. The user can select "On" for full pro-active response to the limits being exceeded, or "Logging Only" in order to record (in the Health Check Data) the limits being exceeded without taking any further action.

ℹ️ Note: An entry is always made in the Audit Log if any of the limits are exceeded.

2.6.1   Configuration Options

If the Logging Only option is selected, then the payShield 10K provides counts of how many times the per-minute and per-hour limits have been exceeded and the total number of PIN Attacks detected.

This information is provided as part of the Health Check Data. Initiating the data capture or resetting counts can be done via console command or via payShield Manager.

ℹ️ Note: The term "Logging" refers to capture of the information in the Health Check data. Audit Log entries are always made when the limits are exceeded.

If the "On" option has been selected, then the reporting provided by the Logging Only option is again provided. In addition, if either of the per-minute or per-hour counts exceed the specified limits, the HSM forces all PIN verification commands to return an Error 39 in their response.

The HSM will continue to return Error 39 until the console command **A7** is used to re-enable PIN verification. If the PIN Attack Counter reaches the PIN attack limit, then the HSM will clear the LMKs from it memory. Installing the LMKs will set the PIN attack counter to 0.

The following list specifies the PIN verification host commands to which the limits apply:

- **DA** – Verify a Terminal PIN Using the IBM Method
- **EA** – Verify an Interchange PIN Using the IBM Method
- **CG** – Verify a Terminal PIN Using the Diebold Method
- **EG** – Verify an Interchange PIN Using the Diebold Method
- **DC** – Verify a Terminal PIN Using the Visa Method
- **EC** – Verify an Interchange PIN Using the Visa Method
- **BC** – Verify a Terminal PIN Using the Comparison Method
- **BE** – Verify an Interchange PIN Using the Comparison Method

To enable fraud detection options using payShield Manager, navigate to the **Configuration** tab, then navigate to **General Settings**, select the **Fraud** tab.
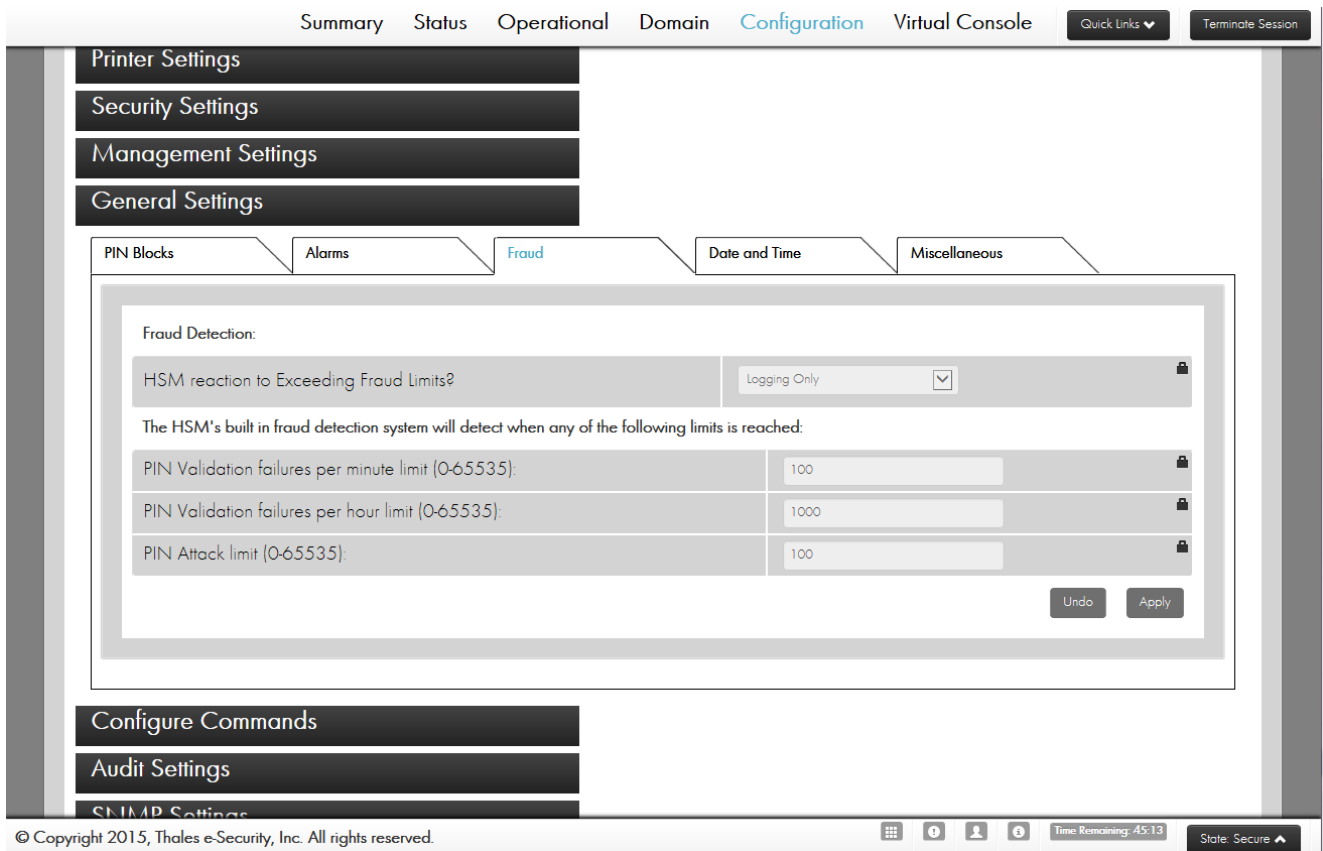
To enable fraud detection, use the console **A5** command. For additional information, see the *payShield 10K Installation and User Guide*, Console Reference appendix.

3 Tamper Protection

Tamper refers to an intentional manipulation of the system in order to attempt to compromise the secrets in the system, or enable unauthorized operation. Tamper protection is accomplished via tamper resistance, detection, and response.

Tamper protection is implemented in three tiers:

1. Tamper resistance – using a design that makes it difficult for the attacker to attempt to access the secure area of the payShield 10K. This is done partially using physical characteristics such as using toughened materials, or providing no path that can be used by probes to make contact with the electronics inside the HSM.

   However, an HSM cannot prevent all attempts at physical access to its internal components. An HSM that could resist high-performance drills, gunshots, explosives, chemical attacks, oxyacetylene cutting torches, etc., would be so expensive, large, and heavy that it would not be a practicable proposition for potential users.

2. Tamper detection – any tamper activity should be detected by the HSM. Detected tamper attempts must be evident to the owner of the HSM.

   For example:

   - payShield 10K has a permanently locked lid. Removal of the lid will put the payShield into a tampered state

   - Detected tamper attempts are recorded in Error and Audit Logs

   - LEDs are illuminated on the front panel of the payShield 10K to indicate a tamper has occurred

3. Tamper responsiveness – the payShield takes actions in response to a detected tamper event to ensure that the secret data being protected by the HSM cannot be accessed by attackers even where they have gained access to the internal components of the HSM.

This chapter focuses on the tamper protection and responsiveness of the payShield 10K.

3.1 Tamper Responsiveness

3.1.1 Types of Tamper Actions

A payShield 10K may be subjected to the following types of tamper attempts:

1. Physical access to the components inside the HSM.
2. Environmental changes
3. Intended erasure of Customer Key Material
4. Fraud Attack

These are discussed in the sections that follow.

3.1.1.1 Physical Access

An attacker may attempt to gain physical access to the components inside the HSM, for example, to attach probes to data paths or microchips in order to read data. This may be attempted by removing or bending the lid, or by drilling or cutting through the casing to reach the circuit boards inside the casing.

The payShield 10K can detect removal or partial removal of the lid, distortion of the lid, and physical access to the secure components of the HSM.

On detection of such an attempted tamper, the payShield 10K will enter the tamper state, as described in a later section.

3.1.1.2 Environmental Changes

An attacker may attempt to change environmental conditions, such as temperatures or voltages, in order to affect the operation of the HSM. The payShield 10K will detect such actions. The temperature sensor is described in more detail later in this chapter.

An attacker may also try to remove an HSM and take it to a workshop or to another location, where they can attempt attacks at their leisure. To thwart this threat, the unit is designed with a locking mechanism. When the unit is placed in either the Online or the Offline state, the mechanism engages and the unit is physically locked to the rack/cabinet. In addition, the payShield 10K has a configurable motion sensor that detects if the unit is being moved. The motion sensor is described in more detail later in this chapter.

On detection of such an attempted tamper, the payShield 10K will enter the tamper state, as described in a later section.

3.1.1.3 Intended Erasure of Customer Key Material

A payShield 10K operator can voluntary trigger a tamper condition on the HSM, by inserting a probe into the "Erase" hole on the rear of the HSM. This might be done, for example, if the operator believes some kind of attack is being launched somewhere on their system and they want to rapidly disable the HSM.

On detection of such a voluntary tamper, the payShield 10K will enter a tamper state, as described in a later section.

3.1.1.4 Fraud Attack

Whereas the preceding tamper actions require physical access to the payShield 10K, a Fraud Attack could be launched from any computer that can communicate with the HSM.

A Fraud Attack is essentially a brute force attack to uncover PINs. By issuing a sequence of commands to the HSM to verify a PIN, the attacker can keep trying different PINs until they receive a positive PIN verification response to indicate that the PIN is correct.

The payShield 10K offers an optional Fraud Detection mechanism to protect against this type of attack.

For additional discussion, see *Section 2.6, Fraud Detection Function*.

3.2   Tamper States

There are two levels of Tamper on payShield 10K:

- Medium tamper - This tamper type indicates that the unit is experiencing persistent failures or abnormal conditions, and may no longer be able to ensure its security state. This may be an indication that the unit is under attack or is compromised. When this level of tamper is detected, the HSM erases all sensitive customer data.

- High tamper – This tamper type indicates that the unit is no longer able to protect itself with assurance, and should be removed from service. There is a likelihood that the unit is under attack, has already been compromised, or has experienced a failure of a security-relevant component. When this level of tamper is detected, the HSM erases all sensitive data and permanently disables use of the unit.

3.2.1   Medium Tamper

When the payShield 10K detects a medium tamper attempt, it will:

1. Delete the HSM's customer-specific secrets.
2. Re-start the HSM.
3. Make an entry in the Error Log.
4. Illuminate the "Tamper" LED on the front panel of the payShield 10K; the LED will extinguish when the cause of the tamper is removed.
5. Turn the "Health" LED on the front panel of the payShield 10K red.
6. If Health Check Counts have been enabled, increment the tamper count.

As described above, detection of a medium tamper results in deletion of the HSM's secrets (depending on user settings, in the case of Fraud Attacks). The secrets that will be deleted are

- Local Master Keys (LMKs)

  The LMKs are stored in the HSM and used to encrypt all the keys that are protected by the payShield 10K, and some other data such as PINs and Decimalization tables. If the LMKs are deleted, the HSM can no longer decrypt any protected data and essentially becomes inoperative.

  To re-enable the payShield 10K, the LMKs must be re-installed from components held on smartcards; this requires the co-operation of multiple (usually three) officers, ensuring that the HSM is not re-enabled until the cause of the tamper has been investigated.

- Private keys

  Private keys are used for capabilities such as payShield Manager and Secure Host Communications. To re-enable these capabilities, the Private keys must be re-loaded by using the HSM Recovery Key (HRK). (For additional information, refer to the *payShield 10K Installation and User Guide*.)

3.2.1.1   Recovering from a Medium Tamper

No attempt should be made to return the payShield 10K to an operational state until an appropriate incident management process has been followed to investigate the cause of the tamper, and determine whether a true attack took place and whether the attack was successful.

The LED indicators will show the following:

1. If the "Tamper" LED is still illuminated, the cause of the tamper state is still present and the payShield 10K should not be put into service.

2. The "Health" LED will turn red after the automatic restart, indicating that there are new Error Log entries that have occurred since the Error Log was last viewed. These new entries (which will include those resulting from the tamper detection) should be viewed, and the cause of the tamper identified and any appropriate action taken. Viewing the Error Log will cause the "Health" LED to return to normal (white).

When all investigatory and corrective actions have been taken, the LMK(s) must be reloaded. Where multiple LMKs are being used, they should be loaded into the same "slots" or IDs that they occupied before the tamper event.

Where the medium tamper condition arose from the Fraud Detection facility, PIN verification processing must be re-enabled by using the A7 console command. If a medium tamper state cannot be cleared or tamper states recur without apparent reason, users with support contracts should contact their support provider.

Only if you are confident that the payShield 10K has not been compromised should you return it to production use by:

- Re-installing LMKs
- Confirming that security settings have the correct values
- Confirming that the correct host/console commands are enabled
- Confirming that the correct PIN Block formats are enabled
- Confirming that the appropriate alarms are set
- Confirming that the host/management/console port settings are correct

3.2.1.2   Error Log Entries

When a tamper is detected, an entry is made in the payShield 10K's Error Log; this will in turn cause the "Health" LED on the front panel of the payShield 10K to turn red.

3.2.2   High Tamper

When the payShield 10K detects a high tamper attempt, the response is fundamentally the same as in the medium tamper response, with the following differences:

3. Delete all HSM's secrets, rendering the unit non-functional.

4. Re-start the HSM. The HSM will boot into a restricted Boot Manager.

5. Illuminate the "Tamper" LED on the front panel of the payShield 10K.

6. Turn the "Health" LED, on the front panel of the payShield 10K, red.

7. If Health Check Counts have been enabled, increment the tamper count.

As noted above, when a high tamper response occurs, all secrets in the unit, including customer keys, private keys for secure communications, and the HSM Recovery Key, are all deleted. In addition, the unit will boot only to a Boot Manager application, available via the console prompt. Code updates and other recovery actions are not possible. payShield Manager will no longer be able to connect to the machine. The payShield application will not boot.

The payShield never recovers from a high tamper state and the unit must be returned to Thales for disposal, or be disposed of by the customer.

3.2.2.1   Error Log Entries

As mentioned, with a high tamper, the payShield 10K loads into a Boot Manager application, as such, there is error information available to allow for a root cause analysis.

3.3   Temperature Sensor

3.3.1   Description

The payShield 10K is built around a secure cryptographic module called the Thales Advanced Security Platform (TASP). This provides the core of the security for the payShield 10K and is where all the processing occurs and all the sensitive material is held. The TASP is certified to FIPS 140-2 Level 3.

The TASP incorporates a temperature sensor. This is designed to detect an operational environment which could result in unreliable performance of the security processing within the payShield 10K, and if triggered, it will result in a tamper state. The temperature alarm cannot be disabled by users and is permanently enabled, as can be seen in payShield Manager **Configuration / General Settings / Alarms**:
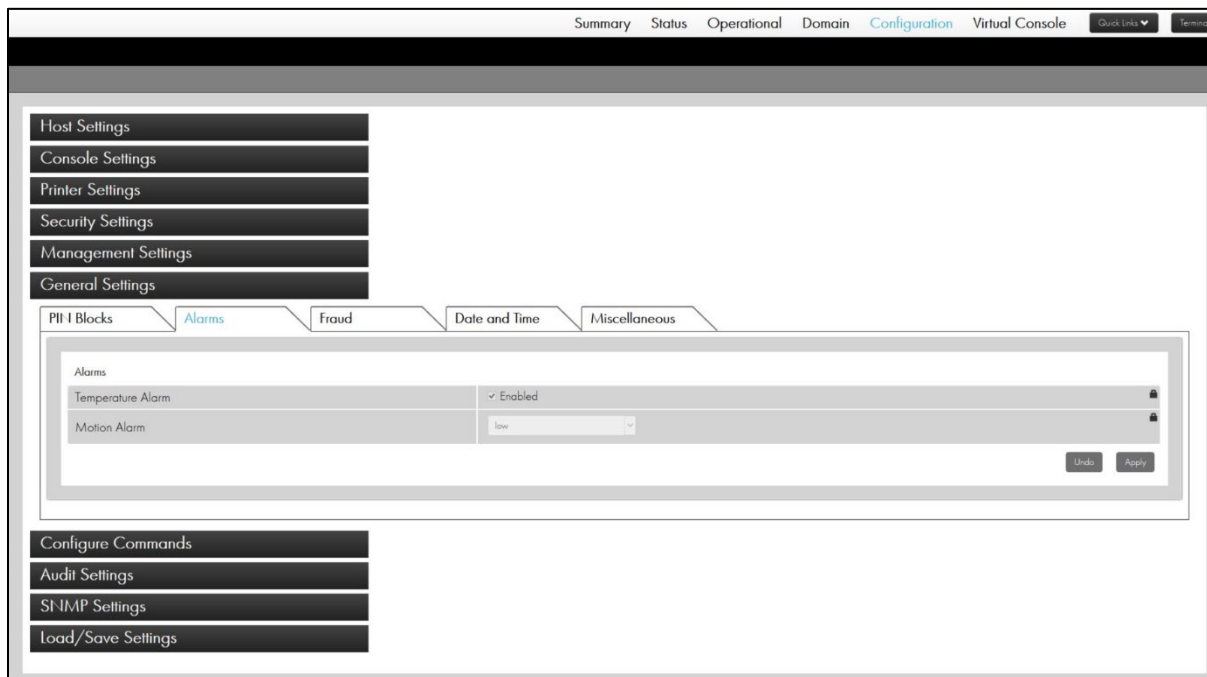
The temperature sensor is active even if the payShield 10K is disconnected from an electric power supply; in this environment, the temperature sensing capability is maintained by the payShield 10K's internal battery, and will still initiate LMK deletion and tamper state.

3.3.2   Triggering of the Temperature Sensor

If the monitored temperature falls outside of predefined limits, the temperature sensor will initiate a tamper response, causing the LMKs to be deleted and the unit will automatically reboot and attempt to clear the tamper state. If the alarm condition persists, the unit will stop attempting to clear the tamper after 2 attempts and will remain powered on with limited functionality, such that LMKs cannot be loaded. Deletion of the

LMKs prevents the payShield 10K from executing host commands or console commands, which require an LMK to be present.

Once the stimulus that triggered the alarm has ended, the payShield 10K will need to be rebooted to clear the tamper state and allow the LMKs to be reloaded.

An entry will be made in the payShield 10K Error Log and the "Health" LED, on the front panel of the payShield 10K, will be illuminated to indicate that there is a new Error Log entry.

3.4 Motion Sensor

3.4.1 Description

The payShield 10K incorporates a motion sensor to allow operators additional protections against physical attacks in their operational environments, (e.g., removal from a rack). The user can configure the motion sensor for one of four settings:

- Off
- Low
- Medium
- High

The motion sensor, when enabled, uses an accelerometer to detect tilt in either the x or y axis, i.e., tilt, with variation in sensitivity controlled by the low, medium, and high setting. The motion sensor, if enabled, is active with/or without mains power due to the internal battery.

3.4.2 Sensitivity of the sensor

The motion sensor has 4 settings which are described below:

Motion Sensor Setting	Minimum Activation Tilt Angle (x or y axis)	Maximum Activation Tilt Angle (x or y axis)
Off	Disabled	Disabled
Low	8°	12°
Medium	4°	8°
High	1°	3°

Activation of the motion sensor is considered a "medium tamper" event which triggers several actions including erasure of the LMKs.

The sensor logic includes a high pass filter to remove very low frequency and static acceleration. The gravity acceleration vector is automatically adjusted to account for any slight tilt due to the unit not being perfectly level.

The logic also avoids triggering of the alarm by a sudden and short shock (e.g., someone bumping into the rack). An acceleration event occurs if the acceleration thresholds above are exceeded for 2 consecutive sampling periods (of 25 milliseconds each). For the alarm to be triggered, 12 acceleration events must be recorded over a period of 1.5 seconds.

3.4.3   If the Motion Sensor is activated

If a motion event exceeding the selected threshold level occurs, the motion sensor will initiate a tamper alarm causing the LMKs to be deleted and the unit will automatically reboot and attempt to clear the tamper state. Deletion of the LMKs prevents the payShield 10K from executing host commands or console commands, which require an LMK to be present.

Because a motion is a transient event, the payShield 10K will normally reboot and clear the tamper state (but the LMKs will still be deleted, of course). If the unit detects an additional motion event after the reset, it will go through the tamper process again.

An entry will be made in the payShield 10K Error Log and the health LED on the front panel of the payShield 10K will turn red to indicate that there is a new Error Log entry. The Tamper LED on the front panel will turn red, indicating a tamper.

3.4.4   Enabling the Motion Alarm

By default, the motion alarm is disabled when the payShield 10K is shipped by Thales. This is to prevent the unit entering a tamper state prior to delivery to the user as a result of movement during shipping.

This means that users must actively enable the motion alarm in order to benefit from the additional security that this offers. This can be done by using:

> The CL Console command, by entering "L", "M", or "H" to indicate the desired sensitivity level after the prompt:
> "Motion Alarm [Low/Med/High/ofF] (OFF):".

The Alarms dialogue box in the payShield Manager (General Settings tab in the Configuration section menu) provides a selection box with the Motion Alarm sensitivity options:
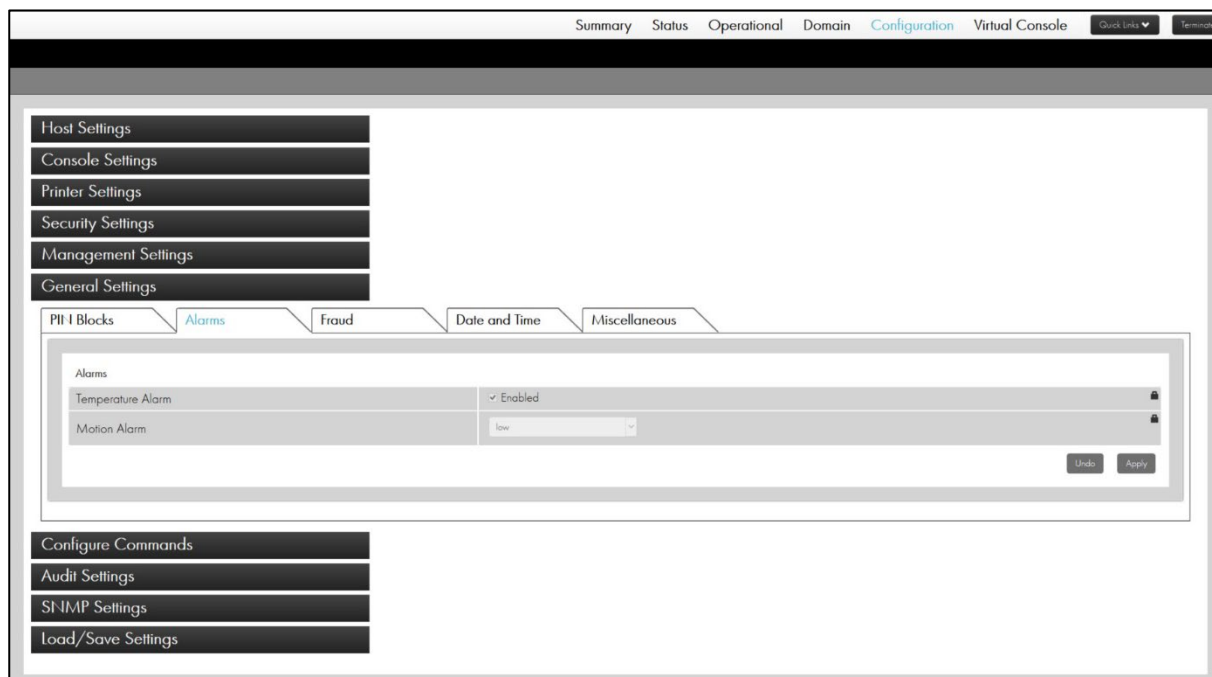
> Full details are available in the *payShield Manager 10K Installation and User Guide*.

4   Secure Host Communications

4.1   Introduction

Traditionally, HSMs have been connected to host computers via a dedicated network, and both HSMs and hosts have been located in the same physical location (typically a data center).

Now, however, HSMs may be located remotely from host computers, for example, where hosts are in "the cloud". Some users are looking to use networks, which are shared with other traffic, and which may even be public networks. This introduces new requirements to maintain the security of the HSM environment, i.e.:

1. Mutual authentication between the host application and the HSM - to provide confidence to each "end" that the communication partner is what they expect it to be.

2. Privacy of transmitted data - to prevent any interceptor of the traffic from being able to read it. (Most secret information (such as keys, PINs) is in fact already encrypted when outside of the HSM, although PINs may be communicated in the clear for the purpose of PIN mailer printing. Other information, such as account numbers, has traditionally been sent in the clear, as it was not viewed as being secret.)

3. Integrity of the transmitted data - to ensure that the data is not modified between sender and receiver.

These requirements are driven by best security practise. In addition, the PCI DSS standard requires cardholder data, such as account numbers, to be protected when transmitted over non-private communication interfaces.

4.2   payShield 10K Secure Host Communications

To meet this emerging requirement for secure host communications, payShield 10K supports the use of TLS to secure traffic between host applications and HSM. Only TLS 1.2 is supported.

ℹ This capability is available for Ethernet connections; it is not appropriate for Asynchronous or FICON interfaces.

4.3   Overview of TLS on the payShield 10K

4.3.1   What TLS Provides

TLS provides a high level of security for sessions between an Ethernet connected client application and server application with no prior knowledge of each other and without any prior exchange of encryption keys. A mutually trusted third party (the CA, or Certificate Authority) is used to certify that the client and server are the owners of their respective private and public key pairs used in establishing the communication session.

This trusted environment provides:

1. Authentication - the server may authenticate itself to the client (typically a browser), or the client and server may mutually authenticate themselves to each other.

2. Privacy - the communications traffic is encrypted.

3. Integrity assurance - using hash and signature algorithms.

ℹ Note that TLS works between applications. This means that both communicating applications must be TLS-enabled, rather than the host and client devices. Proxies can be implemented to allow non-TLS-enabled applications to be used over a TLS-protected link; here, the authentication is from/to the proxy rather than the application.

4.3.2   How TLS Works

The process for setting up a TLS session can be summarized as follows:

1. Both the client and server have their own private (secret) and public keys.

2. The public keys are certified by Certificate Authorities (CAs).

3. The public key certificates can include multiple, chained CA hierarchies - e.g., the public key can be certified by one CA (e.g., operated by the organization owning the key), and this CA certificate is then certified by a higher-level CA (e.g., a third-party CA trusted by both the key owner and the key user).

4. The client and server can use different CAs.

5. The client and server applications negotiate which cipher suite they will use, and exchange some information (but not keys) that will be needed to establish the session. The cipher suite defines the algorithms and key lengths that will be used to establish and protect the session.

6. The client and server applications exchange certificates (including their public keys).

7. The client and server validate each other's certificate and extract the public key. The validation may be performed by contacting the CA online or by using previously stored CA materials.

8. The client application sends an encrypted "Pre-master" secret to the Server application.

9. Server and client applications both independently compute a Master secret from the Pre-master secret and use this to calculate the symmetric keys to be used to protect the exchanged data. The keys therefore do not need to be exchanged.

10. Following a successful client-server handshake, the application data is exchanged in records, with the data encrypted using the independently computed keys, and MAC'd using the hashing algorithm in the agreed cipher suite.

The following diagram illustrates this, with some additional detail:

Client

Server

Supported algorithms, random number

Chosen algorithms, random number, session ID

X.509 certificate

Verify Certificate

X.509 certificate

Verify Certificate

Calculate Pre-master Secret, computed from random numbers.

Pre-master Secret. Encrypted with Server public key.

Certificate Verify – signature over previous messages.

Verify Certificate Verify

Compute Master Secret from Pre-master Secret & Random Nos. Used to calculate symmetric keys

Compute Master Secret from Pre-master Secret & Random Nos. Used to calculate symmetric keys

Authenticated/encrypted "Finished" message

Verify

Authenticated/encrypted "Finished" message

Verify

Exchange authenticated/encrypted data

——— Plaintext   ——— Encrypted

4.3.3   TLS Support

The payShield 10K supports TLS v1.2. (PCI DSS v3.1 recommends the use of this protocol.)

The payShield 10K can simultaneously support TLS and non-secured (TCP or UDP) traffic. It is possible to disable all TLS or non-secured traffic.

4.3.4   Supported Cipher Suites

The payShield 10K supports the following TLS cipher suites.

Cipher Suite Name	Protocols	Algorithms		
		Asymm	Symm	Hash
ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS v1.2	ECDSA	AES 256-bit GCM	SHA-384
ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS v1.2	ECDSA	AES 256-bit CBC	SHA-384
ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS v1.2	ECDSA	AES 128-bit GCM	SHA-256
ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS v1.2	ECDSA	AES 128-bit CBC	SHA-256
DHE_RSA_WITH_AES_256_GCM_SHA384	TLS v1.2	RSA 2048-bit	AES 256-bit GCM	SHA-384

Cipher Suite Name	Protocols	Algorithms		
		Asymm	Symm	Hash
DHE_RSA_WITH_AES_256_CBC_SHA256	TLS v1.2	RSA 2048-bit	AES 256-bit CBC	SHA-256
DHE_RSA_WITH_AES_128_GCM_SHA256	TLS v1.2	RSA 2048-bit	AES 128-bit GCM	SHA-256
DHE_RSA_WITH_AES_128_CBC_SHA256	TLS v1.2	RSA 2048-bit	AES 128-bit CBC	SHA-256

4.3.5   Cipher Suite Negotiation

The Cipher Suites in the table above are listed in decreasing order of preference by the payShield 10K. When negotiating Cipher Suites, the HSM's preferences will take precedence over the client's preferences.

Ephemeral key cipher suites are preferred by the payShield 10K. When selected, every new handshake will require new ephemeral keys to be generated; this provides perfect forward secrecy such that if an attacker should ever break the cryptography being used for a connection, then this will be of no use to the attacker in a subsequent connection. All of the cipher suites, except the last in the above table, use ephemeral keys.

When performing a renegotiation of an existing connection, the payShield 10K will always force a new session to be negotiated; this protects against a known renegotiation vulnerability.

4.3.6   Data compression

Connections will not use data compression, protecting against the CRIME vulnerability.

4.4   Configuring TLS on the payShield 10K

The following sections discuss the use of the following console commands and payShield Manager actions to configure the payShield 10K to use TLS.

Operation	Console Command
Check Availability of TLS	VR
Configure Ethernet host ports	CH
Generate HRK	SK
Change HRK Passphrase	SP
Restore HRK	SL
Generate/Export TLS Server Certificate Signing Request	SG
Export Server (HSM) CA	SE
Import Signed Certificate	SI
Viewing Certificates held on the HSM	SV
Delete Certificate	SD

4.4.1 Checking availability of TLS

The VR console command will report on the availability of TLS on the payShield 10K. The start of the output will consist of the following information:

ℹ In the following example output, text in bold+underscore represents inputs made by the user.

Row	Dialogue
1	**VR**
2	`Base release: 1.0d`
3	`Revision:      1500-0020`
4	`Build Number: 0058`
5	`Base Version:    1.2.4`
6	`Deployment Version:  1.2.4`
7	`PCI HSM Compliance:` `Some security settings are not PCI HSM compliant`
8	`Serial Number: S0246376952J`
9	`Model:    PS10-S`
10	`Power supply #1:` `     Serial number:  XQ1823RE1929`
11	`Power supply #1:` `     Serial number:  XQ1823RE1698`
12	`Fan #1:` `      Warning – Serial Number Not Detected`
13	`Fan #2:` `Serial number:  FM01161900022`
14	`Unit info:            Licensed`
15	`Host Configuration: .Ethernet, <optional> TLS/SSL`

The element relevant to configuring TLS:

Row 15: the availability of TLS is indicated in the "Host Configuration" information.

ℹ The example above reflects non-PCI compliant settings. A PCI compliant example would reflect:

```
Base release:        1.0d
Revision:            1500-1020
Build Number:        0064
Base Version:        1.2.5
Deployment Version: 1.2.5


PCI HSM Compliance:
```

```
Refer to the PCI web site
(https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_tr
ansaction_security.php) for current certification status of this version of
payShield 10K software.
Security settings are consistent with the requirements of PCI HSM.
```

4.4.2   Working with IBM z/OS Mainframes

Users who have payShield 10K units working with IBM z/OS host systems should make use of the AT-f feature in z/OS. Contact Thales Support (https://www.thalesesecurity.com/support) for assistance.

Relevant information is also available on the IBM website:
https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.gska100/toc.htm).

4.5   Managing Certificates

Console commands are available to manage the HSM, application, and CA certificates required to establish TLS sessions.

When using the payShield Manager, refer to the payShield 10K Installation and User Guide for further instruction.

4.5.1   HSM Certificates

The key pair for the HSM is created by the HSM.

An unencrypted copy of the private key is held in tamper-protected memory, and the HRK-encrypted copy is held in non-volatile memory.

It is important to note that both the encrypted and unencrypted copies of the HRK are held within the payShield 10K tamper protected physical boundary.

The HSM generates a Certificate Signing Request (CSR) containing its public key in PKCS#10 format, and outputs this to the console and, if attached, to a USB memory device. A security officer will generate a certificate signed by their chosen CA and return the public key certificate and CA's certificate chain to the HSM.

The key pair for the HSM is created by the HSM.

An unencrypted copy of the private key is held in tamper-protected memory, and the HRK-encrypted copy is held in non-volatile memory.

The HSM generates a Certificate Signing Request (CSR) containing its public key in PKCS#10 format, and outputs this to the console and, if attached, to a USB memory device. A Security Officer will generate a certificate signed by their chosen CA and return the public key certificate and CA's certificate chain to the HSM.

Note: If the host computer applications are using a different CA than the payShield, the payShield's CA certificate also needs to be imported by the security officers to the applications.
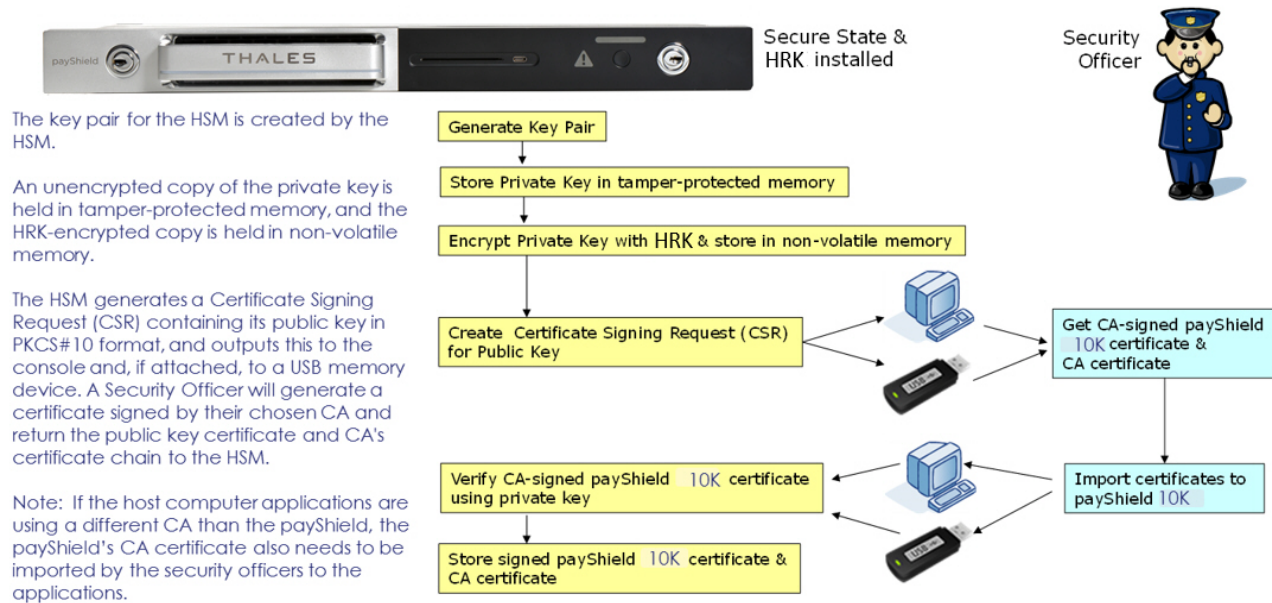
If the host computer applications are using a different CA to the HSM, the HSM's CA certificate also needs to be imported by the security officers to the applications.

Intermediate CA certificates can be included to a maximum certificate chain depth of 6, and must include the X509 v3 optional extensions of Subject Key Identifier and Authority Key Identifier. The signed HSM (server) certificate must include the Authority Key Identifier extension.

4.5.2   Application Certificates

Each application that wishes to establish a secure communications session using TLS needs to provide to the payShield 10K a public key in the form of a certificate signed by a CA (or by a hierarchy of CAs). The way that this certificate is obtained depends on the standard procedures of the organization and its selected CA mechanism.

The application certificates and their associated CA chain certificates are imported by the security officer into the HSM using the console, or a USB memory device.

The set of client endpoint certificates forms an effective "White List" of applications that are entitled to use the HSM through Secure Host Communications. This is used by the payShield 10K to mitigate against "man-in-the-middle" attacks.

Intermediate CA certificates can be included to a maximum certificate chain depth of 6, and must include the X509 v3 optional extensions of Subject Key Identifier and Authority Key Identifier. The signed application (client) certificate must include the Authority Key Identifier extension.

4.5.3   Out-of-Date Certificates

If an attempt to establish a Secure Host Communications session is made using an out-of-date (i.e., expired or not yet valid) certificate, the connection fails. As a result, it is important for users to have suitable processes in place to manage certificate introduction and expiry.

As an option, users can audit attempts to use out-of-date certificates.

ℹ The certificates accepted by the payShield are required to be in UTC 24-hour format.

4.5.4   Support for USB Memory Sticks

USB memory sticks are used to transfer material such as certificates in and out of the payShield 10K. The Operating System used in the payShield 10K supports most types of USB memory sticks, but may not have the drivers for some of the newer types. If difficulties are experienced when trying to read from or write to a USB device, an alternative memory stick should be used.

4.6   Generate and Export TLS Server Certificate Signing Request

This process generates the HSM key pair, stores the private key in tamper-protected memory and (in HRK-encrypted form) in non-volatile memory, and creates a Certificate Signing Request for the public key.

On the console, this is done by using the SG command while the HSM is in Secure state:

Row	Dialogue
1	**SG**
2	Please enter the Subject Information for the Certificate Request:
3	Country Name (2 letter code) [US]: **US**
4	State or Province Name (full name) []: **Texas**
5	Locality Name (e.g., city) []: **Austin**
6	Organization Name (e.g., company) []: **Banking Corporation**
7	Organizational Unit Name (e.g., section) []: **CorpSecurity**
8	Common Name (e.g., server FQDN or YOUR name) []: **HSM1**
9	Email Address []: **owner@bankingcorp.com**
10	Select key type:
11	1 - RSA
12	2 - ECDSA P-256
13	3 - ECDSA P-384
14	4 - ECDSA P-521
15	Type [4]: **1**
16	Generating key pair
17	....+++
18	...+++
20	DONE
21	Do you wish to save to a file [Y/N]:**y**

Row	Dialogue
22	Enter filename: **HSM1**
23	File exists - replace? [Y/N]:**y**
23	-----BEGIN CERTIFICATE REQUEST-----
25	MIIC9zCCAd8CAQAwgbExCzAJBgNVBAYTAlVLMRgwFgYDVQQIEw9CdWNraW5naGFt . . . . ehNJSXN703d6vP2aktV3VRHkMvbrkjqT37dU3chCaqkOYOqEMhnCEMdVGw==
26	-----END CERTIFICATE REQUEST-----

Notes:

Rows 10-15: The key type is selected. If RSA is used, the key is of 2048-bit length.

Rows 11: The RSA is 2048-bit key length.

Rows 11-14: The client certificate must use the same key type as is used in the HSM's Certificate Signing Request.

Rows 21-23: The certificate can be saved to a file - e.g., on a USB memory device - to allow it to be exported.

Rows 23-25: The certificate signing request is also displayed on the screen.

4.6.1   Export HSM Certificate's Chain of Trust

The CA certificate used by the HSM must be made available to the host applications. It can be exported using the SE console command while the HSM is in Secure state:

Row	Dialogue
1	**SE**
2	Do you wish to save to a file [Y/N]:**y**
3	Enter filename: **CACertpS10K.crt**
4	payShield Certificate
5	MIID+TCCAuGgAwIBAgIJAJyPxxP6oxAQMA0GCSqGSIb3DQEBBQUAMIGyM . . . X4FkYiQv2CJb7J/vAw==
6	-----END CERTIFICATE-----

Notes:

Rows 2-3: The certificate can be saved to a file - e.g., on a USB memory device - to allow it to be exported.

4.6.2   Import Signed Certificate

Following the certificate signing request, the signed certificate for the HSM's public key needs to be imported. It is also necessary to import:

1. All signed certificates for applications.

2. Self-signed certificate for the root CA.

3. Where a chained CA hierarchy is being used, certificates for each intermediate CA signed by the next CA up in the hierarchy.

On the console, this is done using the SI command while the HSM is in Secure state:

Row	Dialogue
1	<u>SI</u>
2	Select File
3	1 - RsaServerRootCA.crt
4	2 - TCPUDPSIM.crt
5	3 - RsaClientRootCA.crt
6	4 - hsm1.crt
7	File: <u>1</u>
8	Imported Trusted CA Certificate
9	Issued to: payShield Certificate, Issued by: payShield Certificate
10	Validity : May 9 10:59:22 2013 GMT to May 7 10:59:22 2023 GMT
11	Unique ID: 9C8FC713FAA31010 - AC03FAD5 (Root)
12	Do you wish to import another certificate? <u>n</u>

Notes:

Rows 3-6, in this example, identify files available on a USB memory device attached to the HSM. The user identifies at Row 7 which of these is to be imported.

The user is informed if no certificates are found on the USB memory device.

4.6.3   Viewing certificates held on the HSM

The payShield 10K establishes TLS sessions only with applications for which it has stored a copy of their certificate. All stored certificates (including the payShield's own certificate and CA certificates) can be viewed using the SV console command:

Row	Dialogue
1	<u>SV</u>
2	HSM Private Key installed: Yes
3	HSM Certificate installed:
4	1 - Issued to: HSM-0002, Issued by: Bank XYZ
5	Validity : May 21 15:05:51 2013 GMT to May 21 15:05:51 2014 GMT
6	Unique ID: 2050 - AC03FAD5
7	Client certificate(s) installed:
8	2 - Issued to: Client Certificate, Issued by: Client Certificate
9	Validity : May 7 09:37:18 2013 GMT to May 7 09:37:18 2014 GMT

Row	Dialogue
10	Unique ID: 2016 - D221289A
11	CA Certificate(s) installed:
12	3 - Issued to: Client Certificate, Issued by: Client Certificate
13	Validity : May 7 09:24:10 2013 GMT to May 5 09:24:10 2023 GMT
14	Unique ID: C14FF9DE78FB441A - D221289A (Root)
15	4 - Issued to: payShield Certificate, Issued by: payShield Certificate
16	Validity : May 9 10:59:22 2013 GMT to May 7 10:59:22 2023 GMT
17	Unique ID: 9C8FC713FAA31010 - AC03FAD5 (Root)
18	Chain of Trust validated:
19	payShield Certificate (Root)
20	Select an item to view: **1**
21	Certificate:
22	Data:
23	Version: 3 (0x2)
24	Serial Number: 8273 (0x2051)
25	Signature Algorithm: sha1WithRSAEncryption
26	Issuer: C=UK, ST=Greater London, L=London, O=Bank XYZ, OU=RootCA, CN=Bank XYZ/emailAddress=root@bankxyz.com
27	Validity
28	Not Before: May 21 15:05:51 2013 GMT
29	Not After : May 21 15:05:51 2014 GMT
30	Subject: C=UK, ST=Greater London, O=Bank XYZ, OU=Operations, CN=HSM-0002/emailAddress=bill@bankxyz.com
31	Subject Public Key Info:
32	Public Key Algorithm: rsaEncryption
33	Public-Key: (2048 bit)
34	Modulus:
35	00:aa:31:e6:90:46:fe:e9:26:8b:93:39:5a:8c:be:
36	…
37	3d:39:2b:d7:06:47:04:6a:54:d2:12:4e:ac:9a:a3:
38	5b:49
39	Exponent: 65537 (0x10001)
40	X509v3 extensions:
41	X509v3 Basic Constraints:
42	CA:FALSE

Row	Dialogue
43	`        X509v3 Key Usage:`
44	`            Digital Signature, Non Repudiation, Key Encipherment`
45	`    Signature Algorithm: sha1WithRSAEncryption`
46	`        b8:e9:e9:8f:2e:f9:50:93:a1:8b:8d:0b:e5:fd:ef:6f:6c:05:`
47	`        …`
48	`        59:0d:df:85:b7:48:c6:02:d9:16:f9:80:e5:c9:c2:69:7f:06:`
49	`        2b:ba:18:9f`
50	`Do you wish to view another certificate? `**`N`**

Notes:

Row 20: The number for the required certificate as offered in rows 4, 8, 12, and 15 should be entered.

4.6.4   Delete Certificate

Where it is no longer required to establish TLS connections with an application or where a certificate has been withdrawn or updated, it is necessary to delete the certificate stored on the payShield 10K. This can be achieved using the SD console command while the HSM is in Secure state:

Row	Dialogue
1	**`SD`**
2	`HSM Private Key installed: Yes`
3	`HSM Certificate installed:`
4	`    1 - Issued to: HSM1, Issued by: payShield Certificate`
5	`        Validity : May 20 08:51:27 2013 GMT to May 20 08:51:27 2014 GMT`
6	`        Unique ID: 204D - AC03FAD5`
7	`Client certificate(s) installed:`
8	`    2 - Issued to: Client Certificate, Issued by: Client Certificate`
9	`        Validity : May  7 09:37:18 2013 GMT to May  7 09:37:18 2014 GMT`
10	`        Unique ID: 2016 - D221289A`
11	`CA Certificate(s) installed:`
12	`    3 - Issued to: Client Certificate, Issued by: Client Certificate`
13	`        Validity : May  7 09:24:10 2013 GMT to May  5 09:24:10 2023 GMT`
14	`        Unique ID: C14FF9DE78FB441A - D221289A (Root)`
15	`    4 - Issued to: payShield Certificate, Issued by: payShield Certificate`
16	`        Validity : May  9 10:59:22 2013 GMT to May  7 10:59:22 2023 GMT`
17	`        Unique ID: 9C8FC713FAA31010 - AC03FAD5 (Root)`
18	`Chain of Trust validated:`

Row	Dialogue
20	`        payShield Certificate (Root)`
21	`    5 - HSM Private Key`
22	`Select an item to delete (6 for ALL): `**`6`**
23	`Do you wish to delete another certificate? `**`n`**

4.6.5   Auditing attempted use of out-of-date certificates.

Users can choose to record, in the payShield 10K's Audit Log, any attempts made to establish a Secure Host Communications session using an out-of-date certificate. This option is enabled/disabled using the AUDITOPTIONS console command:

Row	Dialogue
1	**`AUDITOPTIONS`**
2	`Audit User Actions: NO`
3	`Audit Error Responses to Host Commands: NO`
4	`Audit utilization data resets: NO`
5	`Audit diagnostic self tests: NO`
6	`Audit ACL connection failures: YES`
7	`Audit out-of-date Certificates for Secure Host Sessions: NO`
8	`Audit Counter Value:` `0000005A`
9	`List of Audited Console Commands:`
10	`List of Audited Host Commands:`
11	`Audit User Actions? [Y/N]: `**`n`**
12	`Audit Error Responses to Host Commands? [Y/N]: `**`n`**
13	`Audit Utilization Data Resets? [Y/N]: `**`n`**
14	`Audit Automatic Self Testing? [Y/N]: `**`n`**
15	`Audit ACL connection failures? [Y/N]: `**`n`**
16	`Audit out-of-date Certificates for Secure Host sessions? [Y/N]: `**`y`**
17	`Current Audit Counter value is: 0000005A`
18	`Enter new value or <Return> for no change:`
20	`Modify Audited Command List? [Y/N]: `**`n`**
21	`Audit User Actions: NO`
22	`Audit Error Responses to Host Commands: NO`
23	`Audit utilization data resets: NO`
24	`Audit diagnostic self tests: NO`
25	`Audit ACL connection failures: NO`

Row	Dialogue
26	Audit out-of-date Certificates for Secure Host Sessions: YES
27	Audit Counter Value: 0000005A
28	List of Audited Console Commands:
29	List of Audited Host Commands:
30	Save Audit Settings to Smartcard? [Y/N]: n

The resulting audit log entries will be of the following formats:

```
0000002F  10:25:22  02/Jul/2016  Certificate has expired.
Unique ID: A8F66A587213303F - 2BA3B089

00000027  22:24:33  02/Jul/2014  Certificate not yet valid.
Unique ID: A8F66A587213303F - 2BA3B089
```

4.7   Certificate Examples

4.7.1   Intermediate CA Certificate

```
Intermediate CA Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 762114 (0xba102)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=Florida, L=Plantation,
                CN=RsaClientRootCA.thalesesec.com
        Validity
            Not Before: Jul 10 18:55:49 2013 GMT
            Not After : Jul 10 18:55:49 2014 GMT
        Subject: C=US, ST=Florida, CN=RsaClientIntCA1.thalesesec.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b0:2d:f9:ce:ba:b1:40:f5:c2:43:1d:3f:bd:a1:
                    2e:e6:5b:73:f3:0c:ed:ce:de:71:80:2a:dc:ca:3a:
                    0e:b7:8a:82:56:86:80:1c:65:b2:47:6f:0d:77:d7:
                    78:db:d3:51:e4:32:50:5e:cf:ae:05:7b:a4:5f:c2:
                    d2:90:d5:70:63:b4:6a:56:a4:c5:4c:2e:1d:47:f0:
                    59:b6:10:f4:c9:46:1e:9c:db:43:43:80:76:aa:40:
                    78:fe:23:73:ab:c1:1e:15:8b:7a:e1:66:b5:57:3b:
                    bf:d0:3a:e6:7d:ed:32:c2:21:fc:57:7b:b1:62:51:
                    bc:d7:38:8f:4e:df:76:cc:5a:c3:5a:ca:75:2c:86:
                    e6:fc:82:b6:5e:fd:c8:14:ca:f2:c6:9b:c8:33:58:
                    9b:fd:90:ea:ec:b6:77:0e:fe:12:35:be:89:b3:68:
                    6e:69:46:5c:03:8c:41:5f:c3:d3:99:58:d5:35:7a:
                    88:41:ce:50:7e:5a:a2:ff:28:36:73:86:61:94:23:
                    24:69:86:5c:73:31:60:ee:b8:ad:d4:fe:3c:b8:65:
                    50:35:49:6d:08:9a:2b:d4:26:b6:97:1c:ba:d1:c2:
                    c3:fe:4b:bf:4b:27:be:d6:57:d7:97:37:10:23:f1:
                    4d:33:5b:41:d7:8e:55:bf:9a:76:05:50:5d:8f:f0:
                    ef:43
                Exponent: 65537 (0x10001)
```

```
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:TRUE
        X509v3 Subject Key Identifier:
            DE:C0:02:1B:48:37:6B:C3:34:F5:9E:D0:8A:32:12:5E:ED:1C:50:2C
        X509v3 Authority Key Identifier:
            keyid:08:20:EB:E6:51:CF:7F:08:D3:9D:33:A4:DC:48:AE:2E:5D:6C:
                  F3:EC

Signature Algorithm: sha1WithRSAEncryption
    4b:07:e2:e2:90:60:0a:dc:29:56:bb:65:8b:9a:62:3c:a0:70:
    22:0c:8c:fe:2f:7b:9f:46:9a:ac:fb:6b:f7:e4:4a:d5:54:b4:
    c9:46:97:e3:82:d7:66:ed:5d:e6:24:e8:8c:b8:8b:86:0c:82:
    bf:00:e3:6c:73:bc:27:0b:aa:02:07:f9:10:1d:9a:fc:2e:7e:
    34:6d:74:6a:90:73:14:8a:ba:81:77:74:66:01:e5:da:4d:54:
    ed:18:c5:f7:7d:e4:62:24:ec:f6:80:86:b3:56:43:ec:d5:48:
    90:fd:a4:28:e5:89:7f:60:a9:a9:a7:67:3c:cd:f1:22:7b:0e:
    dd:16:a8:09:a8:6e:0e:97:a8:26:cc:94:fb:95:a2:1f:8e:83:
    ee:6c:6d:f7:f4:ec:fe:2b:bd:bf:ce:a8:5f:f2:6f:92:89:80:
    f0:41:83:89:56:3e:9a:47:e0:24:28:6a:fd:69:05:a7:6a:fd:
    66:4e:2d:35:69:54:4c:00:8b:52:3c:26:f1:8a:35:82:e3:d4:
    b8:f8:09:e6:0e:6f:3b:3a:c6:9c:f5:23:c6:5e:9c:00:fa:90:
    21:aa:4c:fa:fd:84:bf:87:55:b9:a1:0e:d8:82:92:07:79:08:
    9b:49:fd:89:3d:c1:f4:61:ba:c0:9a:ac:e3:d5:75:ec:3a:51:
    c5:70:59:23
```

4.7.2   Client Certificate

```
Client Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 762369 (0xba201)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=Florida, L=Plantation,
            CN=RsaClientRootCA.thalesesec.com
        Validity
            Not Before: Jul 16 21:34:50 2013 GMT
            Not After : Jul 16 21:34:50 2014 GMT
        Subject: C=US, ST=Florida, CN=RSAClient.thalesesec.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:f6:26:4d:61:3d:62:22:62:44:59:57:f0:60:a4:
                    a0:63:c0:2a:24:a3:45:d5:2c:c2:1b:2c:70:f7:2d:
                    29:da:48:af:cd:17:b2:5b:05:08:dd:b6:27:5e:d6:
                    f7:e6:a7:56:df:d5:e6:07:e6:dd:4f:2a:68:58:60:
                    4d:e2:08:8d:ee:04:e0:d2:29:35:36:0c:8b:38:88:
                    f3:ea:9a:2e:35:f6:3d:b9:73:99:53:f1:0f:76:10:
                    74:10:19:9d:02:71:49:0b:0c:29:e4:af:91:f5:ac:
                    73:0c:d2:e0:7c:d8:b1:d3:0b:72:94:6b:6b:9b:f1:
                    c1:6e:22:5e:ee:77:d0:40:3c:cd:2a:cc:82:83:a6:
                    af:c3:b6:d9:b5:9b:85:c3:b3:00:64:f1:50:5a:f1:
                    88:c0:3b:f2:c7:d0:c2:d2:76:bf:9f:5c:7a:f4:a4:
                    7c:8e:c7:ab:a0:2b:dc:69:c3:95:51:f4:73:ad:ac:
                    a3:32:85:a1:15:79:d6:d0:e1:be:a7:00:33:60:1c:
                    21:90:7c:2b:9e:e1:09:13:fa:de:fd:31:90:db:6d:
                    89:f8:f4:e7:a4:b0:0b:c4:d5:e4:f3:67:20:e1:17:
                    4a:65:3a:f0:08:57:4b:85:a2:3c:1f:17:cd:a3:3a:
                    01:3c:e0:d2:39:27:de:38:53:3e:e7:43:09:58:21:
```

```
              95:f7
        Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Key Usage:
            Digital Signature, Key Agreement
        X509v3 Authority Key Identifier:
                keyid:08:20:EB:E6:51:CF:7F:08:D3:9D:33:A4:DC:48:AE:2E:5D:
                6C:F3:EC

Signature Algorithm: sha1WithRSAEncryption
    78:e5:d2:5f:cd:03:8e:65:e3:40:7d:9c:25:15:41:ed:da:67:
    7d:d4:86:cb:7c:84:75:e4:3a:36:a0:ec:a1:28:ba:7d:37:ba:
    b3:2f:48:f4:0e:24:56:e1:df:0e:f9:cf:8c:7f:b7:bc:57:99:
    6c:de:c9:30:3b:47:12:d0:be:c9:f9:d4:c3:87:c0:e6:36:b4:
    7a:e1:fa:8e:51:32:fb:6a:fd:08:87:93:ab:3b:67:42:a7:1d:
    a8:46:07:04:4a:5a:ad:a6:b6:60:89:7a:50:e1:8d:48:97:af:
    8b:e1:98:8b:f2:3a:26:a6:cf:c6:a7:18:36:ff:9c:05:95:3a:
    b2:a3:88:61:02:d8:31:df:bc:97:77:9c:e7:ce:33:65:20:f0:
    27:0c:2e:db:b5:d2:ab:82:3d:c3:d4:c5:2b:29:82:b4:21:d1:
    48:ed:eb:ff:56:14:34:c9:62:99:cd:7b:73:c9:93:01:3d:d2:
    a8:37:5f:0d:4a:2f:56:1d:d0:57:95:f8:7c:aa:f7:5e:bb:09:
    1e:7c:74:81:be:b4:1e:03:a3:e5:1a:bc:ba:7a:04:02:57:b5:
    00:1f:f8:32:29:74:1b:5d:f1:96:b8:f9:3e:f3:02:bb:dc:de:
    4e:35:43:cd:4e:80:a3:60:69:a2:47:97:7a:2e:e4:0f:f3:d3:
    b1:22:76:40
```

4.8   Considerations When Using TLS

4.8.1   Performance considerations

For payShield 10K, there is no noticeable difference in performance when implementing Secure Host Communications.

4.8.2   Security considerations

TLS can only provide a secure environment when implemented correctly. When implementing TLS on the payShield 10K, the guidance in the latest version of PCI's Data Security Standards (DSS) requirements should be followed.

4.8.3   OpenSSL Configuration File

Where OpenSSL is being used to provide TLS support on the host system, the configuration file must contain the following:

```
[ v3_client ]

basicConstraints      = CA:FALSE
#extendedKeyUsage      = clientAuth
keyUsage              = keyAgreement, digitalSignature
authorityKeyIdentifier = keyid,issuer

[ v3_server ]

basicConstraints      = CA:FALSE
```

```
extendedKeyUsage        = serverAuth
keyUsage                = keyAgreement, keyEncipherment,
                                    digitalSignature, nonRepudiation
authorityKeyIdentifier = keyid,issuer


[ v3_ca ]


basicConstraints        = CA:true
subjectKeyIdentifier    = hash
authorityKeyIdentifier = keyid,issuer
```

4.8.3.1   Notices

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.
(*http://www.openssl.org/*)

This product includes cryptographic software written by Eric Young (*eay@cryptsoft.com*)

4.9   Configuring the Ethernet Ports

The CH (Configure Host) console command allows the Ethernet ports to be configured for TLS. The following example shows a payShield 10K being configured for a single physical Ethernet port:

Row	Dialogue
1	**CH**
2	Please make a selection. The current setting is in parentheses.
3	Message header length [1-255] (4):
4	Host interface [[A]sync, [E]thernet] (E):
5	Enter Well-Known-Port (1500):
6	Enter Well-Known-TLS-Port (2500):
7	UDP [Y/N] (Y):
8	TCP [Y/N] (Y):
9	Enable TLS [Y/N] (Y):
10	Number of connections [1-64] (5):
11	Enter TCP keep alive timeout [1-120 minutes] (120):
12	Number of interfaces [1/2] (1):
13	Interface Number [1/2] (1):
14	Interface Number 1:
15	Enter IP Address (193.240.100.216): **193.240.100.215**
16	Enter subnet mask (255.255.255.0):
17	Enter Default Gateway Address (193.240.100.1):
18	Save HOST settings to smart card? [Y/N]: **n**

The following elements are relevant to configuring TLS:

Row 6: A well-known port must be specified for TLS - the default is 2500. This is analogous to the well-known port for unsecured host traffic (Row 5), and can be used in the same way to identify the LMK required for the host command, i.e.:

- o 2500 = default LMK
- o 2501 = LMK 0
- o 2502 = LMK 1
- o etc.

Row 7 and 8: Enable or disable non-secured host traffic (TCP or UDP).

Row 9: Enable or disable secured host traffic.

Row 10: Specifies the number of connections/threads for each port. If a value of 5 was entered and both Ethernet ports were enabled, a total of 10 connections/threads would be available. These connections/threads are shared between secured and non-secured traffic.

The QH (Query Host) console command used to view the port settings has been modified to display the new parameters.

4.10   HSM Recovery Key (HRK)

The HSM Recovery Key (HRK) is used to encrypt the HSM's private key used by the HSM in establishing the TLS session.

The HRK-encrypted private key is held outside of the tamper-protected memory such that if the HSM detects a tamper event it is not lost; the unencrypted private key used during live running is held in tamper-protected memory and is lost if the HSM detects a tamper event. The private key can therefore be recovered after a tamper event, once the HRK is installed, by decrypting the encrypted version.

The HRK is generated by the HSM using 2 passphrases entered by security officers. These passphrases must be provided to reconstitute the HRK when recovering the private key after a tamper event. It is held in tamper-protected memory such that it is automatically erased if the HSM detects an attempted tamper.

The HRK also enables recovery of the private key for the payShield Manager CA.

4.10.1   Managing the HRK

The HRK can be managed using console commands or payShield Manager functions.

Refer to the *payShield 10K Installation and User Guide* for additional information.

4.10.1.1   Generate HRK

The HRK is generated using the SK console command while the HSM is in Secure state:

Row	Dialogue
1	SK
2	**** NOTE ****
3	Passphrase rules as follows:
4	1 - Must be between 8 and 30 characters long.
5	2 - Can contain spaces
6	3 - Must be comprised of (at a minimum):
7	2 digits
8	2 uppercase characters

Row	Dialogue
9	2 lowercase characters
10	2 symbols (ex. !/?.#:')
11	Enter administrator 1 passphrase: ********************
12	Re-enter administrator 1 passphrase: *******************
13	Enter administrator 2 passphrase: *************
14	Re-enter administrator 2 passphrase: *************
15	Creating HRK. Please, wait ... DONE
16	HRK generated successfully
17	Key synchronisation complete

Notes:

Rows 11-14: Two different passphrases are required, each entered by a different security officer. These passphrases must be stored securely (in the same way as key components) to allow subsequent HRK recovery in the event that the HSM enters a tampered state.

Rows 3-10: The passphrases must be of an acceptable complexity. Spaces are allowed.

4.10.1.2 Change HRK Passphrase

The HRK passphrase should be changed regularly as a best security practice, and will need to be changed if a security officer is replaced by another person. This is accomplished using the SP console command while the HSM is in Secure state:

Row	Dialogue
1	SP
2	**** NOTE ****
3	Passphrase rules as follows:
4	1 - Must be between 8 and 30 characters long.
5	2 - Can contain spaces
6	3 - Must be comprised of (at a minimum):
7	2 digits
8	2 uppercase characters
9	2 lowercase characters
10	2 symbols (ex. !/?.#:')
11	4 - Cannot use the same passphrase that was used within the past 10 previous attempts
12	Select administrator password to change [1,2]: 1
13	Enter administrator 1 current passphrase: ********************
14	Enter administrator 1 new passphrase: ************
15	Re-enter administrator 1 new passphrase: ************
16	Changing passphrases. Please, wait ... DONE
17	HRK generated successfully

Notes:

Rows 11-14: Two different passphrases are required, each entered by a different security officer. These passphrases must be stored securely (in the same way as key components) to allow subsequent HRK recovery in the event that the HSM enters a tampered state.

Rows 3-10: The passphrases must be of an acceptable complexity. Spaces are allowed.

A Passphrase cannot be re-used until at least 10 generations of passphrase changes have been made.

4.10.1.3   Restore HRK

If the HSM detects a tamper event, its private key used to establish TLS sessions is deleted. An HRK-encrypted copy of the private key is held in non-volatile memory, and the key itself can be recovered and restored to tamper-protected memory by entering the passphrases used at HRK generation into the SL console command while the HSM is in Secure state:

Row	Dialogue
1	`SL`
2	`Enter administrator 1 passphrase: ********************`
3	`Enter administrator 2 passphrase: **************`
4	`Recovering HRK. Please, wait ... DONE`
5	`HRK recovered successfully`
6	`Key synchronization complete`

4.11   Access Control Lists (ACLs)

Another host communications security feature, although not directly associated with the Secure Host Communications facility, is the ability to set up whitelists of acceptable host IP addresses using Access Control Lists (ACLs). See the *payShield 10K Installation and User Guide* for information on setting up ACLs.

5   Secure 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.

ℹ️ 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.

5.1   Verifying the Contents of the LMK Store

The LMKs installed in the HSM should be checked periodically.

ℹ️ The payShield is in the Secure state.

To display the current LMKs installed in the Local Master Key table and Key Change Storage table using payShield Manager,

- Navigate to: **Summary > Local Master Key**
- The system displays both tables.

Local Master Key

Local Master Key Table

ID	AUTH	SCHEME	ALGORITHM	STATUS	CHECK	COMMENTS
0	No	Variant	3DES(2key)	Test	268604	Thales test variant
1	No	KeyBlock	3DES(3key)	Test	165126	Thales test keyblock
2	No	KeyBlock	AES-256	Test	9D04A0	Thales test AES
3	No	KeyBlock	AES-256	Live	6A4309	rlmk

Key Change Storage Table

ID	OLD/NEW	SCHEME	ALGORITHM	STATUS	CHECK	COMMENTS

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.

To inspect a smartcard using payShield Manager:

- Select the card icon.

☑ Change PIN
☑ Inspect Smart Card
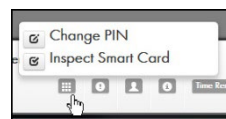
- The system displays two options.
- Select **Inspect Smart Card**
- The smart card details page displays.

ℹ (The **V** and **NC** console commands provide the equivalent functionality.)

5.2   Loading the Test Keys

It is a 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.

Customers are provided with a means to generate three test LMK cards.

ℹ The payShield is in the Secure state.

To generate and install a test LMK using payShield Manager,

- Navigate to: **Operational > LMK Operations**
- Select **Generate**
- Expand **Generate LMK** and select **Generate Standard Thales Test LMK**
- Select the type from the drop down – follow prompts
- Select **Generate LMK** – follow prompts
- Select **Install** – follow prompts
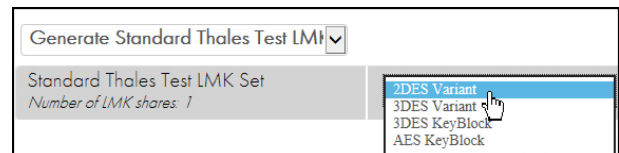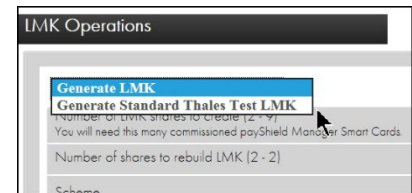
ℹ (The **LK** console command provides the equivalent functionality.)

Refer to the *payShield 10K Installation and User Guide* and to the *payShield 10K Host Programmer's Manual* for additional information regarding loading and managing LMK cards.

6 The Audit Log

6.1 Introduction

The payShield 10K provides an audit logging capability, enabling security officers to select a number of activities and functions whose usage is recorded in an audit log. Certain items are always recorded in the Audit Log, and this cannot be disabled.

The purpose of the Audit Log is to enable security officers to make regular checks on security-related actions that the payShield 10K is being asked to perform, and to assist in forensic examination of any suspected security breaches.

The Audit Log also provides facilities for its entries to be viewed, printed, and archived to a host computer.

This chapter describes the capabilities and usage of the payShield 10K Audit Log.

With Semantic Versioning changes in 1.0e, there is a change to the firmware upgrade audit log.

When upgrading from 1.0d to 1.0e, the following audit log is generated:

0000000141 13:38:54 12/Mar/2020 Firmware update to 1500.0021.0000 (uboot 0001.0001.0040) successful

Note that the above log is generated by the 1.0d firmware prior to the reboot and revision number is used for the audit log.

With 1.0e and later, the audit log is generated using the firmware version with 1.0e and later.

6.2 Overview

The Audit Log is held securely in non-volatile memory in the payShield 10K; it survives power cycling, payShield 10K restarts, tamper attempts, and software upgrades.

It always records certain events and use of functions. In addition, security officers can elect to log other events and functions.

The Audit Log can be viewed, printed, erased, and retrieved or archived to a host computer. It can record 100,000 items. When the audit log is filled, the earliest entry is deleted to allow the most recent entry to be added. It is therefore important that entries are archived to a host computer frequently enough such that the Audit Log does not get filled. The frequency with which this needs to be performed will depend on how many items are being recorded.

A message authentication code (MAC) is associated with each individual audit entry, enabling easy detection of any fraudulent attempt to modify the audit record.

6.3 Correct Use of the Audit Log

The audit log has been designed to capture information which will be examined when investigating any potential security issues; it is not intended for use as a general log of what the HSM is being used for, for example by logging all host commands (which can impact on performance). Audit Log entries should be reviewed at regular and frequent intervals to allow:

- Any necessary actions to be taken
- Any records that need to be retained for future reference to be printed or archived to the host system
- The Audit Log to be cleared

ℹ️ It is important that the Audit Log is kept as small as possible to optimize performance. It is particularly important that the Audit Log is not allowed to reach its maximum size.

Logging high-frequency events which correspond to normal usage of the HSM and which have no significance in terms of security introduces a number of problems:

- Creating too many records to allow significant records to be found and interpreted
- Causing loss of audit records if the audit log capacity is exhausted before the audit records have been archived
- Negatively impacting performance, because of the additional processing required to create and record audit records, especially when the audit log capacity is exhausted and the log needs to be "rotated" (i.e., the oldest record deleted to allow the new record to be added).

It is recommended that as few host commands as possible are audited; error responses to host commands may well be indicative of a security threat, and the audit options allow such responses to be logged without having to audit normally executing host commands.

6.4   Forcibly recorded items

A number of items are always recorded in the Audit Log; this cannot be disabled.

6.5   PCI HSM Compliance:

Most of these forcible recorded items were introduced to meet requirements of PCI HSM certification. These items are:

- Use of smartcards to authenticate users to the payShield 10K or payShield Manager. The serial number of the smartcard is recorded as part of the Audit Log record.
- Use of the A and C console commands to initiate and cancel authorization of activities. The Audit Log entry shows for how long the activity was authorized.
- Use of the following console commands or the equivalent payShield Manager actions. The Audit Log records made in this way will indicate the successful completion of the command:

Console Command	
CV	Generate a Card Verification Value
FK	Form Key from Components
IK	Import a Key
LK	Load LMK
LO	Load 'Old' LMK into Key Change Storage

Console Command	
LN	Load 'New' LMK into Key Change Storage
PV	Generate a Visa PIN Verification Value
UPLOAD	Upload new firmware/license
BK	Form a Key from Components
D	Form a ZMK from Encrypted Components
DE	Form a ZMK from Clear Components
IV	Import a CVK or PVK

6.6 Recording Deletion of Audit Log

The Audit Log will include a record to indicate that the Audit Log has been erased.

6.7 Discretionary Audit Log entries

It is possible to request that any of the following events are recorded in the Audit Log:

- Use of combination of any console commands or payShield Manager actions. The Audit Log records made in this way will indicate the initiation of the command rather than its successful completion. This is different to the way that a forcibly audited command would be recorded, where the successful completion of the command/action is recorded.

Auditing activity on host ports:

- Use of any desired selection of host commands. As discussed, this facility should be used carefully to avoid logging of high volumes of host commands which are executing normally; it is generally better to log just error responses, as these may well be indicative of a security issue.
- Receipt of an error response to a host command
- Failures to establish host connections arising from the Access Control List (ACL)
- Attempts to use out-of-date certificates when trying to establish Secure Host Communication sessions

User actions:

- Clearing of Audit Log
- Loading an LMK or an Old/New LMK
- Erasing an LMK or an Old/New LMK
- Loading a license file - successful
- Loading a license file - failed
- Change of state
- Power cycle
- Resetting of Utilization Data
- Results of automatic daily self-tests – indicating whether the tests were successful or identifying any specific tests that failed

6.8   Protection of the Audit Log

The payShield 10K provides a number of features specifically aimed at protecting the Audit Log:

- Each Audit Log record is MAC'd using a unique MACing key protected by the LMK. A host command is available to allow the MAC to be verified at a later time.

- Audit log entries can be archived by printing to a printer attached to the payShield 10K

- Audit Log entries can be retrieved to the host system for secure electronic archiving

- Console actions to configure or delete the Audit Log require Authorization using the Management LMK. Equivalent actions on payShield Manager require Security Officers to be logged on.

- Host Commands to delete Audit Log records must be authorized

- Deletion of the Audit Log always results in a record of this event being added into the otherwise now blank Audit Log.

7 Shipping and Product Handling

This section describes Thales' understanding of the PCI HSM Version 3.0 standard and its impact on shipping and receipt by the user.

Thales is not qualified to provide advice on PCI standards and so readers must make their own judgements as to proper courses of action to take or discuss their intentions with a PCI QSA.

This section also provides suggestions as to how users should manage the payShield 10K after it has been delivered to them. The PCI HSM standard is not explicit in this area, but certain clarifications have been received and are included in the information provided below.

Warning: The information in this section is not intended to constitute security or standards compliance advice and should not be relied upon in lieu of consultation with appropriate technical security and audit compliance advisors in your own area of operations.

7.1 Responsibilities

Any organization, which is involved in arranging the shipping (whether for the whole journey, or a "leg" of a multi-part journey) of an HSM which is to be PCI HSM compliant, must ensure that the shipping is conducted in a manner which is compliant with the requirements of the PCI HSM standard as described here in.

The table below outlines a number of common delivery scenarios and shows which party has responsibility for which section of the payShield 10K's journey. It is important to understand that Thales' resellers are distinct organizations from Thales, and that Thales does not have responsibility for the shipping "legs" organized by the resellers.

Scenario	Responsible party	Extent of reesponsibility
Thales arranges shipping from manufacturing facility direct to end user	Thales Manufacturing Facility	Complete journey, until receipt of payShield 10K is signed for by the end user.
Thales arranges shipping from its manufacturing facility to a Thales regional office, and that Thales regional office arranges shipping to the end user.	Thales Manufacturing Facility	Up to receipt of payShield 10K by the Thales regional office.
	Thales regional office	From receipt of the payShield 10K until receipt of the payShield 10K by the end user.
Thales arranges shipping from its manufacturing facility to another Thales regional office, then that Thales	Thales Manufacturing Facility	Up to receipt of payShield 10K by the Thales regional office.
	Thales regional office	From receipt of the payShield 10K until receipt of the payShield 10K by the reseller.

Scenario	Responsible party	Extent of reesponsibility
regional office arranges shipping to a reseller, and the reseller arranges shipping to the end user.	Thales reseller	From receipt of the payShield 10K until receipt of the payShield 10K by the end user.
Thales arranges shipping from its manufacturing facility to a reseller, and that reseller arranges shipping to the end user.	Thales Manufacturing Facility	Up to receipt of payShield 10K by the Thales reseller.
	Thales regional office	From receipt of the payShield 10K until receipt of the payShield 10K by the end user.
Reseller arranges collection of payShield 10K from Thales manufacturing facility and then onward-ships to the end user.	Thales reseller	Complete journey, until receipt of payShield 10K is signed for by the end user.
End user arranges collection of payShield 10K from Thales manufacturing facility.	End user	Complete journey.

The PCI HSM standard discusses delivery of the HSM to the "facility of initial deployment". (The version 1.0 requirements used the term "initial key loading facility".) It does not explicitly place any requirements on the end user where the point of receipt by the end user organization is not the place where the first LMK will be loaded. However, Thales recommends that the end user organization implements the controls described later in this section.

7.2   PCI shipping requirements

The requirements that the PCI HSM standard makes for shipping of payment HSMs can be found in the document:

> *Payment Card Industry (PCI) Hardware Security Module (HSM) Security Requirements Version 3.0*

> in the section entitled:

> Device Security Requirements Between Manufacturer and Initial Key Loading.

This document can be found on the PCI web site at the following URL:

https://www.pcisecuritystandards.org/security_standards/documents.php?association=PTS

For reference, the v1.0 requirements can be found at:

https://www.pcisecuritystandards.org/documents/PCI%20HSM%20Security%20Requirements%20v1.0%20final.pdf .

8 Information for Security Auditors

8.1 Certifications

8.1.1 FIPS 140-2

The TASP (Thales Advanced Security Platform – the secure cryptographic module in the payShield 10K) is undergoing certification at Level 3 of the FIPS 140-2 security standard.

For all vendors' HSMs being used for card payment and issuance applications, the HSM's application software is not included in the certification and the HSM is operating outside of its FIPS certificate when performing any payment card functions. This information is included in the Security Policy associated with each HSM's FIPS certificate.

See: Section 8.2 *References*.

8.1.2 PCI HSM

payShield 10K hardware and specific software versions are undergoing certification to the PCI HSM Version 3 standard. Any customized software must be separately certified, as it is not covered by the certification for the base software that it is based on.

The certificate identifies specific hardware and software (i.e., firmware) versions which are covered by the certificate.

See: Section 8.2 *References*.

8.1.3 APCA (Australian Payments Clearing Association)

The payShield 10K and specific versions of base software are undergoing approval by APCA. When approved, the hardware and software (firmware) can be found on the APCA website.

See: Section 8.2 *References*.

ℹ️ The operation of the payShield 10K as an APCA-compliant device is described in *the payShield 10K Host Command Reference Manual*.

8.1.4 MEPS (Methode d'Evaluation des Produits Securitaire "bancaires")

Products intended for use on the banking networks in France are submitted for evaluation by Groupement des Cartes Bancaires. This involves the submission of detailed design documentation and other information about the security mechanisms implemented. The payShield 10K with a modified version of software is undergoing certification by MEPS. Users needing information about MEPS approval should approach their Thales representative or authorized partner.

8.1.5   GBIC (German Banking Industry Committee) / ZKA (Zentraler Kreditausschuss)

GBIC was formerly referred to as ZKA. Systems processing German domestic cards must be approved under GBIC. There is no certification process for individual components such as HSMs, but these components are evaluated as part of the system. Successful evaluation of an HSM for one system applies only to that system and is not transferrable to another system: the HSM must be re-evaluated for each system which is to be certified.

The payShield 10K is undergoing evaluation as part of a number of systems.

8.2   References

Follow the links in the table below to find additional support documentation.

To find:	Link	Notes
FIPS certificate	https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search	National Institute of Standards and Technology (NIST) Computer Security Resource Center
PCI HSM Version 3	https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss	PCI Security Standards Council
APCA IAC Approved devices list	http://pub1.apca.com.au/ExtraNet/CS3AppDevices.nsf/wApprovedSeries?open&count=2000&restrictToCategory=SECURITY%20CONTROL%20MODULES	Scroll down the displayed page to locate Thales
OpenSSL Project	http://www.openssl.org/	For use in the OpenSSL Toolkit

9 Appendix A - Security Recommendations

9.1 Introduction

This appendix 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.

9.2 Procedural Security

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

9.2.1 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 is important to check that the first entries in the AUDITLOG correspond exactly with the last time the AUDITLOG was cleared. It is also important to check that each change to the Secure state was in support of a legitimate activity.

9.2.2   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.

9.2.3   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, then activities that are not being used MUST NOT be authorized.

9.2.4   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.

9.2.5 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.

9.2.6 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.

9.3 Command Security

There are a number of standard features provided by the payShield 10K 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. In the payShield 10K, host commands are disabled by default. Use the CONFIGCMDS console command to enable only those commands necessary for operation of the HSM.

2. Use CONFIGCMDS Console command to disable all unused Console commands.

3. Use CONFIGPB Console command to disable all unused PIN block formats.

4. Use Multiple Authorized Activities instead of the global Authorized state, thus permitting specific authorized commands, rather than all authorized commands.

5. All Authorized Activities SHOULD be time limited to reduce the risk of abuse.

6. 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'.

9.4 Measures to Protect HSM Secure Area

The figure below shows an HSM, printer, and console in a "secure area with limited access". The Host Computer and the 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).
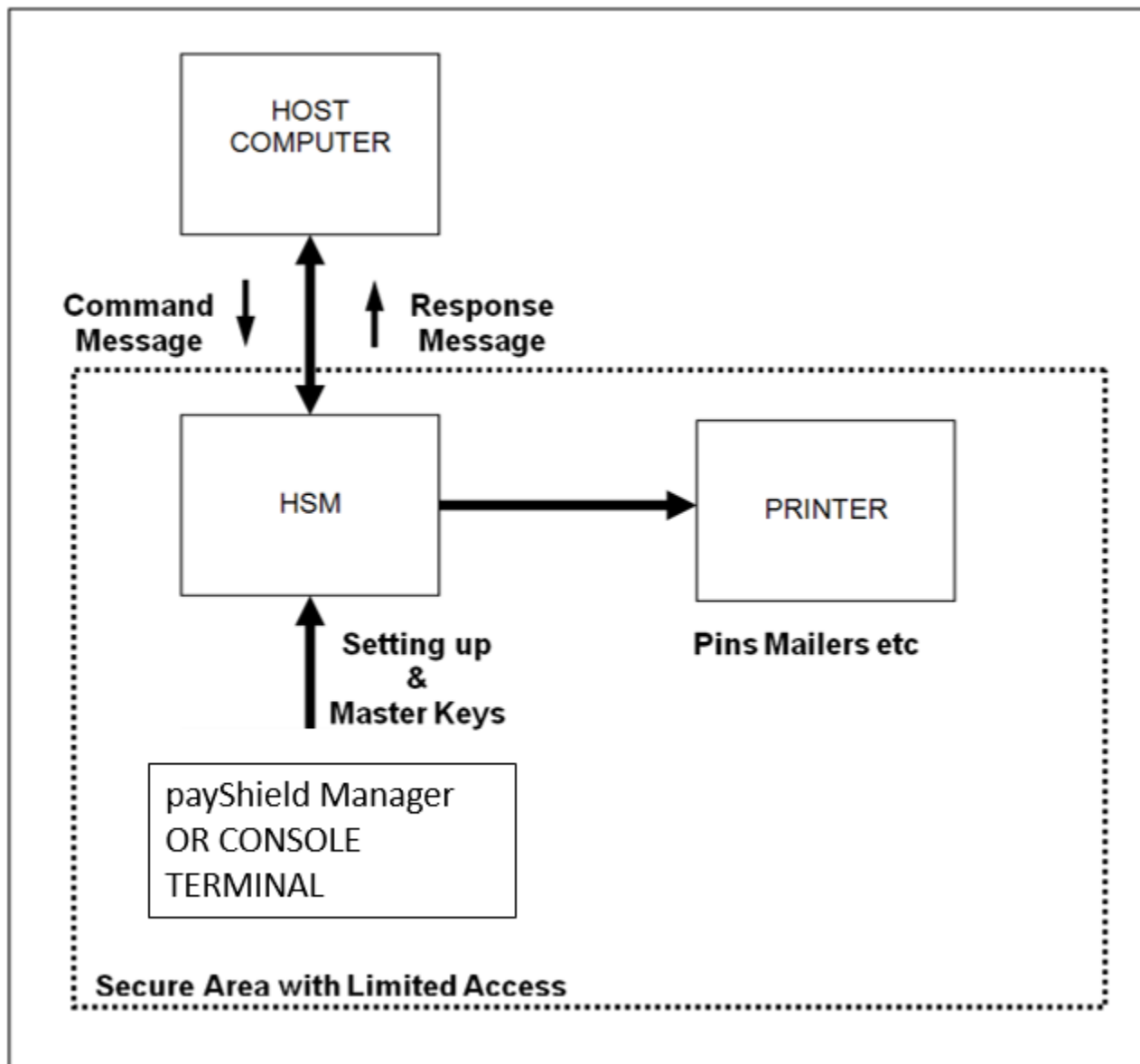
Recommendations for the HSM secure area are as follows:

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 an 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).

9.5 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.

9.6 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.

9.7 Local payShield Manager Functions

payShield Manager users should refer to the *payShield 10K Installation and User Guide* for additional information, as needed.

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

Refer to the relevant *payShield 10K Installation and User Guide* 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.

9.8　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.

9.8.1　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.

9.8.2　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, 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.

9.8.3   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.

9.8.4   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
   - Do not contain dictionary words
   - Do not use spouse's/children's names
   - Do not 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.

9.8.5   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.

ℹ 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.

9.8.6   Physical Key Security

The payShield 10K 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.

9.8.7   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 Medium 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. (See Appendix A.)

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

The HRK is generated securely within each HSM using payShield Manager or 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 recovers the Secure Host Communications and Remote Management key material.

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 provided in the *payShield 10K Installation and User Guide*.

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 (in Appendix A) **Error! Reference source not found.**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.

9.9   HSM Integrity

9.9.1   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.

9.9.2 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 <u>NOT</u> 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.

9.9.3 HSM Maintenance

The HSM contains a long-life battery that can be replaced only by Thales at their premises.

1. HSM maintenance and repair, other than replacement of FRU components, 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 ERASE button.

6. Before an HSM is given to Thales for maintenance, follow the relevant instructions in the payShield 10K 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.

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

9.10   Normal Operations

These measures are applicable while the HSM is being held or used within the users Secure Area. If a functional HSM is to leave the Secure Area, this is considered to be a maintenance activity, e.g., the LMK SHOULD be deleted or replaced by the Test LMK.

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

1. When the HSM is to have an online connection to the host application it MUST be locked in position and put into the Online state.

2. When the HSM contains an LMK, the motion alarm SHOULD be enabled.

3. The payShield 10K temperature sensor is always enabled.

4. 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.

5. Only host commands required for operations SHOULD be enabled, and Host commands not required for operations MUST be disabled.

6. 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.

7. 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.

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

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

10. 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.)

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

12. All online HSMs MUST be subject to regular monitoring, particularly with respect to the management of any HSM where the "Health" LED is illuminated red, or the "Tamper" LED has become illuminated.

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

9.10.1   Timely Return to the Online State

The device MUST NOT be left 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.

9.11   Inspection Procedures

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

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

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

3. The results of each step of the inspection procedures MUST be recorded.

9.11.1 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.

9.11.2 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.

9.11.3 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. 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 "Health" and "Tamper" LEDs.

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 "Health" LED to be illuminated red. When looking for evidence of tampering, consideration should be given to the possibility that the tamper-evident lid has been opened 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 results in a High Tamper that is unrecoverable and the unit should be removed from operation and destroyed or returned to Thales.

Remark: The inspection should check that the tamper lid is still intact and that the lid has not been drilled into.

The HSM's diagnostic test console DT command, as described in the *payShield 10K 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 10K Installation and User Guide* to perform the equivalent functions.

1. The HSM's self test console ST command, as described in the *payShield 10K Console Reference Manual*, MUST confirm that the self tests are running at the expected time.

ⓘ Users of payShield Manager should refer to the *payShield 10K Installation and User Guide* to perform the equivalent functions.

2. The HSM VR Console command, as described in the *payShield 10K Installation and User Guide, Appendix A,* 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/approved_pin_transaction_security.php) for current certification status of this version of payShield 10K software.

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

ⓘ Users of payShield Manager should refer to the payShield 10K Installation and User Guide to perform the equivalent functions.

3. 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.
4. 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.

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

10 Appendix B - Error Log Codes

10.1 General

The Error Log lists each error with a severity, an error code and a sub-code. The Error Log only contains the numerical part of the error code and sub-code. Sub-codes relate to a specific error code.

This Appendix describes the Error Log as viewed when using the Console. When viewing the Error log using payShield Manager please refer to the payShield Manager User's Guide.

The text below will make use of the following example of an error log entry:

```
1: Nov 30 00:43:18  ERROR: [Tamper(1) Latched at [2000/00/00, 00:42:57]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
```

10.2 Description

The error description is contained within a pair of square brackets:

```
1: Nov 30 00:43:18  ERROR: [Tamper(1) Latched at [2000/00/00, 00:42:57]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
```

The meaning of some of these descriptions will be obvious, for example:

```
[Power Supply:   FAILED (PSU 2 Failed) ]
```

whereas the full meaning of some messages will require interpretation by Thales.

10.3 Severity

A severity level is provided by the error message:

```
1: Nov 30 00:43:18  ERROR: [Tamper(1) Latched at [2000/00/00, 00:42:57]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
```

The meaning of the severity level is given in the following table:

No.	Code	Meaning
0	LOG_EMERG	System is unusable.
1	LOG_ALERT	Action must be taken immediately.
2	LOG_CRIT	Critical conditions.
3	LOG_ERR	Error conditions.
4	LOG_WARNING	Warning conditions
5	LOG_NOTICE	Normal but significant condition.
6	LOG_INFO	Informational.
7	LOG_DEBUG	Debug-level message.

10.4   Error Codes

The error log entry includes a main error code:

```
1: Nov 30 00:43:18  ERROR: [Tamper(1) Latched at [2000/00/00, 00:42:57]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
```

The main error code indicates the general source of the error, as per the following table:

No.	Shown as …	Code	Meaning
1	0x00000001	LS_UTIL	Utility system
2	0x00000002	LS_CRYPTO	Cryptographic system
3	0x00000003	LS_APP	Application system
4	0x00000004	LS_KEYMGR	Key Manager system
5	0x00000005	LS_ENCFS	Encrypted File System

10.5   Sub-Codes

The error log entry also includes a sub-code to provide a more detailed source of the error:

```
1: Nov 30 00:43:18  ERROR: [Tamper(1) Latched at [2000/00/00, 00:42:57]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)
```

The value of sub-codes depends on the value of the main error code, as described in the tables below. A value of *0x00000000* indicates that a more detailed sub-code is not appropriate.

10.5.1   Sub-Codes for Main Error Code = 1 (Utility System Errors)

No.	Shown as …	Sub-code	Meaning
1	0x00000001	LSS_UTIL_CONFIG	Configuration utility sub-system
2	0x00000002	LSS_UTIL_UNUSED	Deprecated (was Encrypted File utility sub-system)
3	0x00000003	LSS_UTIL_I2C	I2C utility sub-system
4	0x00000004	LSS_UTIL_INCOMINGD	Incoming daemon utility sub-system
5	0x00000005	LSS_UTIL_LED	LED utility sub-system
6	0x00000006	LSS_UTIL_NAMESPACE	Namespace utility sub-system
7	0x00000007	LSS_UTIL_PATCH	Program patch utility sub-system
8	0x00000008	LSS_UTIL_PROC	Process manager utility sub-system
9	0x00000009	LSS_UTIL_PSHAPE	Performance shaping utility sub-system

No.	Shown as …	Sub-code	Meaning
10	0x0000000A	LSS_UTIL_SMARTCARD	Smartcard utility sub-system
11	0x0000000B	LSS_UTIL_SPARTAN	Spartan FPGA management utility sub-system
12	0x0000000C	LSS_UTIL_SWITCH	User switch (push-button & keylock) utility sub-system
13	0x0000000D	LSS_UTIL_SYSID	System ID utility sub-system
14	0x0000000E	LSS_UTIL_UPDATER	System update utility sub-system
15	0x0000000F	LSS_UTIL_SHMEM	Shared memory utility sub-system
16	0x00000010	LSS_UTIL_LICENSING	License management utility sub-system
17	0x00000011	LSS_UTIL_SCR	Smartcard Reader utility sub-system
18	0x00000012	LSS_UTIL_EEPROM	Resident configuration utility sub-system
19	0x00000013	LSS_UTIL_MEM	Memory utility sub-system
20	0x00000014	LSS_UTIL_EVENT	Event manager utility sub-system
21	0x00000015	LSS_UTIL_THREADPOOL	Thread-pool manager utility sub-system
22	0x00000016	LSS_UTIL_COOKIE	Cookie manager

10.5.2 Sub-Codes for Main Error Code = 2 (Cryptographic System Errors)

No.	Shown as …	Sub-code	Meaning
1	0x00000001	LSS_CRYPTO_DES	DES cryptographic sub-system
2	0x00000002	LSS_CRYPTO_RNG	Random number generator cryptographic sub-system
3	0x00000003	LSS_CRYPTO_SHA	SHA cryptographic sub-system
4	0x00000004	LSS_CRYPTO_SEC	Security engine cryptographic sub-system
5	0x00000005	LSS_CRYPTO_RMAPI	Resource management API cryptographic sub-system
6	0x00000006	LSS_CRYPTO_RM_SEC	Resource management security engine cryptographic sub-system
7	0x00000007	LSS_CRYPTO_RM_SW	Resource management software cryptographic sub-system
8	0x00000008	LSS_CRYPTO_RSA	RSA cryptographic sub-system

No.	Shown as …	Sub-code	Meaning
9	0x00000009	LSS_CRYPTO_BIGINT	Big integer cryptographic sub-system
10	0x0000000A	LSS_CRYPTO_ESS	ESS API cryptographic sub-system
11	0x0000000B	LSS_CRYPTO_AES	AES cryptographic sub-system
12	0x0000000C	LSS_CRYPTO_HASH	Hash cryptographic sub-system

10.5.3 Sub-Codes for Main Error Code = 3 (Application System Errors)

No.	Shown as …	Sub-code	Meaning
1	0x00000001	LSS_APP_DIAG	Diagnostic application sub-system
2	0x00000002	LSS_APP_AUTH	Authorization application sub-system
3	0x00000003	LSS_APP_LMK	LMK application sub-system
4	0x00000004	LSS_APP_COMMS	Communications (TCP, UDP, Async, FICON) application sub-system
5	0x00000005	LSS_APP_GENERAL	General application sub-system
6	0x00000006	LSS_APP_AUDITLOG	Audit log application sub-system
7	0x00000007	LSS_APP_CONFIG	Configuration application sub-system
8	0x00000008	LSS_APP_CONSOLE	Console application sub-system
9	0x00000009	LSS_APP_HOSTCMD	Host command application sub-system
10	0x0000000A	LSS_APP_PINBLOCK	PIN block application sub-system
11	0x0000000B	LSS_APP_USRSTORE	User storage application sub-system
12	0x0000000C	LSS_APP_CHIPCARD	Chip card application sub-system
13	0x0000000D	LSS_APP_DES	DES application sub-system
14	0x0000000E	LSS_APP_FRAUD	Fraud application sub-system
15	0x0000000F	LSS_APP_KEYBLOCK	Key Block application sub-system
16	0x00000010	LSS_APP_KEYMAN	Key manager application sub-system

No.	Shown as ...	Sub-code	Meaning
17	0x00000011	LSS_APP_MAC	MAC application sub-system
18	0x00000012	LSS_APP_MGMT	payShield Manager application sub-system
19	0x00000013	LSS_APP_PARSE	Parsing application sub-system
20	0x00000014	LSS_APP_PRINT	Printing application sub-system
21	0x00000015	LSS_APP_RSA	RSA application sub-system
22	0x00000016	LSS_APP_VISA	Visa application sub-system
23	0x00000017	LSS_APP_VPN	VPN for remote management application sub-system
24	0x00000018	LSS_APP_X509CERT	X.509 certificate application sub-system
25	0x00000019	LSS_APP_STATE	System state application sub-system
26	0x0000001A	LSS_APP_POWER	Power management application sub-system
27	0x0000001B	LSS_APP_STORAGE	Storage application sub-system
28	0x0000001C	LSS_APP_COMMANDS	Command processing application sub-system
29	0x0000001D	LSS_APP_DIGEST	Digest application sub-system
30	0x0000001E	LSS_APP_LICENSE	Licensing application sub-system
31	0x0000001F	LSS_APP_UTILIZATION	Utilization application sub-system
32	0x00000020	LSS_APP_SNMP	SNMP application sub-system

10.5.4 Sub-Codes for Main Error Code = 4 (Key Manager System Errors)

There are currently no sub-codes.

10.5.5 Sub-Codes for Main Error Code = 5 (Encrypted File System Errors)

There are currently no sub-codes.

10.6 Multiple Entries

A single cause may result in multiple entries being made in the error log. The following example arises from a triggering of the temperature alarm, which initiates a tamper condition:

```
PayShield 10K Error Log

----------------------

1: Nov 30 00:43:18  ERROR: [Tamper(1) Latched at [2000/00/00, 00:42:57]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)

2: Nov 30 00:43:18  ERROR: [Tamper Latched State [LR1 = 0x0004, LR2 = 0x0000]] (Severity:
2, Code = 0x00000004, Sub-Code = 0x00000000)

3: Nov 30 00:43:18  ERROR: [   Tamper LR1 [0x0004 = Temperature exceeded maximum
operational range]] (Severity: 2, Code = 0x00000004, Sub-Code = 0x00000000)

4: Nov 30 00:43:18  ERROR: [Tamper Current State [CR1 = 0x0004, CR2 = 0x8000]] (Severity:
2, Code = 0x00000004, Sub-Code = 0x00000000)

5: Nov 30 00:43:40  ERROR: [Tamper(2) Latched at [2000/00/00, 00:43:19]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)

6: Nov 30 00:43:41  ERROR: [Tamper Latched State [LR1 = 0x0004, LR2 = 0x0000]] (Severity:
2, Code = 0x00000004, Sub-Code = 0x00000000)

7: Nov 30 00:43:41  ERROR: [   Tamper LR1 [0x0004 = Temperature exceeded maximum
operational range]] (Severity: 2, Code = 0x00000004, Sub-Code = 0x00000000)

8: Nov 30 00:43:41  ERROR: [Tamper Current State [CR1 = 0x0004, CR2 = 0x8000]] (Severity:
2, Code = 0x00000004, Sub-Code = 0x00000000)

9: Nov 30 00:43:41  ERROR: [   Tamper CR1 [0x0004 = Temperature exceeded maximum
operational range]] (Severity: 2, Code = 0x00000004, Sub-Code = 0x00000000)

10: Nov 30 00:43:41  ERROR: [   Tamper CR2 [0x8000 = DS3640 TEI asserted]] (Severity: 2,
Code = 0x00000004, Sub-Code = 0x00000000)

11: Nov 30 00:43:41  ERROR: [Tamper State is 0x0004 and retry count exceeded (2)]
(Severity: 2, Code = 0x00000004, Sub-Code = 0x00000000)

12: Nov 30 00:43:47  ERROR: [Temperature:     FAILED - temperature too high ] (Severity:
3, Code = 0x00000001, Sub-Code = 0x0000000E)
```

The messages show that a tamper event occurred and is still ongoing. The value of "0x0004" for the LR1 and CR1 elements indicate that the tamper cause was the temperature rising above the maximum acceptable level; a value of "0x0002" would have indicated a temperature that was too low.

11 Appendix C – payShield Manager Recommendations Background

payShield Manager is a web-based product that allows communication with, and management of, a payShield 10K unit over a wide area network. As such, it permits "remote" users to perform almost all console activity without requiring physical access to the HSM.

In order to provide secure communications between a remote user and an 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 10K and the currently authenticated remote management smartcards.

11.1.1 Remote Management States

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

11.1.2 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.

11.1.2.1   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 is 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 10Ks that support payShield Manager. All user interaction with the CTA functionality is via either the HSM's console interface or the payShield Manager.

11.1.2.2   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.

11.1.2.3   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 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.

11.2   PayShield Manager Best Practice

11.2.1 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.

11.2.2 Assumptions

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

11.2.2.1   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.

11.2.3 Personnel

An individual responsible for the overall operation and security of 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 payShield Manager.

9. All users SHOULD sign affidavits stating that they understand their roles and responsibilities with respect to 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, payShield Manager, or by physically destroying the card.

11.2.4 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.

11.2.5 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

11.2.6 Physical Security

Many payShield Manager activities are extremely sensitive and need to be carried out in a secure environment. In particular, compromising 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 10K 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 10K for payShield Manager, to avoid a possible man-in-the-middle attack, the network connection between the payShield 10K and the management client MUST be trusted;

ℹ The recommended method of achieving this is to connect to the payShield 10K locally.

ℹ **IMPORTANT:** 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 payShield Manager MUST NOT be brought into the Operations Room. Such equipment includes, e.g.,: data analyzers, cameras, cell phones, 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.

11.2.7   HSM Security Configuration

1. HSM configuration is described in the *payShield 10K Installation and User Manual*, 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 10K Installation and User Manual*, this may impact HSM performance and so the extent of auditable activity SHOULD be reviewed from time to time.

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.

11.2.8   Customer Trust Authority

The *Customer Trust Anchor* (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 10K Installation and User Manual*.

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 10K Installation and User Manual*.

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.

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".

Note that 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.

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. 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:

   o PINs SHOULD be at least 8 digits in length
   o PINs SHOULD be randomly generated
   o "obvious" PINs MUST NOT be chosen (e.g., "12345678" or "99999999")
   o 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).

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.

11.2.9 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.

ⓘ 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:
   o   PINs MUST be at least 8 digits in length
   o   "random" PINs SHOULD be chosen
   o   "obvious" PINs MUST NOT be chosen (e.g. "12345678" or "99999999")
   o   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).

11.2.10 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).

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.

11.2.11 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 10K Installation and User 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.

11.2.12 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.

11.2.13 Operational Security

Details of payShield Manager operations are given in *payShield 10K Installation and User 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.

12 Appendix D –TLS Security Recommendations

12.1 Background

The payShield 10K allows for secure host communications via the TLS protocol. These connections are secured using a Public Key Infrastructure (PKI) trust system.

12.1.1 payShield 10K TLS Server

The payShield 10K provides the TLS server for secure host communications. To enhance the security of the connections, the server has been configured with options described in the sections that follow.

12.1.2 Protocol Support

The TLS server only supports the TLS v1.2 protocol.

12.1.3 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.

12.1.4 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.

12.1.5 Man-In-The-Middle Mitigation

The payShield 10K 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 10K 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).

12.1.6 TLS Clients

The payShield 10K 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 10K 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.

12.1.7 Client Mitigations

The payShield 10K 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 10K.

Technical Support Contacts

Our team of knowledgeable and friendly support staff are available to help. If your product is under warranty or you hold a support contract with Thales, do not hesitate to contact us using the link below. For more information, consult our standard Terms and Conditions for Warranty and Support.

https://supportportal.thalesgroup.com/csm

THALES