cpl.thalesgroup.com

payShield® 10K

Installation and User Guide

PUGD0535-006

Date: January 2021

Doc. Number: PUGD0535-006, updated 15 January 2021

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as “Thales”) information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

• The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

• This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Follow this link to find the End User Licensing Agreement: https://cpl.thalesgroup.com/legal/eula

Contents

1 Introduction 1-9
1.1 Documentation Overview 1-9
1.2 Audience 1-9
1.3 payShield 10K General Description 1-9
1.4 Typical Configuration. 1-10
1.4.1 Command Flow 1-11
1.5 Smart cards. 1-11
1.6 Customer Trust Authority (CTA) 1-12
1.6.1 Customer Security Domain 1-13
1.7 Keys 1-13
1.7.1 Encryption Mechanism. 1-13
1.7.2 HSM Recovery Key 1-13
1.7.3 Local Master Keys (LMKs). 1-14
1.7.3.1 Multiple LMKs 1-14
1.7.4 Zone Master Key 1-15
1.7.4.1 Zone PIN Key 1-15
1.7.5 Terminal Master Key 1-15
1.7.5.1 Terminal PIN Key 1-15
1.7.6 Terminal Authentication Key 1-15
1.7.7 Terminal Encryption Key 1-16
1.7.8 PIN Verification Key. 1-16
1.7.9 Card Verification Key 1-16
1.7.10 Master Session Key 1-16
1.8 Key Shares 1-16
1.9 Host Commands supporting multiple LMKs 1-17
1.9.1 LMK Usage in Host Commands. 1-18
1.10 payShield 10K license packages. 1-19
1.11 Trusted Management Device (TMD). 1-21
1.11.1 Introduction. 1-21
1.11.2 Background 1-21
1.11.3 Description 1-21
1.11.4 How Keys Are Shared With payShield and 3rd Parties 1-22
1.11.5 Example Sequence of Steps to Set-Up and Transfer Keys 1-23

2 Backwards Compatibility and Differences. 2-25
2.1 payShield 9000 / payShield 10K 2-25
2.1.1 Host Interface and Commands. 2-25
2.1.2 Options for Managing payShield 10K. 2-26
2.1.3 Modifications made to the console commands 2-26
2.1.4 Feature Comparison. 2-27
2.1.5 Front Panel. 2-29
2.1.6 Front Panel LEDs. 2-29
2.1.7 Front Panel Key Lock Positions 2-29
2.1.8 Rear Panel 2-30
2.1.9 Enhanced Security Features 2-30
2.1.10 Diagnostics. 2-31
2.1.11 Monitoring. 2-31
2.1.12 Transitioning Smart Cards 2-31
2.1.12.1 Transitioning legacy Manager Smart Cards 2-32

2.1.12.2 Transitioning non-supported legacy HSM Smart Cards 2-33
2.1.12.3 Copying a card at the console 2-33
2.1.13 User Documentation 2-33

3 Physical Description 3-35
3.1 Front panel 3-35
3.1.1 Key locks and keys 3-35
3.1.1.1 Changing the HSM state via the key locks 3-35
3.1.2 Smart Card Reader 3-36
3.1.3 Front panel LEDs 3-36
3.1.3.1 Health LED 3-37
3.1.3.2 Service LED 3-37
3.1.3.3 Tamper LED 3-38
3.1.3.4 Boot-up LED Sequence 3-38
3.1.3.5 Blue LED 3-38
3.1.4 Air Inlets 3-38
3.2 Rear panel 3-39
3.2.1 AC/DC power supplies 3-39
3.2.1.1 Swapping out the Power Supply 3-39
3.2.2 Fan trays 3-40
3.2.3 Battery 3-40
3.2.4 AC Power on/off switch 3-41
3.2.5 PCIe card interface 3-41
3.2.6 Ethernet ports 3-41
3.2.7 USB Type A port 3-41
3.2.8 Erase Button and LED 3-41
3.2.9 Ground Lug 3-41

4 Installation 4-43
4.1 Pre-installation tasks 4-43
4.1.1 Mechanical and Electrical Specifications 4-43
4.1.1.1 Physical Characteristics 4-43
4.1.1.2 Power Considerations 4-43
4.1.1.3 Environmental Considerations 4-44
4.1.1.4 Battery consideration 4-44
4.2 Installation Procedure 4-44

5 payShield 10K 10G Ethernet Hardware Platform Variant 5-49
5.1 Introduction 5-49
5.2 Rear Panel Overview 5-50
5.3 General Notes 5-50
5.4 Installing 10Gb ports 5-50
5.5 Power Consumption 5-51

6 payShield Management Options 6-53

7 Commission using payShield Manager 7-55
7.1 Introduction 7-55
7.2 Prerequisites 7-55
7.3 Preparing for Commissioning 7-55
7.3.1 Configuring payShield 10K for Static IP (if required) 7-55
7.3.2 Install Smart Card Reader Driver 7-56
7.3.3 Check the Proxy Configuration 7-56
7.3.4 Configure DNS 7-56

7.3.5 Connect to the Network . . . 7-57
7.4 Connecting to payShield 10K, Installing Browser Extensions and Configuring Smart Card Reader . . . 7-58
7.4.1 Connecting to payShield 10K . . . 7-58
7.4.2 Installing Thales Browser Extensions . . . 7-59
7.4.3 Configure the Smart Card reader . . . 7-65
7.5 Commissioning payShield 10K . . . 7-66
7.5.1 Open the Commissioning Wizard page . . . 7-67
7.5.2 Create a new Security Domain . . . 7-68
7.5.3 Load the Security Domain . . . 7-73
7.5.4 Set HSM Recovery Key (HRK) passphrases . . . 7-78
7.5.5 Create Left and Right Remote Access Control key cards . . . 7-79
7.5.6 Adding Additional Warranted HSMs to the Security Domain . . . 7-84
7.6 Additional Information . . . 7-85
7.6.1 Using payShield Manager with MacOS Catalina . . . 7-85

8 Using payShield Manager . . . 8-89
8.1 Introduction to payShield Manager . . . 8-89
8.2 Logging into payShield Manager . . . 8-89
8.3 Top Tab descriptions . . . 8-91
8.3.1 Summary Tab . . . 8-91
8.3.2 Status Tab . . . 8-91
8.3.3 Operational Tab . . . 8-92
8.3.4 Domain Tab . . . 8-93
8.3.5 Configuration Tab . . . 8-93
8.4 Virtual Console Tab . . . 8-94
8.4.1 Quick Links . . . 8-94
8.4.2 Terminate Session . . . 8-94
8.5 Lower screen icons . . . 8-94
8.5.1 payShield 10K States . . . 8-95
8.5.1.1 Online . . . 8-95
8.5.1.2 Offline . . . 8-95
8.5.1.3 Secure . . . 8-95
8.5.1.4 Switching to Online or Offline State . . . 8-95
8.5.1.5 Switching to Secure State . . . 8-95
8.5.2 Time Remaining . . . 8-96
8.5.3 Information . . . 8-96
8.5.4 User . . . 8-96
8.5.5 Status . . . 8-97
8.5.6 Smart Card Operations . . . 8-97
8.5.7 Login/Logout of Users . . . 8-98
8.5.7.1 Login Additional Users . . . 8-98
8.5.7.2 User Logout . . . 8-98
8.6 Summary Page . . . 8-99
8.6.1 Summary Dashboard . . . 8-99
8.6.2 Health Dashboard . . . 8-100
8.6.2.1 How to resolve reported errors . . . 8-100
8.6.3 Configuration Dashboard . . . 8-103
8.6.4 Local Master Key . . . 8-104
8.7 Status page . . . 8-105
8.7.1 Device Information . . . 8-106
8.7.2 Utilization Statistics . . . 8-107
8.7.3 Health Statistics/Diagnostics . . . 8-111
8.7.3.1 Health/Stats . . . 8-111
8.7.3.2 Diagnostics . . . 8-112

8.7.3.3 Maintenance 8-113
8.7.4 Error Log 8-113
8.7.5 Audit Log 8-114
8.7.6 Software Info 8-121
8.7.6.1 Software - how to update software 8-122
8.7.7 FIPS/Licensing. 8-123
8.7.7.1 License Summary - how to update Licensing 8-123
8.7.7.2 Installed Licenses 8-124
8.7.7.3 FIPS Validated Algorithms 8-125
8.7.8 Import Certificate 8-125
8.7.8.1 General Information 8-125
8.7.8.2 TLS Management 8-126
8.7.8.3 Secure Host Communications 8-126
8.8 Operational 8-127
8.8.1 Local Master Keys 8-128
8.8.1.1 Generate LMK - create trusted officer 8-128
8.8.1.2 Verify an LMK Card 8-137
8.8.1.3 Create an Authorizing Card 8-137
8.8.1.4 Duplicate an LMK Card. 8-138
8.8.1.5 Generate an LMK 8-138
8.8.1.6 Install an LMK from RLMK Card Set. 8-139
8.8.1.7 Delete an Installed LMK 8-139
8.8.1.8 Replace an installed LMK. 8-140
8.8.1.9 Set the Default LMK 8-140
8.8.1.10 Set the Management LMK 8-141
8.8.1.11 Enter Authorized State 8-142
8.8.1.12 Single Authorization Mode 8-143
8.8.1.13 Multiple Authorization Mode 8-143
8.8.1.14 Key Change Storage 8-143
8.8.1.15 Install LMK from RLMK card set 8-143
8.8.1.16 Delete an installed LMK 8-144
8.8.1.17 Replace an Old LMK. 8-144
8.9 Domain 8-145
8.9.1 payShield Security Group 8-146
8.9.2 Security Domain 8-147
8.9.2.1 Commission a Smart Card 8-147
8.9.2.2 Decommission a Card 8-152
8.9.2.3 Copy a Domain Card 8-152
8.9.2.4 Create a New Security Domain 8-152
8.9.2.5 HRK Operations 8-152
8.10 Configuration 8-154
8.10.1 Host Settings 8-155
8.10.2 Active Host Interface 8-155
8.10.3 Ethernet 8-156
8.10.3.1 IP 8-157
8.10.3.2 Access Control List (ACL). 8-158
8.10.3.3 TCP/UDP 8-159
8.10.3.4 TLS 8-160
8.10.3.5 Printer Settings 8-161
8.10.4 Security Settings 8-163
8.10.4.1 Security Parameter Descriptions 8-165
8.10.5 Management Settings 8-165
8.10.5.1 Management - Interface 8-165
8.10.5.2 Management - Timeouts. 8-167

8.10.5.3 Management - TLS Certificate 8-168
8.10.6 General Settings. 8-168
8.10.6.1 General - PIN Blocks 8-169
8.10.6.2 General - Alarms 8-170
8.10.6.3 General - Fraud 8-171
8.10.6.4 General - Date and Time 8-172
8.10.6.5 General - Miscellaneous 8-172
8.10.7 Configure Commands 8-173
8.10.8 Audit Settings 8-175
8.10.8.1 Audit - General 8-175
8.10.8.2 Audit - Console Commands 8-176
8.10.8.3 Audit - Host Commands 8-177
8.10.8.4 Audit - Management Commands. 8-178
8.10.9 SNMP Settings 8-179
8.10.10 Load/Save Settings 8-180
8.11 Virtual Console 8-180

9 Migrating LMKs 9-183
9.1 Introduction 9-183
9.2 Multiple LMKs 9-183
9.3 Overview of the process 9-183
9.4 Generating new LMK component Smart Cards. 9-184
9.4.1 Types of LMK component cards. 9-185
9.5 Formatting LMK Smart Cards 9-185
9.5.1 HSM LMK Cards 9-185
9.5.2 payShield Manager LMK Cards 9-185
9.6 Generating LMK Component Cards 9-186
9.6.1 HSM LMK Cards 9-186
9.6.2 payShield Manager RLMK Cards. 9-186
9.7 Creating Copies of LMK Component Cards 9-186
9.7.1 Duplicating HSM LMK cards 9-186
9.7.2 Duplicating a payShield Manager RLMK card 9-187
9.8 Loading the new LMK 9-187
9.8.1 Using the Console 9-187
9.8.1.1 Loading (or forming) the LMK 9-187
9.8.1.2 Checking the LMK. 9-187
9.8.2 Using payShield Manager 9-188
9.8.2.1 Installing the LMK 9-188
9.8.2.2 Checking the LMK. 9-188
9.9 Loading the old LMK 9-188
9.9.1 Using the Console 9-188
9.9.2 Using payShield Manager 9-189
9.10 Migrating keys between Variant LMKs 9-189
9.10.1 BW Host command 9-189
9.10.2 BX Response to the Host. 9-192
9.11 Migrating keys from Variant to Key Block LMKs 9-193
9.11.1 BW Host command 9-193
9.11.2 BX Response to the Host. 9-195
9.12 Migrating keys between Key Block LMKs 9-196
9.12.1 BW Host command 9-196
9.12.2 BX Response to the Host. 9-197
9.13 Migrating keys from Key Block to Variant LMKs 9-197
9.14 Migrating keys for PCI HSM compliance. 9-198
9.15 Re-encrypting PINs 9-198
9.15.1 BG Host Command 9-198

9.15.2 BH Response 9-199
9.16 Re-encrypting decimalization tables 9-200
9.17 Switching to the new LMK 9-201
9.18 Taking advantage of Multiple LMKs 9-202
9.19 Clean-up after migration to a new LMK 9-203
9.19.1 Deleting the Old LMK from Key Change Storage 9-203
9.19.1.1 Using the console 9-203
9.19.1.2 Using payShield Manager 9-203
9.19.1.3 Using a Host Command 9-203
9.19.2 Deleting the New LMK 9-204
9.19.2.1 Console 9-205
9.19.2.2 Using payShield Manager 9-205

Appendix A - Console Commands 10-207

Appendix B - Configuring Ports Using the Console 11-449
B.1 Configure the Management Port 11-449
B.2 Configure the Printer Port 11-451
B.3 Configure the Host Ports 11-451
B.3.1 Configuring the Software 11-451
B.3.1.1 Message Header Length 11-452
B.3.1.2 Ethernet Communications 11-452
B.3.1.3 Software Parameters 11-453

Appendix C - Commission payShield Manager using Console Commands . . 12-457
C.1 Background information 12-457
C.2 Prerequisites 12-458
C.3 Procedure 12-458
C.3.1 Secure the HSM 12-458
C.3.2 Generate a Customer Trust Authority 12-458
C.3.3 Create the HRK passphrases 12-460
C.3.4 Commission the HSM 12-461
C.3.5 Commission Smart Cards 12-463
C.3.6 Migrate LMK Cards to become RLMK Cards 12-463

Appendix D - Technical Support Contacts 13-465

Revision Status

Revision	Date	Changes
001	March 2019	Initial Issue
002	December 2019	Editorial updates Addition of FF1 License Correction in Section 2.1.4, Feature Comparison
003	January 2020	Editorial updates
004	March 2020	FF1 license (Section 1.10, “payShield 10K license packages”, on page 19) payShield Monitor updated VR command updated (Chapter 8, “Connect to the payShield 10K” and in Appendix , “Console Commands”) payShield Monitor dashboard updated (Section 8.6.1, “Summary Dashboard”, on page 99 payShield Monitor Summary License updated (Section 8.7.7.1, “License Summary - how to update Licensing”, on page 123 payShield Monitor Software tab modified (Section 8.7.6.1, “Software - how to update software”, on page 122
004a	April 2020	Minor editorial changes
005	October 2020	payShield 10K 10G Ethernet Hardware Platform Variant support documented in Chapter 5, “payShield 10K 10G Ethernet Hardware Platform Variant”. Links to Chapter 5 added to: Chapter 1, “Introduction”, Chapter 2, “Backwards Compatibility and Differences”, Chapter 3, “Physical Description”, Chapter 4, “Installation”
006	January 2021	Editorial updates Trusted Management Device update (Section 1.11, “Trusted Management Device (TMD)”, on page 21)

1 Introduction

1.1 Documentation Overview

Documentation for the payShield 10K Hardware Security Module (HSM) is streamlined into the following manuals:

- payShield 10K Installation and User Guide
- payShield 10K Security Manual
- payShield 10K Host Programmer's Manual
- payShield 10K Applications Using payShield 10K
- payShield 10K Core Host Commands Manual
- payShield 10K Legacy Command Reference Manual
- payShield 10K Regulatory Users Warnings and Cautions

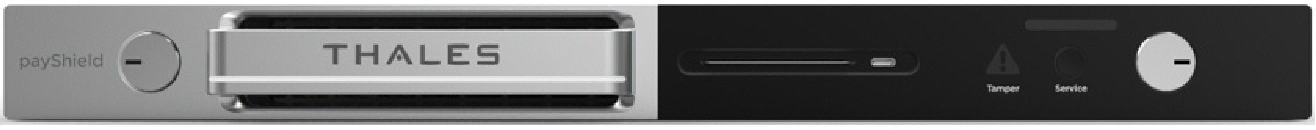
Note: Console Commands are now included in this manual, Appendix A.

1.2 Audience

The manual's audience includes:

- Network installers
- Trusted officers/data security administrators
  - Physical key holders
  - Physical card holders
  - Compliance officers

1.3 payShield 10K General Description



The payShield 10K payment hardware security module (HSM) provides cryptographic functions to support network and point-to-point data security. The payShield 10K acts a peripheral device to a Host computer. It provides the cryptographic facilities required to implement key management, message authentication, and Personal Identification Number (PIN) encryption in real time online environments.

The HSM is secured by physical locks, electronic switches and tamper-detection circuits. It supports a large number of standard commands and can be customized to perform client-specific cryptographic commands.

Standard command functions include:

- Generating and verifying PINs, such as those used with bank accounts and credit cards
- PIN solicitation, to obtain a new PIN from a card holder (against a reference number)
- Generating encrypted card values, such as Card Verification Values (CVV) for the plastic card industry
- Generating keys for use in Electronic Funds Transfer Point of Sale (EFTPOS) systems
- Key management in non-EFTPOS systems
- Generating and verifying Message Authorization Codes (MACs) for messages transferred via telecommunications networks

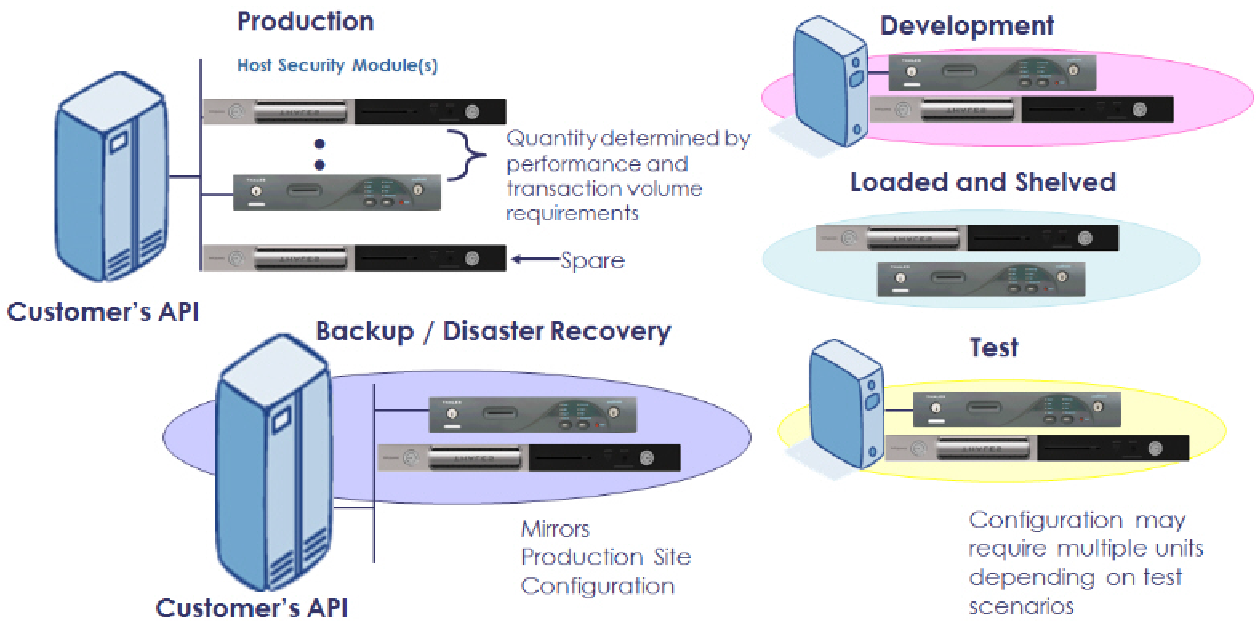
1.4 Typical Configuration

A typical payShield 10K configuration consists of two or more payShield units connected as “live” units. A multi-unit configuration permits concurrent operation for high throughput, and, under control of the application program, provides automatic and immediate backup in the event of a fault in a single unit.

Typically, redundancy is built into the system design by providing more capacity than is required to allow commands to be switched away from a failed or withdrawn unit. Optionally, it is possible to have a backup unit not connected to the Host but ready for connection in place of a faulty unit. This is not the preferred practice because the unit may remain idle for a long time and may itself have developed a fault.

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

The figure that follows illustrates a deployment architecture that includes both payShield 9000s and payShield 10Ks.


Production
Host Security Module(s)
Quantity determined by performance and transaction volume requirements
Spare
Customer's API
Development
Loaded and Shelved
Backup / Disaster Recovery
Test
Mirrors Production Site Configuration
Configuration may require multiple units depending on test scenarios
Customer's API

1.4.1 Command Flow

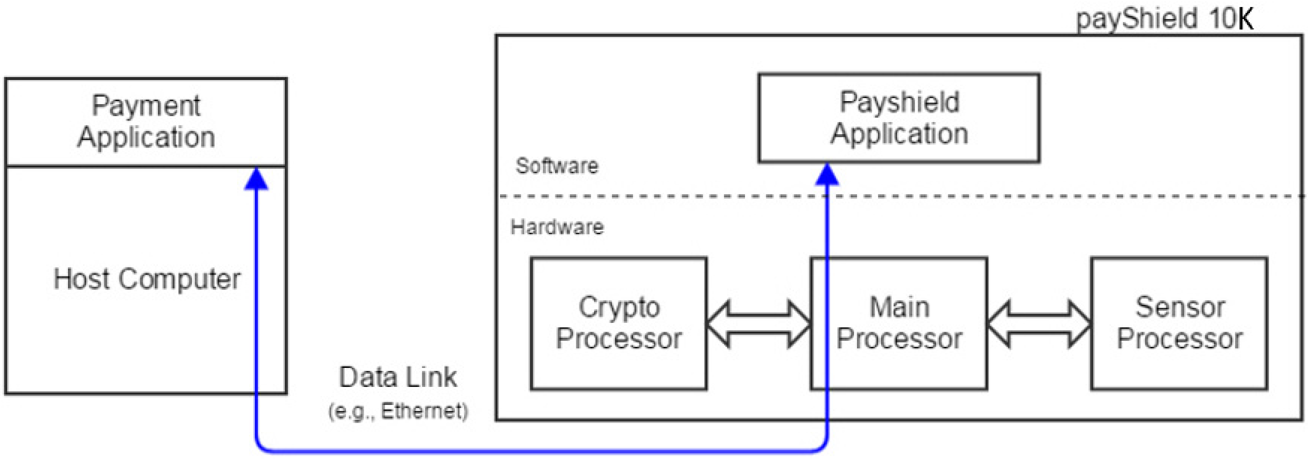
Note: The payShield 10K is normally online to the Host and does not require operator monitoring or intervention.

The HSM processes commands from the Host.

- The Host sends command messages, which consist of command codes and other fields that are required by the HSM in order to process the commands, to the HSM.
- The HSM processes the command messages and generates response messages, which also contain a variable number of fields (depending on the message type).

  Note: Some commands, mainly involving plain text data, are entered by the user via the associated HSM console.

The flow of data through components is represented in the figure that follows.



The throughput of the HSM depends on the types of commands that are executed, and the method and speed of the Host connection.

1.5 Smart cards

The payShield 10K uses smart cards to provide a convenient means of handling sensitive information.

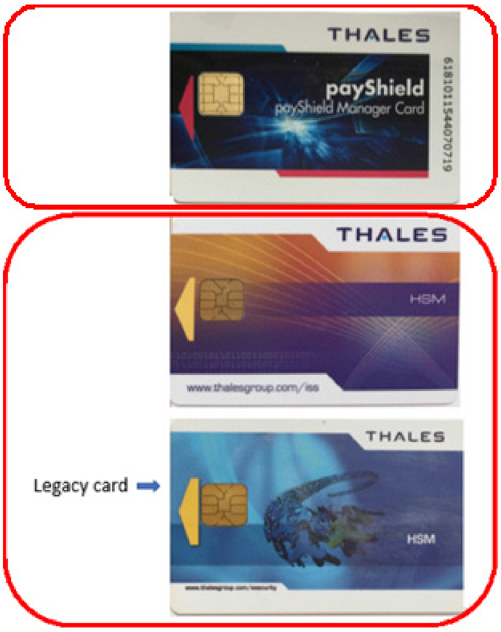
Smart cards are used for storing three distinct types of information:

- Key components - particularly the Local Master Key (LMK)
- Authorizing Officer credentials
- HSM alarm, security and Host settings

There are two types of smart cards:

- payShield Manager smart cards
- HSM smart cards

  Note: Additionally, there are 2 types of HSM smart cards. (See figure that follows.)



The differences between smart cards are identified in the following table.

Operations	payShield Manager Smart Card	HSM Smart Card
Formatting	Can only be formatted using payShield Manager	Can only be formatted using the FC command using USB-C console
Save Settings (Alarm, Host, Security, Audit, Command, Pin Block)	Can be used to save payShield 10K settings via payShield Manager and remote card reader only	Can be used to save payShield 10K settings via USB-C console and embedded card reader only
Customer Trust Authority (CTA)	Can be used as CTA cards both on embedded and remote card reader	Cannot be used on an embedded card reader
Local Master Key (LMK)	Can be used as LMK card both on embedded card reader and remote card reader	Can be used as LMK card from embedded card reader only

Note: Follow this link for additional information: Section 2.1.12, “Transitioning Smart Cards”, on page 31.

1.6 Customer Trust Authority (CTA)

Every commissioned HSM or smart card contains an Elliptic Curve Digital Signature Algorithm (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.

The certificate is 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 smart cards. (Section 1.8, “Key Shares”, on page 16 further explains the split/sharing concept.) The CTA is temporarily loaded into an HSM prior to signing the smart card or HSM public key certificates. The corresponding CTA public key (used to verify the certificates) is stored in each smart card and in the HSM.

A CTA must be reassembled onto a payShield in order to perform certain operations, including commissioning a payShield. After a CTA has been created, it may be used to commission multiple payShields and numerous smart cards to be used in the same security domain.

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

1.6.1 Customer Security Domain

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

A necessary condition for a smart card 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 smart cards can communicate with a specific HSM and what role they possess.

1.7 Keys

1.7.1 Encryption Mechanism

The HSM mechanism for encryption of locally stored keys uses a double length DES key, i.e., the Local Master Key (LMK), stored in the tamper-resistant memory of the HSM. All other cryptographic keys are encrypted under the LMK and stored external to the HSM, usually in a key database on the Host system that is accessible by Host applications. In order to provide key separation (e.g., key encryption keys, MAC keys, PIN verification keys, etc.), different key types are encrypted under different variants of the LMK. Hence, if the “wrong” key is provided in a command, either accidentally or deliberately, a key parity error occurs (highly likely) or a processing error occurs (occasionally).

1.7.2 HSM Recovery Key

One concern relating to the HSMs used in the remote management solution is that if an HSM becomes “tampered”, the public and private keys are removed from memory and it becomes necessary to generate a new key pair. This could involve a considerable operational inconvenience.

Therefore, a recovery mechanism involving an AES HSM Recovery Key (HRK) is available to simplify the task of restoring a public/private key pair to the HSM’s secure memory and re-establishing the previous security group.

1.7.3 Local Master Keys (LMKs)

Each payShield 10K has its own master key. This key is known as the “Local Master Key”. Every generated key is then encrypted under this Local Master Key.

The LMK is used to protect (by encryption) all of the operational keys plus some additional sensitive data that are processed by the HSM.

The payShield 10K can support multiple LMKs, such that up to 20 LMKs, of different types, can be in use at any one time. Each LMK can be managed by a separate security team. This allows a single payShield 10K to be used for multiple purposes - such as different applications or different clients.

The LMK may be common to a number of HSMs. Storing only a single key in the HSM minimizes recovery and operational downtime, in the event of a problem with the unit.

There are two types of LMKs:

- Variant LMK

  A Variant LMK is a set of 40 double- or triple-length DES keys, arranged in pairs, with different pairs (and variants of those pairs) being used to encrypt different types of keys.

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

- Key Block LMK

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

  Note: The term “Key Block LMK” refers to the “key block” method of encrypting keys; a Key Block LMK is not itself stored in the key block format.

For an HSM to operate, the LMKs must be created and loaded. Because the DES /AES algorithms depend on a key for secrecy, and because the security of all keys and data encrypted for storage depend on the LMKs, they must be created and maintained in a secure manner. Provision is made to allow the LMKs to be changed and keys or data encrypted under them to be translated to encryption under the new LMKs.

All keys when stored locally (i.e., not in transit between systems) are encrypted under the LMK.

1.7.3.1 Multiple LMKs

The availability of multiple LMKs makes it easier to migrate operational keys from an old LMK to a new one. Such LMK migration should be performed every few years for security purposes, but may also be necessary for operational reasons, e.g., when upgrading from double- to triple-length Variant LMKs or from Variant LMKs to Key Block LMKs.

Although the payShield 10K allows for changing the LMK, it means that all operational keys need to be translated from encryption under the old LMK to encryption under the new LMK before they can be used. A “big bang” approach typically requires very careful planning and coordination, with possible downtime or need for additional HSM capacity. The use of multiple LMKs allows users to adopt a phased approach to LMK change.

It is possible to install multiple LMKs within a single payShield 10K. The precise details of the number and type of installed LMKs are controlled via the payShield 10K's license file.

1.7.4 Zone Master Key

A Zone Master Key (ZMK) is a key-encrypting key which is distributed manually between two (or more) communicating sites, within a shared network, in order that further keys can be exchanged automatically (without the need for manual intervention). The ZMK is used to encrypt keys of a lower level for transmission. For local storage, a ZMK is encrypted under one of the LMK pairs.

Within the VISA environment this is known as a ZCMK.

The payShield 10K supports the use of a single-length, double-length or triple-length DES ZMK, or a 128-bit, 192-bit or 256-bit AES ZMK.

1.7.4.1 Zone PIN Key

A Zone PIN Key (ZPK) is a data encrypting key which is distributed automatically, and is used to encrypt PINs for transfer between communicating parties (for example, between acquirers and issuers). For transmission, a ZPK is encrypted under a ZMK; for local storage it is encrypted under one of the LMK pairs.

The payShield 10K supports the use of a single-length, double-length or triple-length DES ZPK.

1.7.5 Terminal Master Key

A Terminal Master Key (TMK) is a key-encrypting key which is distributed manually, or automatically under a previously installed TMK. It is used to distribute data-encrypting keys, within a local (non-shared) network, to an ATM or POS terminal or similar. The TMK is used to encrypt other TMKs or keys of a lower level for transmission. For local storage, a TMK is encrypted under one of the LMK pairs.

The payShield 10K supports the use of a single-length, double-length or triple-length DES TMK, or a 128-bit, 192-bit or 256-bit AES TMK.

1.7.5.1 Terminal PIN Key

A Terminal PIN Key (TPK) is a data-encrypting key which is used to encrypt PINs for transmission, within a local network, between a terminal and the terminal data acquirer. For transmission, a TPK is encrypted under a TMK; for local storage it is encrypted under one of the LMK pairs.

The payShield 10K supports the use of a single-length, double-length or triple-length DES TPK.

1.7.6 Terminal Authentication Key

A Terminal Authentication Key (TAK) is a data-encrypting key which is used to generate and verify a Message Authentication Code (MAC) when data is transmitted, within a local network, between a terminal and the terminal data acquirer. For transmission, a TAK is encrypted under a TMK or ZMK; for local storage it is encrypted under one of the LMK pairs.

The payShield 10K supports the use of a single-length, double-length or triple-length DES TAK, or a 128-bit, 192-bit or 256-bit AES TAK.

1.7.7 Terminal Encryption Key

A Terminal Encryption Key (TEK) is a data-encrypting key which is used to encrypt and decrypt messages for transmission, within a local network, between a terminal and the terminal data acquirer. For transmission, a TEK is encrypted under a TMK or ZMK; for local storage it is encrypted under one of the LMK pairs.

The payShield 10K supports the use of a single-length, double-length or triple-length DES TEK, or a 128-bit, 192-bit or 256-bit AES TEK.

1.7.8 PIN Verification Key

A PIN Verification Key (PVK) is a data-encrypting key which is used to generate and verify PIN verification data and thus verify the authenticity of a PIN. For transmission, a PVK is encrypted under a TMK or under a ZMK; for local storage, it is encrypted under one of the LMK pairs.

The payShield 10K supports the use of a single-length, double-length or triple-length DES PVK.

1.7.9 Card Verification Key

A Card Verification Key (CVK) is similar to a PIN Verification Key, but for Card information instead of a PIN.

The payShield supports the use of a single-length, double-length or triple-length DES CVK.

1.7.10 Master Session Key

The master/session key management scheme involves setting up a master key between two communicating parties (for example, an acquirer and an issuer or an acquirer and a terminal) under which data-encrypting keys are exchanged for use during a session. Key installation and updating must be organized by the institutions involved (i.e., within the application programs).

The HSM supports master/session key management in both shared and local networks, but distinguishes between the two and maintains separate key hierarchies.

1.8 Key Shares

By assigning key and policy management to more than one Security Administrator a strong separation of duties over HSM management is enforced. Each Security Administrator is assigned a smart card. Each smart card has a “key share”. To create a “key”, each “key share” must be presented. With “key sharing”, no one person has complete control over the security of data.

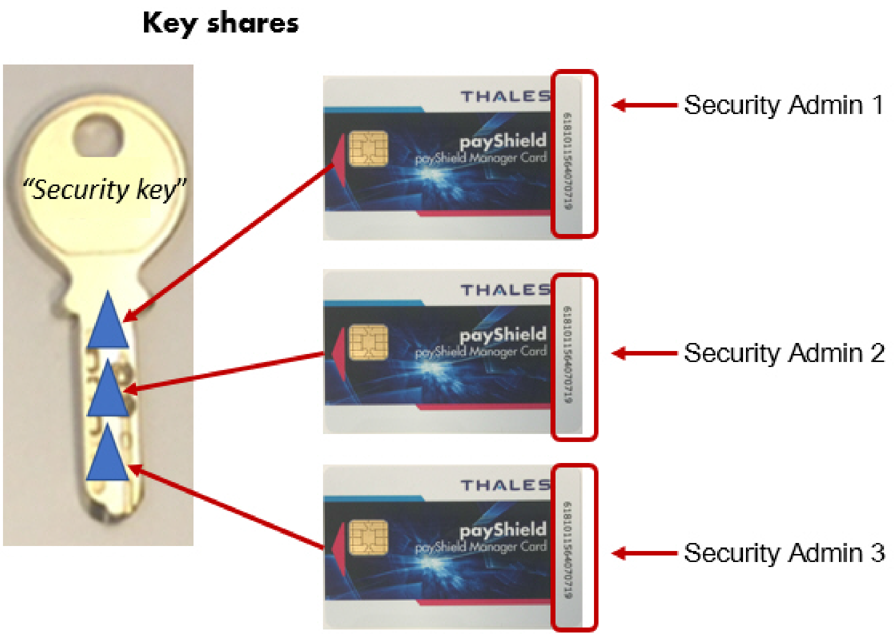


Figure 1 "key share" concept overview

1.9 Host Commands supporting multiple LMKs

The basic mechanism for Host commands to support multiple LMKs and LMK schemes is as follows:

Two additional (optional) fields are added at the end of each Host command request message. These fields are:

Field	Length & Type	Details
Delimiter	1 A	Value '%'. Optional; if present, the LMK Identifier field must be present.
LMK Identifier	2 N	LMK identifier; min value = '00'; max value is defined by license; must be present if the above Delimiter is present.

For Ethernet-attached Host computers, the HSM can infer the LMK Identifier to use for a particular command from the TCP port on which the command is received. Historically, Host commands sent via TCP/IP have been directed to the HSM's Well-Known Port, and this continues to be supported. However, Host commands directed to [the Well-Known Port +1] will automatically use LMK Id 00; Host commands directed to [the Well-Known Port +2] will automatically use LMK Id 01; etc. The situation for an HSM using the default Well-Known Port value of 1500 is summarized in the table below:

Command received on TCP Port	LMK Used
1500	Default LMK ID (or % nn construct)
1501	LMK ID 00
1502	LMK ID 01

Command received on TCP Port	LMK Used
1503	LMK ID 02

1.9.1 LMK Usage in Host Commands

The HSM uses the following mechanisms to determine which LMK Id to use with a Host command:

- The Management LMK is automatically used for command processing and the Delimiter and LMK Identifier fields should not be included in the command message. The only commands that belong in this category are the “Q0”, “Q2”, “Q4” and “Q8” commands.
- For commands using key blocks, the LMK that is identified in the key block header(s) is used; if the Delimiter and LMK Identifier are present in the command message, then all LMK identifiers must agree.
- If the Delimiter and LMK Identifier are present at the end of the command message, then the specified LMK is used in the command processing.
- For commands received via the Ethernet Host port using TCP/IP, the HSM infers the LMK Id to use based on the specific TCP port on which the command was received.
- For all other commands where the Delimiter and LMK Identifier are not present in the command message, the Default LMK is used in command processing.

1.10 payShield 10K license packages

The tables that follow summarize payShield 10K license packages.

Product Code	Product Name	Product Description
PS10-CLA-L	Classic package - 25 cps	Classic Package - 25 cps. Standard processing package containing all the core functionality necessary to route and validate payment transactions.
PS10-CLA-S	Classic package - 60 cps	Classic Package - 60 cps. Standard processing package containing all the core functionality necessary to route and validate payment transactions.
PS10-CLA-M	Classic package - 250 cps	Classic Package - 250 cps. Standard processing package containing all the core functionality necessary to route and validate payment transactions.
PS10-CLA-H	Classic package - 1000 cps	Classic Package - 1000 cps. Standard processing package containing all the core functionality necessary to route and validate payment transactions.
PS10-CLA-X	Classic package - 2500 cps	Classic Package - 2500 cps. Standard processing package containing all the core functionality necessary to route and validate payment transactions.
PS10-PRM-L	Premium package - 25 cps	Premium package - 25 cps. Premium issuing and processing package containing all core functionality available for the payShield 10K platform.
PS10-PRM-S	Premium package - 60 cps	Premium package - 60 cps. Premium issuing and processing package containing all core functionality available for the payShield 10K platform.
PS10-PRM-M	Premium package - 250 cps	Premium package - 250 cps. Premium issuing and processing package containing all core functionality available for the payShield 10K platform.
PS10-PRM-H	Premium package - 1000 cps	Premium package - 1000 cps. Premium issuing and processing package containing all core functionality available for the payShield 10K platform.
PS10-PRM-X	Premium package - 2500 cps	Premium package - 2500 cps. Premium issuing and processing package containing all core functionality available for the payShield 10K platform.
PS10U-CLA-L2S	Classic pack perf upg - 25 to 60 cps	Classic pack performance upgrade - 25 to 60 cps
PS10U-CLA-S2M	Classic pack perf upg - 60 to 250 cps	Classic pack performance upgrade - 60 to 250 cps
PS10U-CLA-M2H	Classic pack perf upg - 250 to 1000 cps	Classic pack Performance upgrade - 250 to 1000 cps
PS10U-CLA-H2X	Classic pack perf upg - 1000 to 2500 cps	Classic pack performance upgrade - 1000 to 2500 cps
PS10U-CLA2PRM	Package upgrade - Classic to Premium	Package upgrade - Classic to Premium

Product Code	Product Name	Product Description
PS10U-PRM-L2S	Premium pack perf upg - 25 to 60 cps	Premium pack performance upgrade - 25 to 60 cps
PS10U-PRM-S2M	Premium pack perf upg - 60 to 250 cps	Premium pack performance upgrade - 60 to 250 cps
PS10U-PRM-M2H	Premium pack perf upg - 250 to 1000 cps	Premium pack performance upgrade - 250 to 1000 cps
PS10U-PRM-H2X	Premium pack perf upg - 1000 to 2500 cps	Premium pack performance upgrade - 1000 to 2500 cps

Optional Licenses

Product Code	Product Name	Product Description
PS10-LIC-RMGT	Remote payShield Manager license	License to operate payShield Manager remotely as well as locally
PS10-LIC-LMKx2	payShield LMK x 2 license	License for multiple LMKx2
PS10-LIC-LMKx5	payShield LMK x 5 license	License for multiple LMKx5
PS10-LIC-LMKx10	payShield LMK x 10 license	License for multiple LMKx10
PS10-LIC-LMKx20	payShield LMK x 20 license	License for multiple LMKx20
PS10-LIC-FF1	FF1 license	License enables the use of the FF1 Format Preserving Encryption (FPE) algorithm within the M0, M2 and M4 host commands.
PS10-LIC-VDSP	Visa Data Secure Platform (DSP) license	License for Visa Data Secure Platform (DSP). Requires written confirmation from customer that they have an agreement with VISA.
PS10-LIC-LEGACY	Miscellaneous Legacy Commands license	License for Miscellaneous Legacy Commands

1.11 Trusted Management Device (TMD)

1.11.1 Introduction

This section provides an outline of the Trusted Management Device (TMD) provided by Thales to securely manage key components to meet the latest standards from PCI. The TMD replaces the Thales Key Management Device (KMD) which is end of sale.

For further detailed information on the TMD please refer to the TMD User Guide.

1.11.2 Background

Secure key management is crucial to the security of the system in which the payShield 10K is used. One particular area of importance is the exchange of symmetric encryption keys between parties in the payment network (such as an Acquirer and a Switch) who need to exchange data securely. There is a large number of such keys, and these need to be refreshed regularly, and so there is a frequent need to exchange working keys between parties. In order to protect these keys while they are being exchanged electronically, the working keys are encrypted by a master key (such as a Zone Master Key, or ZMK).

The master key still needs to be provided by one party to the other, and this transfer also has to be secured. However, master keys need to be transferred only infrequently, and so a less automated mechanism is acceptable. In general the institution providing the master key will issue it in the form of a number (typically 3) of components to different officers in the receiving institution, and these officers will come together and enter their components individually into a secure system.

In the past it has been acceptable to enter the components directly into the payment HSM such as the payShield 10K using the Console interface. However the latest PCI standards require use of a Secure Cryptographic Device (SCD) such as the Thales Trusted Management Device (TMD). This replaces the Thales Key Management Device (KMD) which is end of life.

1.11.3 Description

The TMD offers secure, flexible and efficient key management for payment HSMs. It is a compact, intuitive, self-contained secure cryptographic device (SCD) that enables you to perform symmetric key management tasks including securely forming keys from separate components or splitting existing keys retrospectively into new components. The TMD generates and shares keys in a manner that is compliant with relevant security standards, including X9 TR-31, ANSI X9.24-1 and PCI PIN Security.

Unlike traditional approaches, these critical key management tasks can be carried out without any physical connection to a production HSM, providing greater operational flexibility without compromising security. For example, a single payShield TMD can form keys for multiple payment HSMs distributed across multiple data centers, enabling large payment processors to create and distribute thousands of Key Encrypting Keys (KEKs) or Zone Master Keys (ZMKs) in a timely and secure manner while eliminating data entry errors.

Each TMD shares one or more Master ZMKs (MZMKs) with the HSMs to facilitate secure exchange of key material. The TMD does not require access to the Local Master Keys (LMKs) used by the production HSMs. Keys exchanged between TMD and an HSM are encrypted under the appropriate MZMK.

The Thales Trusted Management Device.

1.11.4 How Keys Are Shared With payShield and 3rd Parties

The following table shows how keys are typically shared securely between the TMD, payShield 10K and third parties. Other options are available for example to secure the transfer of keys.

Phase	Internal System		External Party	Key	Secure Method of Transfer
Set-Up	TMD	payShield 10K	-	MZMK	Component form on Smart Card
	TMD		Third Party	ZMK	Components in Printed Form
	TMD	payShield 10K		ZMK	Encrypted under MZMK
Production	payShield 10K		Third Party	Application and Session Keys (e.g. ZPK, PVK etc.)	Encrypted under ZMK

Note keys can be transferred in both directions.

1.11.5 Example Sequence of Steps to Set-Up and Transfer Keys

This section shows a typical sequence of steps that are used to set up the keys required. Please note:

- From the payShield 10K perspective, the MZMK is a standard ZMK.
- The TMD has comprehensive facilities to manage TMD Administrators and Operators using smart cards and these are set up when the first MZMK is installed – see the *TMD User Guide*

  Note:
- The host application in the description below is the customer's payment application.

The main steps are:

1. Sharing MZMK between the payShield 10K and the TMD:
   a) Use payShield 10K Console Command **GS** to generate MZMK components on HSM smart cards and to display the MZMK encrypted under the LMK.

   b) Install MZMK in the TMD from the components on smart card generated above.

   c) Enter MZMK encrypted under the LMK into the host application database for subsequent use.
2. Sharing ZMK with third party.
   a) Use TMD to import ZMK in component form from third party and display ZMK encrypted under the MZMK.

   b) Enter ZMK encrypted under the MZMK into the host application.

   c) Host application uses host command **A6** (or **BY**) to translate the ZMK from encryption under the MZMK to encryption under the LMK and stores in the host application for subsequent use.

   Note: Instead of using a host command in step c), Console Command **IK** can be used with the payShield Manager Virtual Console (or the standard Console) to translate the ZMK from encryption under the MZMK to encryption under the LMK. This can then be entered into the host application for subsequent use.
3. Sharing Application or Session Keys with Third Party
   a) Application or Session keys (e.g. ZPK, PVK) received from the 3rd party encrypted under a ZMK are translated to encryption under an LMK using host command **A6**.

   b) Host application exports Application or Session keys (e.g. ZPK, PVK) to 3rd party by translating from encryption under a LMK to encryption under the ZMK using host command **A8**.
4. Option - Sharing Application Keys with in Component Form with Third Party
   a) Use TMD to import the application key (e.g. PVK, CVK) in component form and output key encrypted under the MZMK on the display.

   b) Enter key encrypted under the MZMK into the payment application

   c) Host application uses host command **A6** to translate the key encrypted under the MZMK to encryption under the LMK and stores in the host application.

The ZMK can be generated by payShield 10K instead of by the third party. In this case, payShield 10K is used to generate the ZMK (using Host Command **A0**), encrypt the ZMK under a MZMK (using host command **A8** or Console Command **KE**) for import into the TMD. The TMD can then be used generate and print the ZMK Components securely for transfer to a third party. As noted above, the payShield Manager Virtual Console or the standard Console can be used with Console Command KE.

There are also a number of alternative options provided with the TMD and these are documented in the TMD manual. These include:

- Except for the first MZMK, subsequent MZMK can be generated using the TMD and stored in component form on smart card. Console Command **FK** is then used to import from components on smart card and display the key encrypted under the LMK. This is then entered into the host application for subsequent use.
- Key components or encrypted keys generated by the TMD can be displayed on the TMD screen, printed or written to USB memory stick.
- Key components or encrypted keys received from 3rd parties can be entered on the TMD screen, scanned in using QR code or read from USB memory stick if provided in the supported format.

2 Backwards Compatibility and Differences

2.1 payShield 9000 / payShield 10K

Where possible, the payShield 10K provides Host commands that are backwards compatible with implementations on older versions of Thales HSMs, specifically the payShield 9000.

- LMKs generated and written to payShield 9000 Smart Cards using the GK console command work in the payShield 10K
- LMKs set up using payShield Manager work in the payShield 10K using payShield Manager
- Customers who have set up Customer Trust Authorities (CTAs) for payShield Manager on the payShield 9000 can use those same CTAs in payShield 10K

payShield 10K does not support the old Remote HSM Manager. If you have set up LMK cards using the old Remote HSM Manager, migrate the cards to payShield Manager using the payShield 9000. Once migrated, the cards can be used on the payShield 10K.

Note: pay Shield 9000 cards storing **security**, **command or PIN Block configuration settings** cannot be used on the payShield 10K. Conversely, payShield 10K cards storing security, command or PIN Block configuration settings cannot be used on the payShield 9000.

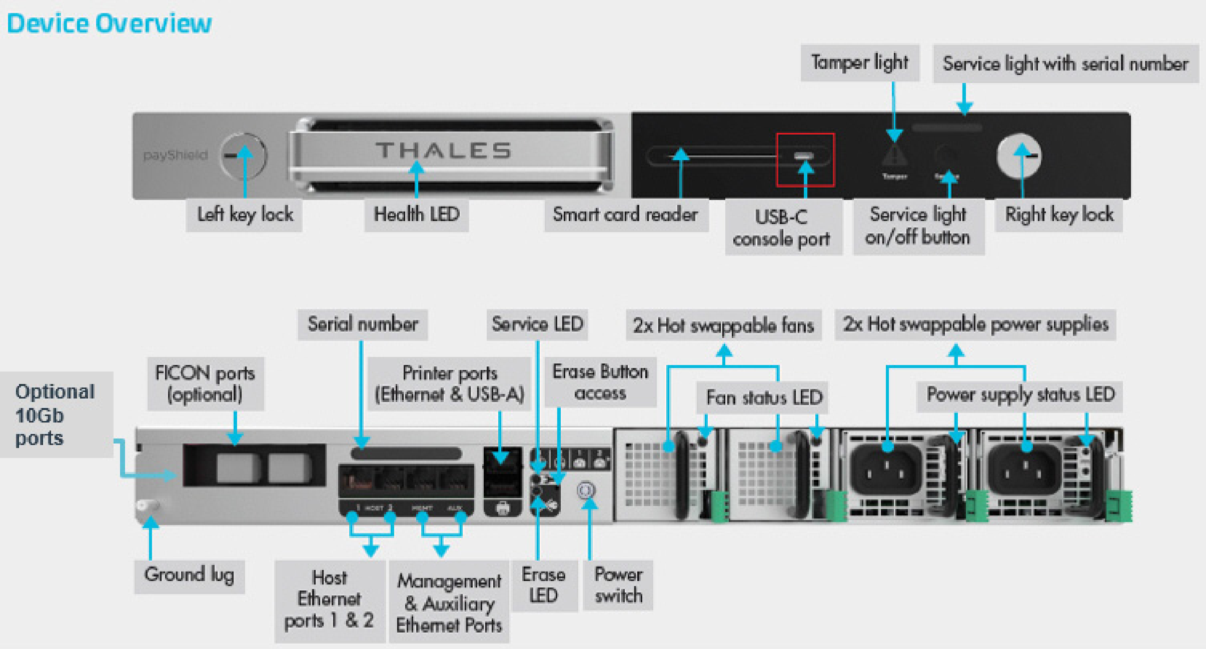
2.1.1 Host Interface and Commands

The only major differences between the Host Interface and Commands for payShield 9000 and for the payShield 10K are as follows:

- Legacy commands must be ordered separately through a license (PS10-LIC-LEGACY).
- Asynchronous Communication capability has been removed from Host1 and Host2 ports.
- The LG Host command to “Set HSM Response Delay” has been depreciated because ASYNC communications are not supported, so it now only returns a ‘00’.

2.1.2 Options for Managing payShield 10K

- Connecting a Console (USB-C on front panel).
- Local payShield Manager, Ethernet directly into management port.
- Remote payShield Manager, Ethernet into network.



Note: Local payShield Manager comes as part of the payShield package and creates a GUI user interface that is much easier to use than the console. Once customer trust has been set up between the payShield and the payShield Manager Smart Cards, you can easily choose to add the remote licenses with minimal set up at a later date.

2.1.3 Modifications made to the console commands

Command	Description
'CC' (Configure Console)	Removed Command because the console is now self-configuring.
'QC' (Query Console)	Removed Command because the console is now self-configuring.
SNMPADD (Add SNMP)	Modified for payShield 10K MIB
SNMP DEL (Delete SNMP)	Modified for payShield 10K MIB
TRAP (Displays Traps configured)	Modified for payShield 10K MIB
TRAPADD (Add a trap)	Modified for payShield 10K MIB
'CH' (Configure Host)	Modified to remove Asynchronous Communications option.
'QH' (Query Host)	Modified to remove Asynchronous Communications option.
'VR' (view software revision)	Modified to reflect payShield 10K Version options.
UPLOAD (upload new code)	Added for secure code and license loading at the console.

Command	Description
AUDITPRINT (print audit log)	Removed because of the increase in Audit size. Logs can be uploaded and then printed.
‘SS’ (Save settings to Smart Card)	Modified for 10K settings.
‘RS’ (Retrieve HSM settings from Smart Card)	Modified for 10K settings, cannot be used for 9K settings and conversely, 9K settings cannot be used for 10K.
‘RI’ (Initialize Domain Authority)	Removed because old HSM Manager is not supported in the 10K.
‘RH’ (Generate an HSM certificate)	Removed because old HSM Manager is not supported in the 10K.
ROUTE (Add static IP Route)	Removed, this command was only relevant to HSM 8000. This can be done using the ‘CH’ command and entering the ‘gateway’ address.
‘CS’ (Configure Security)	Modified for 10K
‘QS’ (Query Security)	Modified for 10K
‘DT’ (Diagnostic Test)	Modified for 10K (added new tolerances for Voltage and Temperature and added hot swappable fans and power supplies).
AUDITOPTIONS (Set up audit options)	Modified for 10K
AUDITLOG (Manage audit log)	Modified for 10K, increased size to 100,000 entries.
‘CL’ (Configure Alarm)	Modified for 10K
NETSTAT (Show network statistics)	Modified because of 10K OS version
PING (Test TCP/IP network)	Modified because of 10K OS version
TRACERT (Trace TCP/IP route)	Modified because of 10K OS version
‘QL’ (Query Alarm)	Modified for 10K
NETSTAT (Show network statistics)	Modified because of 10K OS version
PING (Test TCP/IP network)	Modified because of 10K OS version
TRACERT (Trace TCP/IP route)	Modified because of 10K OS version

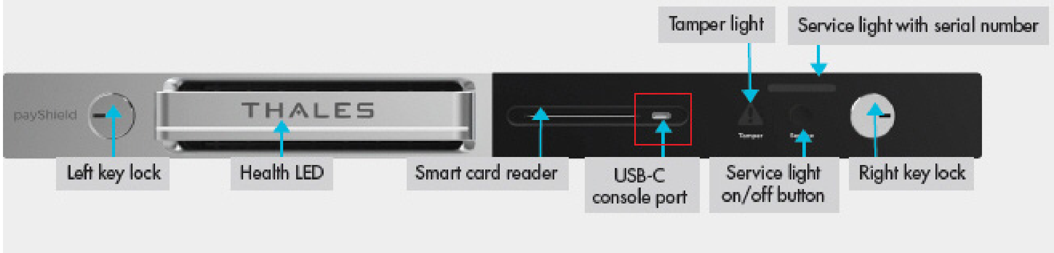
2.1.4 Feature Comparison

Note: For the10G Ethernet Platform Variant, follow this link: Chapter 5, “payShield 10K 10G Ethernet Hardware Platform Variant”.

Feature	payShield 9000	payShield 10K
Form Factor	2U Chassis	1U Chassis
Code loading mechanism	FTP interface or USB stick	HTTPS via payShield Manager or the secure "UPLOAD" console command using the USB-C for the console and the USB-A for the USB memory stick with the software or license update.
Security sub-system	TSPP designed to meet FIPS 140-2 Level 3 and PCI HSM Version 1	TASP 1.0 designed to meet FIPS 140-2 Level 3 and PCI HSM Version 3
PIN block translate performance	20, 50, 150, 250, 800 and 1500 tps (transactions per second)	25, 60, 250, 1000 and 2500 cps (commands per second)
Power supply options	Choice of single or redundant power supplies, not Field Replaceable	Dual, Field Replaceable and Hot Swappable
Fan options	Fixed, not Field Replaceable	Dual, Field Replaceable and Hot Swappable
Management port connections	Six USB-A ports Ethernet for local/remote management	USB-C port on front panel USB-A port on rear panel Ethernet for local/remote management Ethernet for AUX (payShield Monitor)
Host interface connectivity	Dual, 10/100/1000 Mbps Ethernet, Async and FICON	Dual, 10/100/1000 Mbps Ethernet PCIe slot for FICON or 10Gig Ethernet (supported after product launch) (Async no longer supported)
Dimensions	3.35 x 18.82 x 16.42" (85 x 478 x 417mm)	19" x 29" x 1.75" (482.6mm x 736.6mm x.44.45mm)
Weight	7.5kg (16.5lb)	15.9 kilograms (35 lbs)
Electrical Supply	100 to 240V AC Universal input, 47 to 63 Hz	90-264V AC Universal input, 47 to 63 Hz
Power Consumption	100W (maximum)	60W (maximum) with 10GigE ports: • when using 4 optical ports the maximum is 70W • when using 4 copper ports, the maximum is 80W with FICON ports: 70W (maximum)
Operating Temperature	0 deg C to +40 deg C	0 deg C to +40 deg C
Humidity	0% to 90% (non-condensing)	10% to 90% (non-condensing @ +30C)
MTBF	179K hours and an Annual Failure Rate (AFR) of 4.7%.	555K hours without redundant power supplies and fans and an AFR of 1.57% 2,445K hours with redundant power supplies and fans and an AFR of 0.35%

Note: Should temperatures exceed the operational range, return the payShield to the operational range.

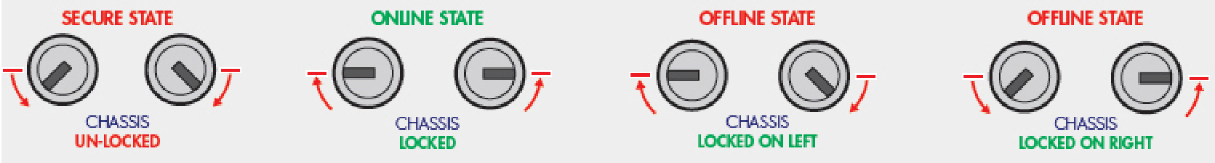
2.1.5 Front Panel



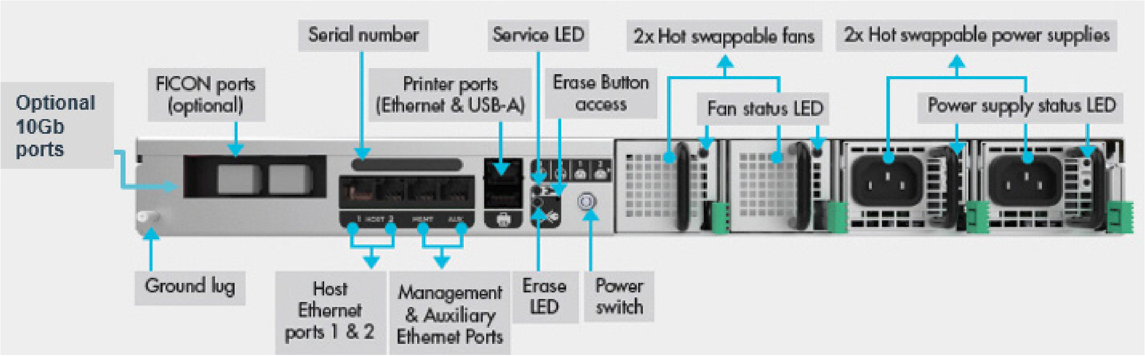
2.1.6 Front Panel LEDs

LED Indicator	LED Color	Description
Front Panel Health	Solid White	Unit booting, firmware validation in process, payShield functional, there are no errors in the error log.
Front Panel Health	Solid Red	Unit booting, application initialization in process, payShield failed diagnostic test or there are errors in the error log.
Front Panel Tamper	Off	No Tamper has been detected.
Front Panel Tamper	Solid Red	A high Tamper has been detected, contact Thales support.
Front Panel Tamper	Flashing Red	A medium Tamper has been detected, customer key material has been erased.
Front Panel Service	Off	Service has not been designated for this unit.
Front Panel Service	Solid Blue	This unit has been designated for service.

2.1.7 Front Panel Key Lock Positions



2.1.8 Rear Panel



2.1.9 Enhanced Security Features

payShield 10K software has been designed, where practical, to be secure by default. Most security settings affecting configurations are set to their most secure value by default.

Attention: All Host commands, most console commands and all PIN Blocks have been disabled by default.

Note: The security parameters required may vary depending on your security policy and system environment, and Thales recommends that you review the *payShield 10K Security Manual* as well as consult your internal Security Manager for full details.

payShield 10K has been designed with the following enhanced physical security features:

- A tamper resistant and responsive design
- Fully locked-down chassis lid with no ability to open
- Tamper sensors for chassis lid, crypto processor cover, motion, voltage and temperature
- Two levels of tamper:
  - Medium tamper erases all sensitive data
  - High tamper erases all sensitive data and permanently disables use of the unit
- Sensitive data immediately erased in the event of any tamper attempt

Compliance with PCI HSM Version 3 requirements introduce some rules which may cause incompatibility between PCI HSM compliant payShield 10K HSMs and earlier non-compliant HSMs:

- In most cases, security settings default to the most secure option
- All Host and console commands are disabled.

  Note: The console command CONFIGCMD is not disabled by default.
- All PIN blocks are disabled

Control is provided in the security settings to allow the user to select whether to operate in the “classic” manner or in the PCI HSM compliant manner.

Three new settings have been added to the “Security Configuration Settings” for PCI HSM V3:

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

Note: Once the security configuration settings are all PCI HSM compliant, they cannot be changed without all customer key material being deleted and the configuration settings set back to factory default.

2.1.10 Diagnostics

The audit log size has been increased to 100,000 entries. The error log size has increased to 1,000 entries. Error and audit logs can be uploaded for printing but **printing audit logs directly from the Console or Virtual Console in payShield Manager has been disabled**.

Diagnostic tests for the hot swappable fan and power supply components have been added.

2.1.11 Monitoring

Changes have been made to payShield Monitor and SNMP.

- There is a new payShield 10K MIB.
- The SNMP port list is modified to allow the user to select between AUX port and Management ports only. Host ports are no longer supported.
- SNMP V1/V2 have been removed and community strings are no longer displayed, only version 3 is supported. Consequently, the prompt that was in the SNMP console commands for version has been removed.
- The prompt to enter a port for the trap now supports a default port of 162.
- AES-128 is provided as a privacy algorithm option in the payShield 10K.
- Objects related to ASYNC Host communications have been removed.
- Objects for the auxiliary Ethernet interface, Field Replaceable Units (FRUs) and battery state have been added.
- Objects for internal sensor processor and boot versions have been added.

2.1.12 Transitioning Smart Cards

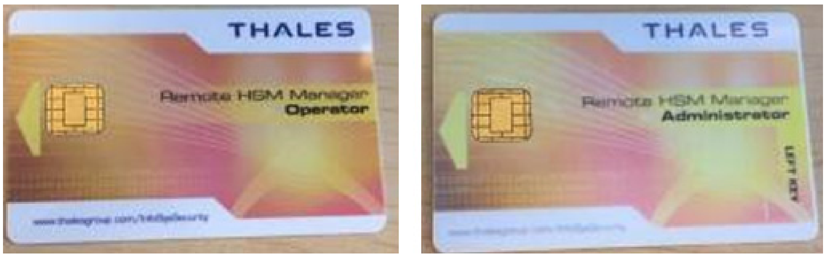
As discussed in Section 1.5, “Smart cards”, on page 11, the payShield 10K supports payShield Manager Smart Cards and HSM Smart Cards. The sections that follow provide guidance for migrating from non-supported Smart Cards to supported Smart Cards.

2.1.12.1 Transitioning legacy Manager Smart Cards

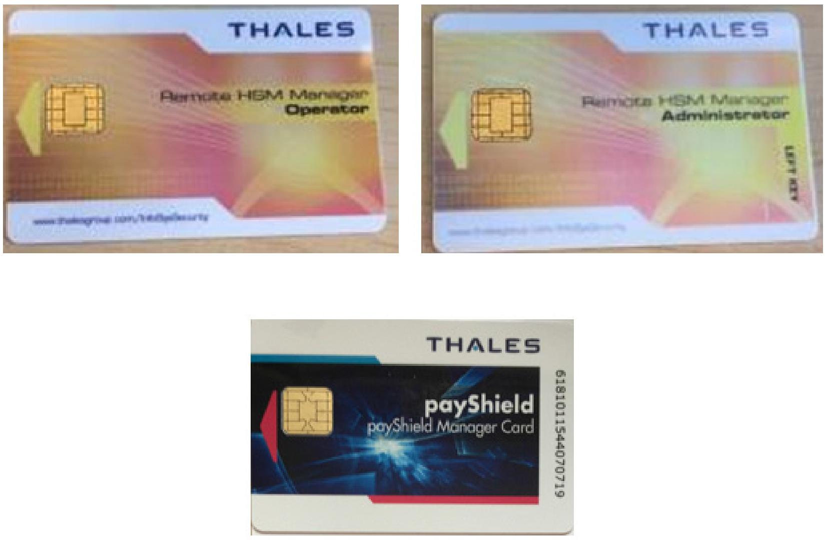
If you are using the old HSM Manager, you will need to migrate your legacy cards (see below) using payShield Manager on the payShield 9000, if you want to keep the same domain. This means updating the payShield 9000 to version 3.0 or above and then going through the payShield 9000 migration process, as outlined in the *payShield 9000 payShield Manager Manual*.

You will then have your CTA and LMK cards and ADMIN cards on the JAVA cards, which can be read by payShield Manager on the payShield 10K.

Non-supported Remote HSM Manager Smart Cards:



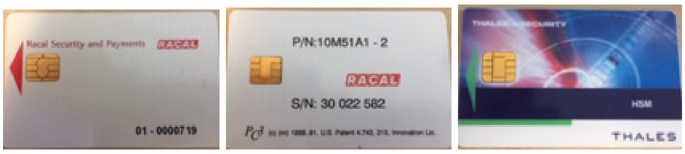
JAVA card which can be read by payShield Manager on the payShield 10K:



2.1.12.2 Transitioning non-supported legacy HSM Smart Cards

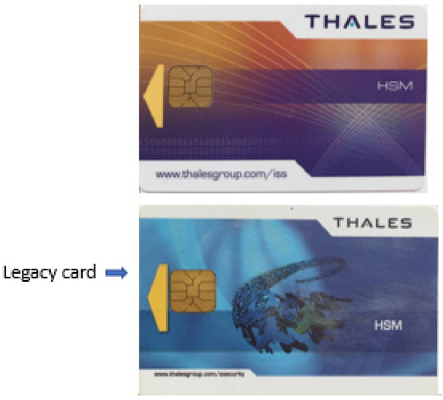
The legacy cards, shown below, are not supported in the payShield 10K.

Non-supported legacy HSM Smart Cards:



You will need to use your payShield 9000 to copy the information stored on the non-supported cards on to the supported LMK "component" cards before loading them into the payShield 10K.

Supported HSM Smart Cards:



2.1.12.3 Copying a card at the console

1. Connect the console using the USB-C and Tera Term or PuTTY.

   Note: The payShield can be in the ONLINE, OFFLINE or SECURE mode.

2. Use the 'FC' command (format card) to format X number of the supported cards.
3. Put the payShield into SECURE mode.
4. Use the 'DC' (Duplicate LMK Component Set) command to duplicate the component from the old card onto the new card.
5. Load the LMK into the payShield 10K.
6. Confirm that the LMK is working in the 10K.
7. Destroy the old LMK cards.

2.1.13 User Documentation

The payShield 10K user manuals are now available for download from the Thales support website.

Follow the link below and to download all the user manuals:

https://supportportal.thalesgroup.com/csm

3 Physical Description

Note: For the10G Ethernet Platform Variant, follow this link: Chapter 5, “payShield 10K 10G Ethernet Hardware Platform Variant”.

The payShield 10K can both stand alone or be part several units installed in a standard 19-inch cabinet.

• Overall rack dimensions (WxDxH)	1U rack 19” x 29” x 1.75” (482.6mm x 736.6mm x 44.5mm)

The unit is supported on telescopic runners that slide out via the front of the cabinet.

3.1 Front panel

3.1.1 Key locks and keys

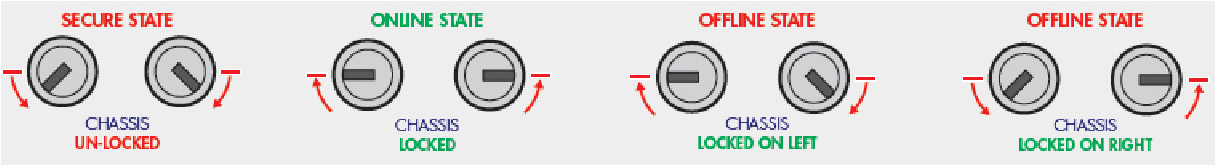
The front panel is equipped with two key locks. Each lock has its own key. Each key is assigned to a “key holder” (i.e., a security officer). To physically lock the unit into the rack, each key holder inserts their key into the appropriate lock and turns the lock to the locked position.

When in the locked position, the HSM cannot be removed from the rack.

The mechanical locking of the unit into the rack provides low level resistance to a direct attack. Note that the unit itself cannot be opened.

To remove the unit from the rack, both key holders insert their respective keys and turn the locks to the unlocked position.

3.1.1.1 Changing the HSM state via the key locks



Micro-switches attached to the locks allow the security state of the HSM to be changed.

Turning the cam lock keys changes the state of the HSM.

HSM states:

- Online (both locks are locked)
- Offline (one lock is locked and the other is unlocked)

- Secure (both locks are unlocked).

3.1.2 Smart Card Reader

The Smart Card Reader is an ISO card complaint type with automatic card ejection. The card is ejected at a standard point in HSM operation.

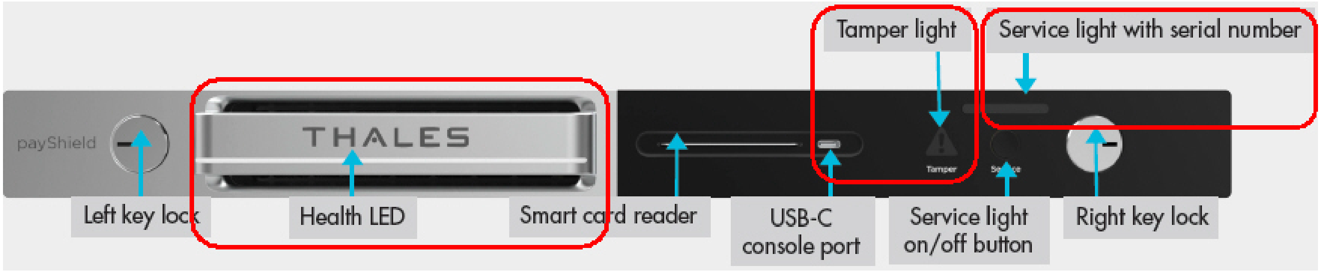
For example:

- At completion of a smart card related instruction from payShield Manager
- At completion of a smart card related Console command
- When the user presses the <Delete> key
- When the user presses CTRL-C key combination
- After a RESET
- During diagnostic testing

3.1.3 Front panel LEDs

There are three LED indicators on the front panel:

- Health (illuminating bar)
- Service (upper right)
- Tamper (warning triangle shape with exclamation mark)



3.1.3.1 Health LED

The Health LED is software controlled and readily identifies whether the unit is operational or if a fault condition exists.

LED Display	Indicates
Off	Power is off
White	Unit is operating properly
Flashing	Unit is booting. (Refer to Section 3.1.3.4, "Boot-up LED Sequence", on page 38)
Red	Errors exist. (Using payShield Manager, Navigate to **Status > Error Log**. Refer Section 8.3.2, "Status Tab", on page 91 for additional information.)

Note: After the error log has been read, the red LED reverts to white.

3.1.3.2 Service LED

The service switch is a momentary contact pushbutton switch used to signal that the Blue Service LED should be cleared.

The Service LED can be turned on by anyone either in the facility or remotely.

Note: There is also a Service LED on the back of the unit that mirrors the Service LED on the front of the unit.

Pushing the button toggles the state of the service function between on and off.

LED Display	Indicates
Off	No maintenance requested
Blue	The HSM has been selected for maintenance by an officer using payShield Manager or the button has been pushed by an operator in the data center

3.1.3.3 Tamper LED

The Tamper indicator illuminates when the HSM is triggered into an alarmed state by a security compromise. All secure data stored in the HSM is erased. When the sensor causing the alarm is no longer triggering, the HSM automatically reboots, and the Tamper LED is extinguished.

Note: To extinguish the LED, the HSM must be rebooted by powering off and powering on again. Following an alarm condition, the LMK(s) will need to be reloaded into the HSM. If the alarm condition is still present after rebooting, the Alarm LED remains illuminated; in this case the HSM must be returned to Thales for investigation and repair.

The tamper LED indicates if the unit is in a tampered state.

LED Display	Indicates
Off	No tamper
Flashing Red	Medium tamper
Solid Red	High tamper

3.1.3.4 Boot-up LED Sequence

As the system powers up, the LEDs display changes as the HSM moves through the power up sequence. The table below provides a key to the LED sequence.

LED Displays	Process
• All LEDs are turned on • Health LED toggles white/red twice	System LED test power up occurring
Health LED flashing white	Firmware Validation occurring
Health LED solid white	Firmware Validation complete
Health LED flashing Red	Application initialization occurring
Solid white or Solid red (Solid red indicates that there are errors in the error log.	Unit Operational

Table 1 Power up LED sequence

3.1.3.5 Blue LED

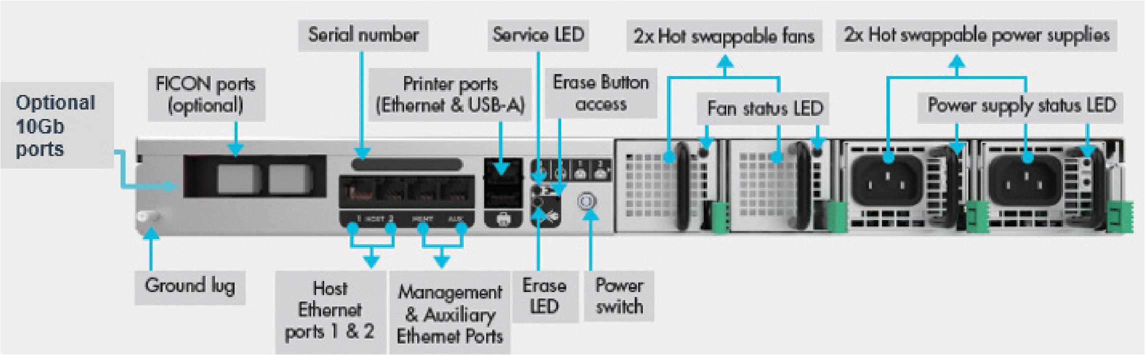
The blue service LED is indicates that the HSM requires service.

3.1.4 Air Inlets

The air inlets on the payShield 10K provide a cooling air entryway for the system and for power supplies.

3.2 Rear panel

Note: Follow this link for: Chapter 5, “payShield 10K 10G Ethernet Hardware Platform Variant”.



3.2.1 AC/DC power supplies

The payShield 10K is equipped with dual power supply units allowing the HSM to receive power from two independent supplies. This redundancy is designed to help prevent any operational break in the event of:

- An outage in either one of the power supplies
- Failure of either of the power distribution units within the HSM

Each supply has the following features:

- 450W power factor corrected high efficiency supply
- Universal AC Inlet, 90 to 264V 50/60 Hz
- 12V main output and 5V standby
- Over-voltage, over-current, over temperature protection
- Latching mechanism to hold the supply in place
- Internal variable speed fan for independent cooling
- Integral LEDs to provide operational status
- Management, status, and control signals on the internal interface

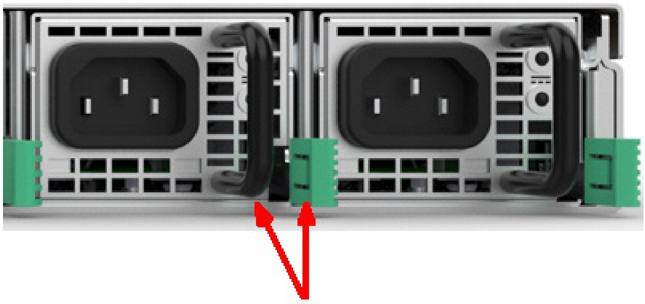
3.2.1.1 Swapping out the Power Supply

Note: The power supplies can be independently removed and replaced without removing the mains power from the other power supply. Each has a positive retention latch and status indicators.

1. Remove the AC supply cord from the PSU that you will be removing.

   Note: This is an important safety issue so you are not left holding a PSU that is still connected to the mains.

2. Using thumb and forefinger, gently press lever to the left to release the hold.

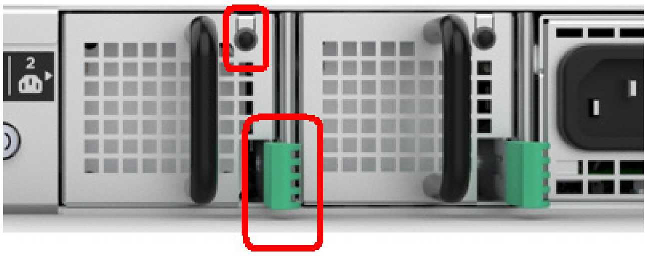


3. Slide the power supply out of chassis.
4. Slide the new power supply into chassis.

   Latches click as the power supply is secured into the chassis.

3.2.2 Fan trays

There are two redundant fans. Each fan has a positive retention latch and a status indicator.



Each fan tray can be independently removed and replaced without taking the system out of service.

Each fan tray contains the following elements:

- 20 CFM fan
- Latching mechanism to hold the tray in the chassis
- Status LED
- EEPROM for manufacturing data
- Temperature based fan speed control

3.2.3 Battery

The HSM contains one battery that provides power to the sensor processor. This battery is designed to last the lifetime of the product and requires no maintenance.

3.2.4 AC Power on/off switch

The AC Power on/off switch provides a way to remove primary voltage from the system. The switch illuminates when ON and is unlit when turned OFF.

Note: A standby voltage is always present when the HSM is connected to the mains power. This standby voltage minimizes the drain on the battery and controls the startup sequence when the power is turned on.

3.2.5 PCIe card interface

The HSM has a single PCIe interface slot.

3.2.6 Ethernet ports

Note: Follow this link for a description of the 10G Ethernet Hardware Platform Variant: Chapter 5, “payShield 10K 10G Ethernet Hardware Platform Variant”.

The HSM has five Ethernet ports.

- Two host ports

  Having two “hot” Ethernet host ports supports network resiliency. You can design dual independent network paths to the HSM, each port with its own IP address, both active, 64 threads on each.

- One management port

  payShield Manager uses this port for communication between the HSM and the Management PC.

- One service port

- One printer port

Note: When connecting serial or parallel interface devices to USB ports, it is essential that a USB adapter is acquired from Thales. Adapters are available for USB-Serial, USB-Centronics parallel, and USB-25 Pin parallel. Adapters from other sources must not be used as the payShield 10K will not have the required drivers.

3.2.7 USB Type A port

There is a single USB host interface with a type A connector. This interface provides power for the attached device, if it is required.

3.2.8 Erase Button and LED

The HSM has a recessed erase button. When pressed, critical security parameters are removed. This does erase volatile memory. After the erase operation is completed, an LED illuminates to confirm completion.

3.2.9 Ground Lug

A single ground lug is provided for system grounding of the chassis.

4 Installation

Note: For the10G Ethernet Platform Variant, follow this link: Chapter 5, "payShield 10K 10G Ethernet Hardware Platform Variant".

4.1 Pre-installation tasks

Before installing, you will need to address space, network and power requirements.

> **Note:** When planning the equipment installation, consideration should be given to the clearances required for servicing the equipment such as removing the unit from the front or removing power supplies and fan trays in the rear. This is typically at least 3 feet in the front of the rack and 1 foot behind the rack.
>
> **Attention:** Read the *payShield 10K Regulatory User Warnings and Cautions* document prior to installing the payShield 10K.

4.1.1 Mechanical and Electrical Specifications

4.1.1.1 Physical Characteristics

Characteristic	payShield 10K
Form Factor	1U Chassis
Rack Mount	1U 19"
Dimensions	19" x 29" x 1.75" (482.6mm x 736.6mm x.44.45mm)
Weight	15.9 kilograms (35 lbs)
Electrical Supply	0-264V AC Universal input, 47 to 63 Hz
Power Consumption	60W (maximum)
Operating Temperature	0 deg C to +40 deg C
Humidity	10% to 90% non-condensing @ +30C

4.1.1.2 Power Considerations

The payShield 10K is a Class I product and must be connected to a power supply system which provides an earth continuity connection.

Suitable cabling to the supply should be provided within the rack system. Consideration should be given to the rating information of the unit and the effects that overloading of circuits might have on the cabling and over-current protection devices. Ensure the wiring is in accordance with the requirements of any local wiring regulations.

4.1.1.3 Environmental Considerations

Consideration must be given to the airflow and temperature when the units are installed in a rack to ensure that this temperature is not exceeded.

Once installed, ventilation holes must not become obstructed, as that could reduce the airflow through the unit.

4.1.1.4 Battery consideration

Each HSM has a battery that maintains sensitive key material stored in protected memory while the external AC power is removed. Without any AC power, the battery will maintain the contents of protected memory for a minimum of 10 years. When the HSM is running on AC power, the battery is not used, and discharge is minimal.

4.2 Installation Procedure

Typically, the HSM is located within a protected corporate data center with multiple layers of security and access controls.

Note: Follow this link should you need to review the environmental considerations: Section 4.1.1, “Mechanical and Electrical Specifications”, on page 43.

Prerequisite:

- A Phillips screwdriver, #2.

1. Read the *payShield 10K Regulatory User Warnings and Cautions* document.
2. Gather the necessary personnel, e.g., security/trusted officers, trusted installer.
3. Verify that the shipment never left the custody of the shipper and log the receipt of the shipment in accordance with your security policies.
4. Unpack the Thales shipping container.

   The box contains:

   - 1 payShield 10K HSM
   - 2 AC power cables
   - 4 security keys (2 copies - 4 total keys)

- 1 USB-C to USB-A cable (for console connectivity)

Note: In certain circumstances, the security keys and the smart cards may be delivered to your two designated key-holders under separate cover (i.e., not included in the box). If the security keys have been delivered separately, the presence of both designated key-holders is required.

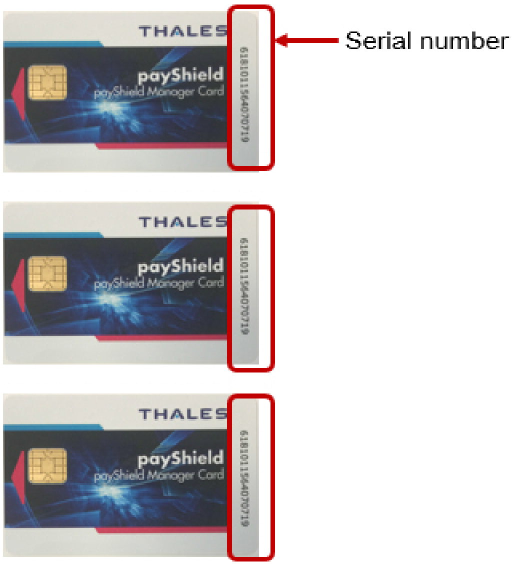
5. Confirm the contents of the box.

   – Verify that the serial number on the bag matches the shipping document.

6. Record the HSM serial numbers in accordance with your security policy.

7. Record the serial number of each smart card in accordance with your security policy.

   Note: The serial number is located along the right edge of the smart card.



Note: Each card may be assigned to an individual security officer. Each officer should also maintain a record of their smart card's serial number.

8. Store the serial number records in accordance with your security policy.

9. Mount the rack.

   a) Unpack the Thales box containing the Thales Universal Rack Mount Kit. The Mount Kit contains 2 rails and 10 M4 x 6 mm screws.

   Note: The 1U 1000 mm Universal Rack Mount Kit is pre-assembled for use with square hole and unthreaded round hole racks. This rack kit is suitable for racks and cabinets where the depth between front and rear posts is in the range 685.8mm – 939.8mm.

   b) Remove inner rail from rack mount assembly.

   - Slide the inner rail until the safety catch locks.
   - Depress the safety catch and continue sliding to separate the inner and outer rails.

   c) Attach inner rail to the chassis.

    - Position the inner rail on the side of the product with the safety catch toward the rear.
    - Align the rear hole of the rail with the rear hole on the chassis and attach using the M4 x 6mm screws provided.
    - Align the other 4 holes with the counter sink in the rail with the corresponding holes in the chassis, insert the M4 x 6mm screws, and tighten all the screws.
    - Repeat this to attach the second inner rail to the other side of the chassis.

  d) Adjust rail length. (The rails support a range of rack mounting depths.)

    - Loosen the two rear retaining plate screws to enable the rear bracket to be extended.

  e) Install outer rails into the rack.

    - Align the bracket marked “FRONT” with the holes in the front post.
    - Once aligned, push the bracket forward until the snap mechanism engages.
    - Slide the rear bracket towards the rear post of the rack.
    - Align the bracket with the holes in the rear post at the same vertical position used for the front and snap it in.
    - Tighten the two rear retaining screws.

  Attention: Slide the bearing retainer all the way forward to avoid damaging the rail kit when the product is installed.

  f) Insert product into the outer rails.

    - With both the left and right bearing retainers moved the entire way forward, align the inner rails mounted on the product with the outer rails mounted in the rack.
    - You may need to apply gentle pressure to the ends of the inner rails to align them with the outer rails.
    - Slide the product into the rack until the safety latches engage.

  g) Push the safety catches in on both sides and slide the product fully into the rack. When sliding the unit into the rack for the first time, the last few inches of travel may experience some resistance as the bearing retainers meet their backstops. The resistance can be overcome by applying slightly more force to the front of the unit to achieve full insertion into the rack.

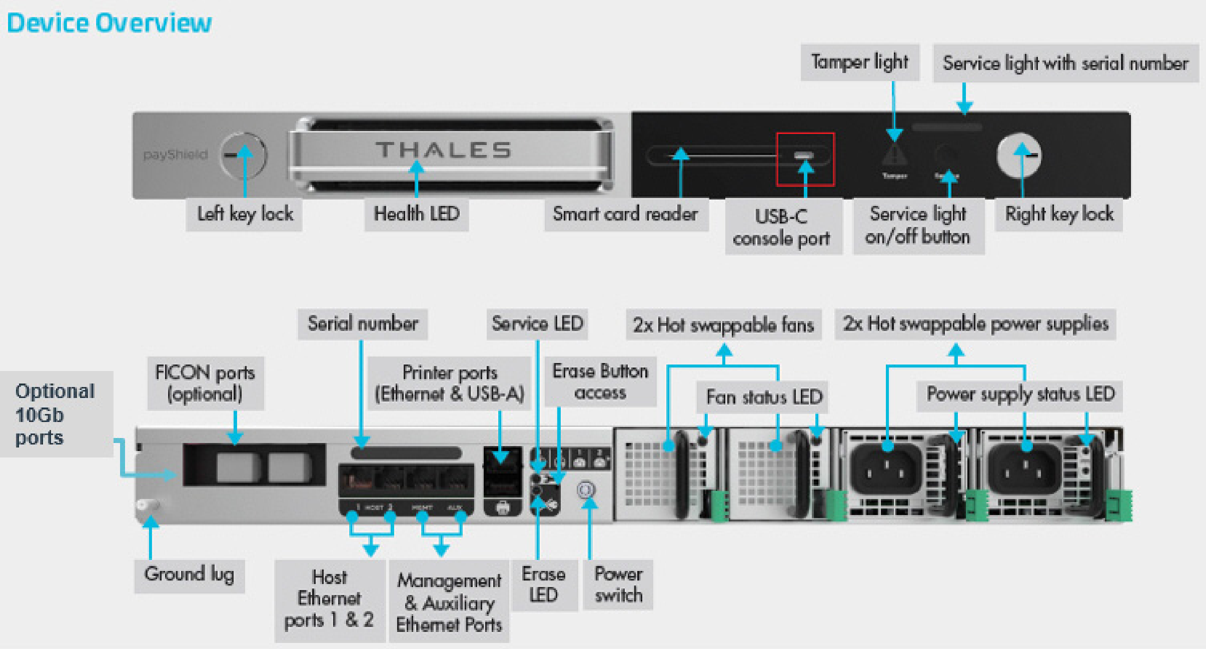
10. Physically lock the unit into the rack.

    - Each key holder inserts their key into their respective lock and turns the lock to the locked position.

11. Connect your HSM to your Host using an Ethernet connection.

12. Connect the power cables.

13. Push the power switch (located on the back of the unit) to turn the unit on.



As the system powers up, the LEDs display changes as the HSM moves through the power up sequence. The table below provides a key to the LED sequence.

LED Displays	Process
• All LEDs are turned on • Health LED toggles white/red twice	System LED test power up occurring
Health LED flashing white	Firmware Validation occurring
Health LED solid white	Firmware Validation complete
Health LED flashing Red	Application initialization occurring
Solid white or Solid red (Solid red indicates that there is an error in the error log. The light extinguishes when you read the error log.)	Unit Operational

Table 2 Power up LED sequence

- Follow this link to connect using payShield Manger: Chapter 6, “payShield Management Options”.
- Follow this link to connect using the console: Chapter , “Commission payShield Manager using Console Commands”

5 payShield 10K 10G Ethernet Hardware Platform Variant

5.1 Introduction

A variant of the standard payShield 10K hardware platform is available supporting 10G Ethernet. This can be ordered in place of the standard PS10-S payShield 10K Ethernet Hardware Platform using the following part number:

Part Number	Description
971-000055-001	PS10-D payShield 10K 10G Ethernet Hardware Platform

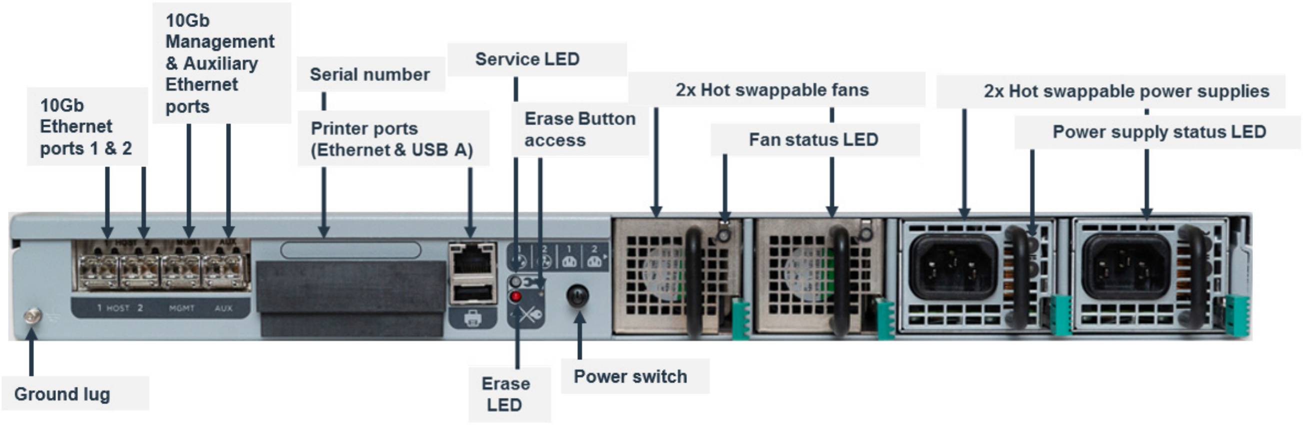
10G (or 1G) Ethernet only is provided on all four Ethernet ports, i.e., Host Port1, Host Port2, Management Port and the Auxiliary port. Transceivers for connection to either copper or optical networks must also be ordered for each port using the part number below:

Part Number	Transceiver type
971-000042-001	PS10-D-SFP+10G-OPT payShield 10K 10G Transceiver SFP+ Short Range 1GbE/10GbE Optical (1 off)
971-000043-001	PS10-D-SFP+10G-CPR payShield 10K 10G Transceiver SFP+ 10GbE RJ-45 Copper (1 off)

As with the standard PS10-S model, a Software Package with Performance must be ordered together with the Hardware Platform as well as any optional licenses and hardware accessories as required.

Support for the PS10-D model is provided in base software version v1.1a and above.

5.2 Rear Panel Overview



5.3 General Notes

- payShield 10K 10G Ethernet Hardware Platform has 4 ports for connecting to a 10G network using the transceivers ordered separately. The transceivers must be connected to a switch or router that supports 10G Ethernet.
- All 4 ports support hot plugin.
- The port settings can be viewed using the QH, QM, and QA console commands, using payShield Manager and using SNMP.
- The speed of the interface is NOT configurable. The only option allowed is “Auto select”. The actual value is negotiated by the interface. The Optical and Copper transceivers can be 1GbE or 10GbE, auto-selected by negotiation.
- When the 10G ports are present, the QUAD Small Form-factor Pluggable (SFP) ports replace the covered Native Ethernet ports.

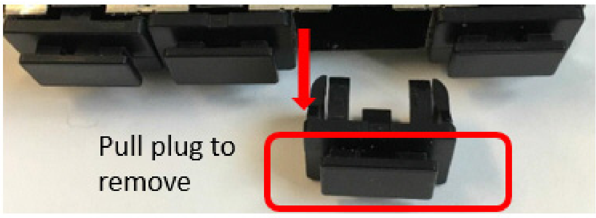
5.4 Installing 10Gb ports

Note: The SFP transceivers can be independently removed and replaced without removing the mains power.

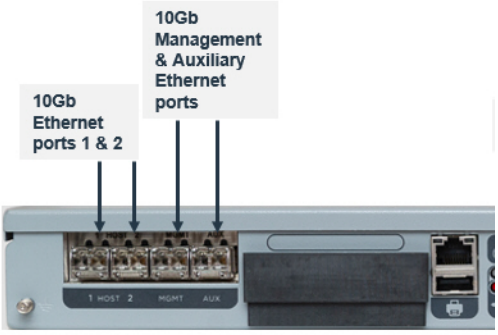
1. Remove the SFP transceivers from packaging.

   Note: The package contains 4 International Integrated Reporting Council (IIRC) SFPs.

2. Remove the plugs that cover the SFP ports.



3. Slide each SFP into a port slot. (Each SFP can be either copper or optical or a mixture.)
   - If a mixture, the media type SFP must match the site requirement.
   - Host 1 in port 1, Host 2 in port 2, Management in port 3, AUX in port 4.


10Gb Management & Auxiliary Ethernet ports
10Gb Ethernet ports 1 & 2
1 HOST 2
MGMT
AUX

4. After removing any cable connection dust covers, attach the cables to ports.

5.5 Power Consumption

- When using 4 optical ports, the max is 70W
- When using 4 copper ports, the max is 80 W
- When using a mixture, the max is 70W to 80W depending on usage

6 payShield Management Options

Thales recommends that payShield Manager is used to manage payShield 10K. payShield Manager provides a secure, authenticated connection allowing a full “remote console”.

payShield Manager is a web-based management application. Management is performed over the network using a web-based interface hosted on payShield. The operator can be either local or remote to the payShield 10K.

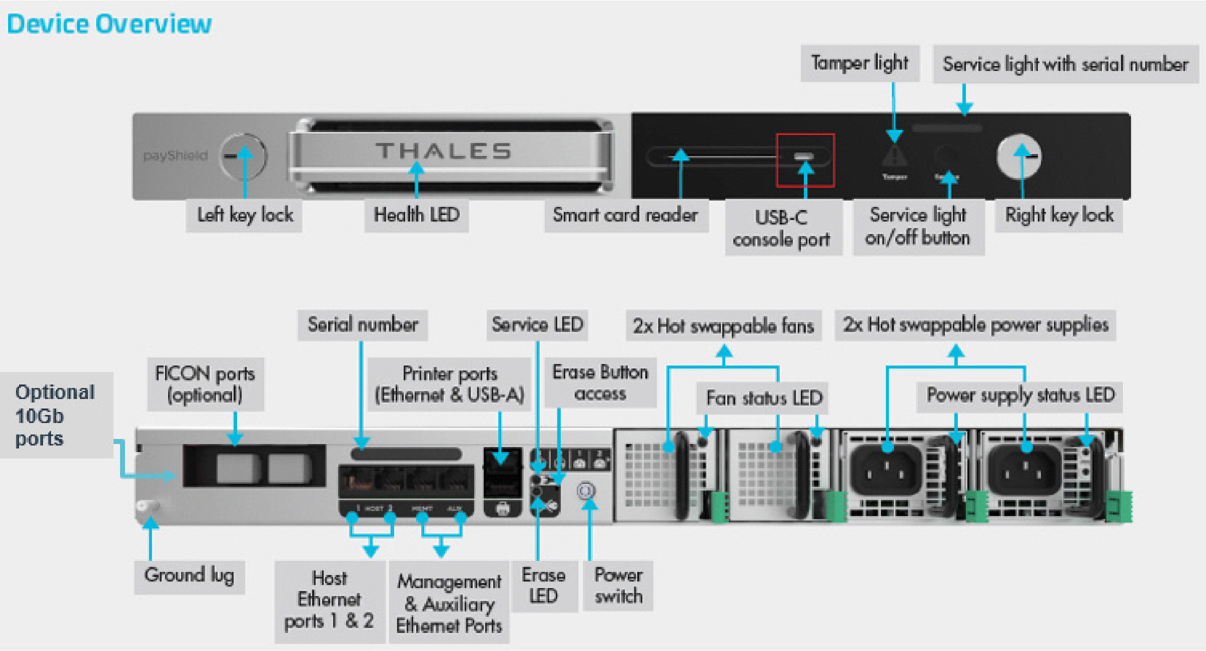
The key feature of using payShield Manager remotely is that it does not require a visit to the Data Center. Rather management is undertaken using a standard web-browser connecting to the payShield 10K over TCP/IP networks, where the payShield 10K is located within a protected corporate data center with multiple layers of security and access controls.

With a standard PC with a supported web-browser, together with the USB connected payShield Manager Reader and payShield Manager smart cards, users connect to the payShield 10K via HTTP(s) using a configured IP address or the HSM’s system name.

To use payShield Manager locally, the PC hosting payShield Manager is connected directly into the payShield 10K’s Ethernet management port. Local payShield Manager is included in all payShield 10K license packages.

To use payShield Manager remotely the PC hosting payShield Manager is connected remotely via the network again to the payShield 10K’s Ethernet management port. The Remote payShield Manager License is required to use this option.

payShield 10K can also be managed using the Console. Here the smart card reader on the front panel is used together with LMK Component Smart cards. The Console Commands are described in Appendix A, Console Commands.



7 Commission using payShield Manager

7.1 Introduction

This Chapter describes how to commission payShield 10K using payShield Manager. The same method is used whether you are commissioning locally or remotely.

The steps included take a payShield 10K installed in the Data Center, as described in Chapter 8, “Using payShield Manager”, to a state ready for generating / loading the Local Master Key and updating the configuration – this is covered in Chapter 10 Using payShield Manager.

7.2 Prerequisites

The following are required before starting the commissioning procedure:

- payShield 10K installed in a cabinet with the keys on the front panel set to “online” as covered in Chapter 4, “Installation”.
- The payShield 10K serial number in order to use the default network name to access the device.
- PC or Workstation with the operating system / browser combinations supported by payShield Manager. These are given in the release note for each version of payShield 10K software and typically include:
    - Windows 10 with either Chrome of Firefox
    - Linux Ubunto with either Chrome or Firefox
    - MAC OSX Mohave with Chrome
- Administration permissions for the PC or Workstation to install drivers and update the configuration etc.
- payShield Manager USB attached smart card reader with PIN Pad
- payShield Manager smart cards in sufficient quantity to complete the commissioning process.

7.3 Preparing for Commissioning

The following steps need to be undertaken before commissioning starts:

7.3.1 Configuring payShield 10K for Static IP (if required)

payShield 10K management port is configured for DHCP when delivered, allowing it to be managed remotely following installation in the Data Center. If a Static IP address needs to be set up, this must be configured in the Data Centre using the Console Commands described in Appendix A - Console Commands on page 207 before continuing.

7.3.2 Install Smart Card Reader Driver

The driver for the smart card reader used must be installed on the PC / Workstation.

Two readers with PIN Pad are supported:

- HSM-RMGT-RDR2 payShield Manager Smart Card Reader which uses the cyberJack® secoder (USB) from Reiner
- HSM-RMGT-RDR payShield Manager Smart Card Reader which uses the HID® OMNIKEY® 3821 Smart Card reader.

For the cyberJack® secoder (USB) reader, the driver is available on-line at:

https://www.reiner-sct.com/support/support-anfrage/?productGroup=77304735&product=77304824&q=driver#choice4

For the HID® OMNIKEY® 3821 Smart Card reader the driver is available on-line at:

https://www.hidglobal.com/drivers

7.3.3 Check the Proxy Configuration

Your Internet browser will need to be configured to direct traffic through a proxy.

When you are configuring the browser proxy settings, click **Use this proxy server for all protocols**. For Internet Explorer and Mozilla Firefox, this setting is via a check box.

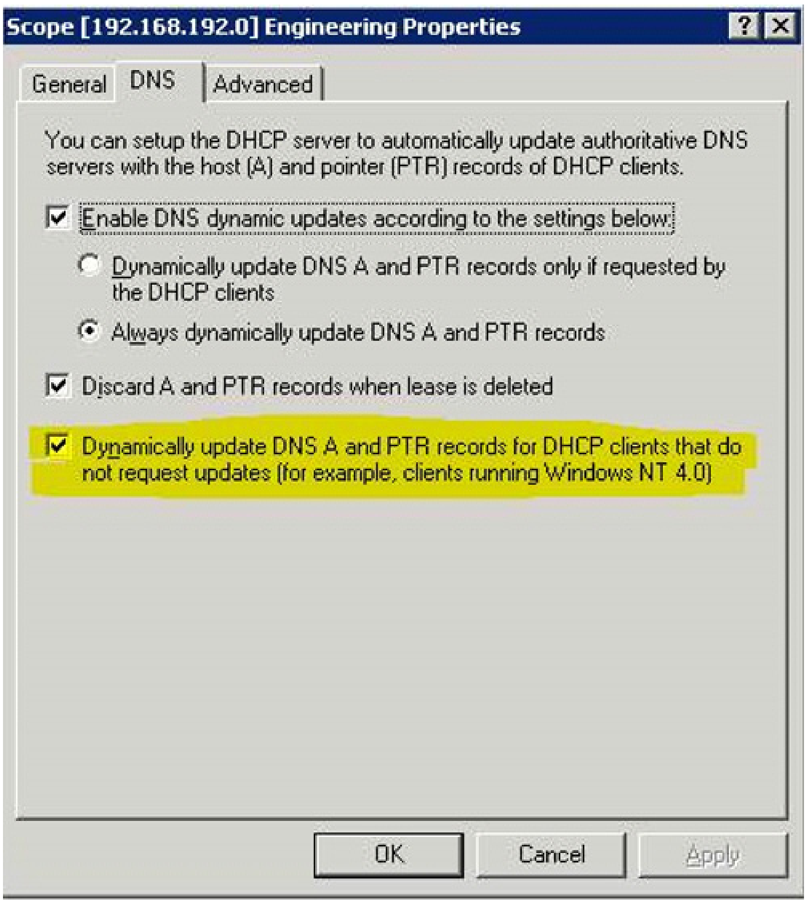
If this is setting is not selected, the payShield Manager Welcome page will display, but you will not be able to login.

7.3.4 Configure DNS

When configuring the DNS in a Windows Server environment, select the setting:

- Dynamically update DNS A and PTR records for DHCP clients that do not request updates.

Note: The DHCP request from the payShield 10K is going to request an IP address and also request a name (with -h option on DHCP client). This option pushes the name and assigned IP address to the DNS.



You can setup the DHCP server to automatically update authoritative DNS servers with the host (A) and pointer (PTR) records of DHCP clients.

☑ Enable DNS dynamic updates according to the settings below:

○ Dynamically update DNS A and PTR records only if requested by the DHCP clients

● Always dynamically update DNS A and PTR records

☑ Discard A and PTR records when lease is deleted

☑ Dynamically update DNS A and PTR records for DHCP clients that do not request updates (for example, clients running Windows NT 4.0)

7.3.5 Connect to the Network

Connect the laptop or Workstation to be used for payShield Manager to payShield 10K using Ethernet as follows:

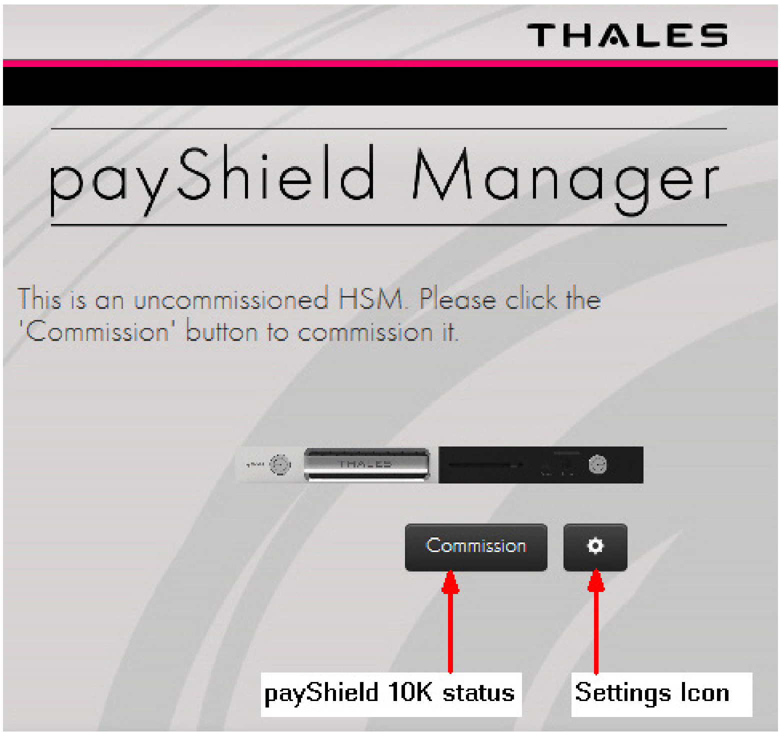
- To use payShield Manager locally, the PC hosting payShield Manager is connected directly into the payShield 10K's Ethernet management port on the rear panel. Local payShield Manager is included in all payShield 10K licence packages.
- To use payShield Manager remotely, the PC hosting payShield Manager is connected remotely via the network again to the payShield 10K's Ethernet management port. The Remote payShield Manager Licence is required to use this option.

7.4 Connecting to payShield 10K, Installing Browser Extensions and Configuring Smart Card Reader

7.4.1 Connecting to payShield 10K

To connect to payShield 10K using payShield Manager and display the “landing page” proceed as follows:

Using the browser on the laptop / workstation being used for payShield Manager, enter the network name or the IP address assigned and access the page. The landing page below is displayed:



This is an uncommissioned HSM. Please click the 'Commission' button to commission it.

Notes:

- The default network interface name for payShield 10K is “<serial number>-mgmt”
- Refreshing the landing page can repair most connectivity issues with accessing the landing page. However, once logged in, refreshing any page will end the current session and you will be required to log back in.
- The Settings/Tools Icon: Allows card reader configuration, the TLS certificate to be downloaded, and the Smart Card to be inspected. Additionally, selecting the icon displays the bridge’s current version.
- If you are already commissioned, simply insert a right or left RACC into the connected Smart Card reader, click Log In and enter your PIN. If the PIN is correct an authentication process will begin which will take several seconds to complete and you can use the functionality described in Chapter 8, “Using payShield Manager”.

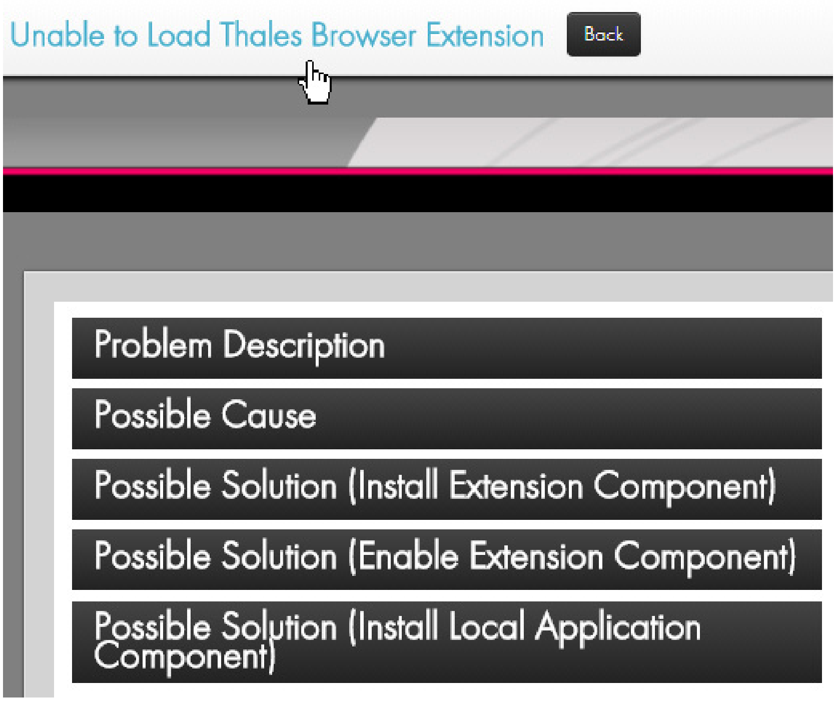
- When using MacOS Catalina there are a few additional steps to be carried out before the landing page can be accessed. These are described in Section 7.6.1, “Using payShield Manager with MacOS Catalina”, on page 85.

7.4.2 Installing Thales Browser Extensions

From the Landing Page, click **Commission**.

If the **Unable to load Thales Browser Extension** message is displayed (as shown in the screen shot below), follow the steps below

Otherwise, continue to Section 7.4.3, “Configure the Smart Card reader”, on page 65.



Unable to Load Thales Browser Extension

Back

Problem Description

Possible Cause

Possible Solution (Install Extension Component)

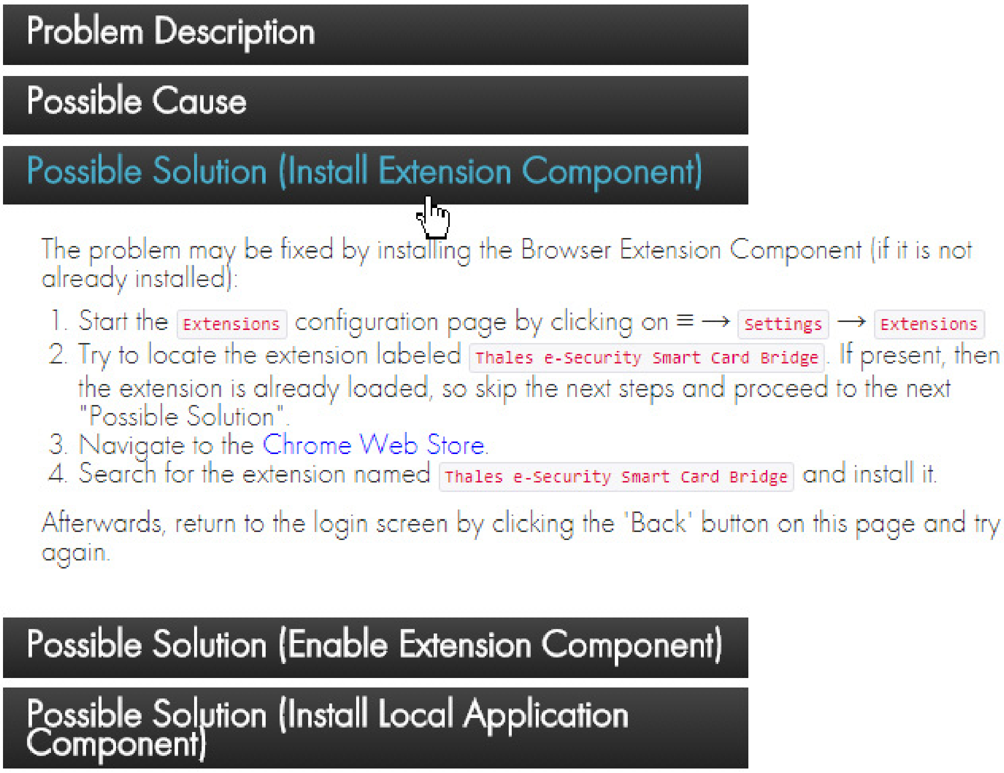
Possible Solution (Enable Extension Component)

Possible Solution (Install Local Application Component)

Note the following procedure is for Chrome. For other browsers, payShield Manager will guide the user through a similar but slightly different process to load the required extensions.

Additional actions are needed to load the Thales Browser Extension. Follow the prompts as described below.

1. Open the **Problem Description** and **Possible Cause** drop downs.
2. Open the **Possible Solution** drop down menus.
3. Follow the instructions under **Possible Solution (Install Extension Component)**.



Problem Description

Possible Cause

Possible Solution (Install Extension Component)

The problem may be fixed by installing the Browser Extension Component (if it is not already installed):

1. Start the `Extensions` configuration page by clicking on ≡ → `Settings` → `Extensions`
2. Try to locate the extension labeled `Thales e-Security Smart Card Bridge`. If present, then the extension is already loaded, so skip the next steps and proceed to the next "Possible Solution".
3. Navigate to the Chrome Web Store.
4. Search for the extension named `Thales e-Security Smart Card Bridge` and install it.

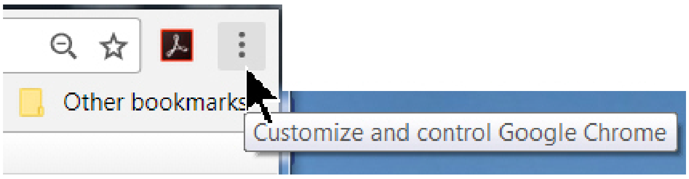
Afterwards, return to the login screen by clicking the 'Back' button on this page and try again.

Possible Solution (Enable Extension Component)

Possible Solution (Install Local Application Component)

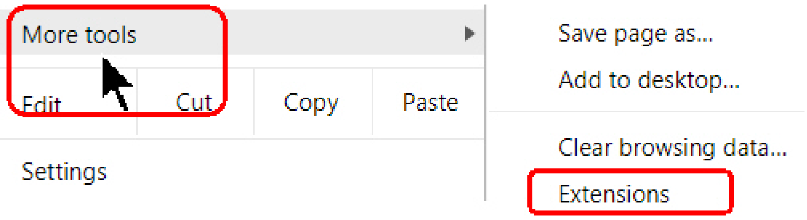
4. Follow the instructions under **Possible Solution (Enable Extension Component)**.

   a) Click the **More** icon.

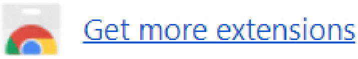


   b) Navigate to:

   More tools > Extensions

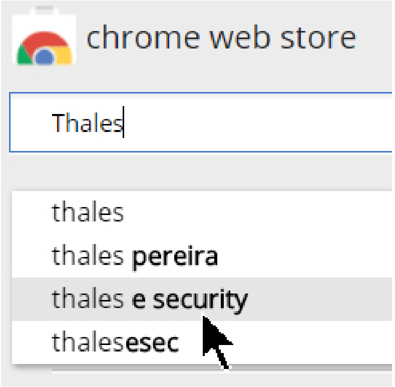


   c) Scroll through the list of Extensions, if a **Thales Extension** is not present, Click **Get more extensions**.

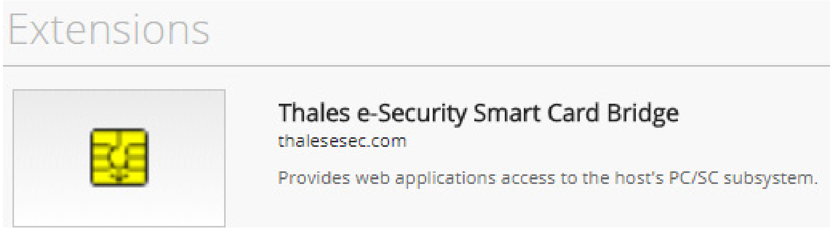


The Chrome web store opens.

d) Type in **Thales** and click **thales e security**.



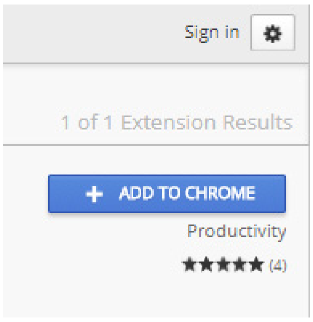
The Thales eSecurity Smart Card Bridge Extension displays.



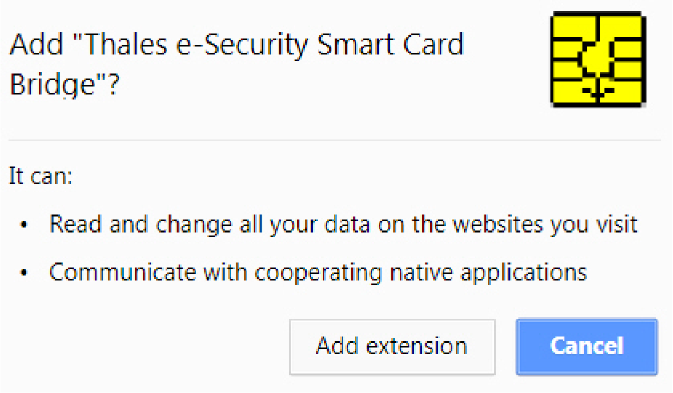
Thales e-Security Smart Card Bridge
thalesesec.com

Provides web applications access to the host's PC/SC subsystem.

e) Click **ADD TO CHROME**.



The system displays:



Add "Thales e-Security Smart Card Bridge"?

It can:

- Read and change all your data on the websites you visit
- Communicate with cooperating native applications

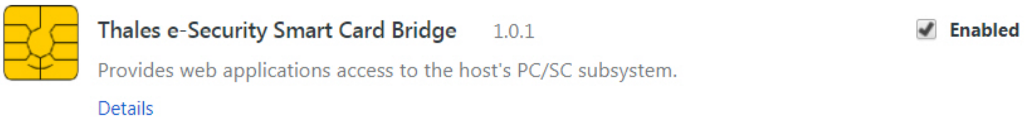
f) Click **Add extension**.

A load confirmation message displays.

g) Confirm that the extension is **Enabled**.

Navigate back to: **More Tools > Extensions**

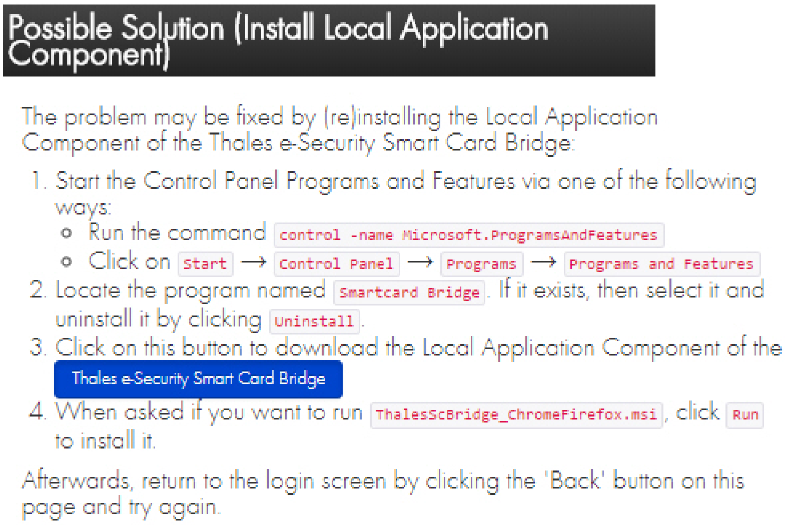
Scroll to the Thales extension and confirm that the Enabled box is checked.



Thales e-Security Smart Card Bridge 1.0.1

Provides web applications access to the host's PC/SC subsystem.

5. Follow the instructions under **Possible Solution (Install the Local Application Component)**.



Possible Solution (Install Local Application Component)

The problem may be fixed by (re)installing the Local Application Component of the Thales e-Security Smart Card Bridge:

1. Start the Control Panel Programs and Features via one of the following ways:
   - Run the command `control -name Microsoft.ProgramsAndFeatures`
   - Click on `Start` → `Control Panel` → `Programs` → `Programs and Features`
2. Locate the program named `Smartcard Bridge`. If it exists, then select it and uninstall it by clicking `Uninstall`.
3. Click on this button to download the Local Application Component of the Thales e-Security Smart Card Bridge
4. When asked if you want to run `ThalesScBridge_ChromeFirefox.msi`, click `Run` to install it.

Afterwards, return to the login screen by clicking the 'Back' button on this page and try again.

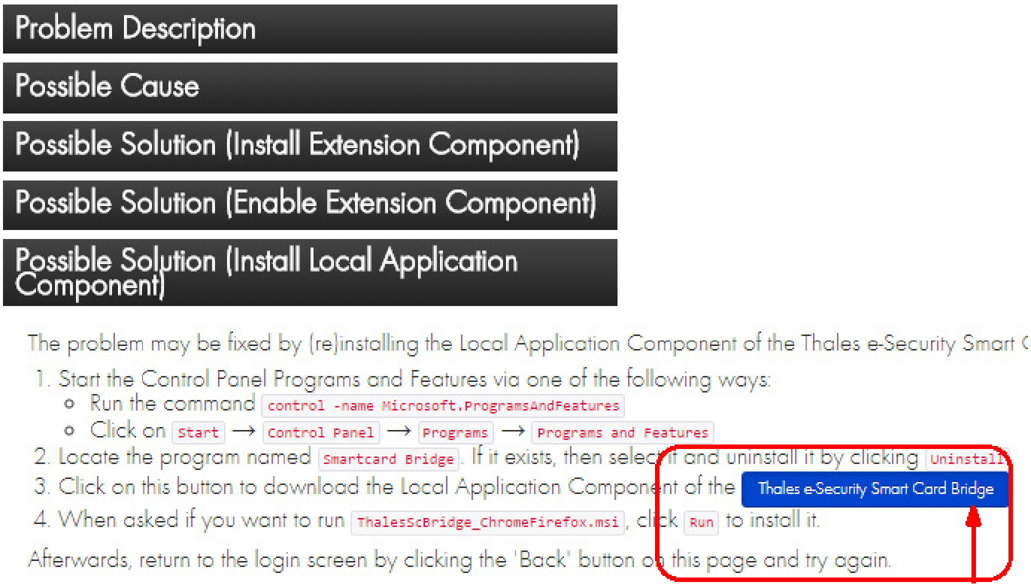
a) Navigate to:

Start > Control Panel > Programs > Programs and Features

b) If you find an existing Smart Card Bridge, select it and click to **Uninstall**.

c) Return to your payShield Manager window.

d) Click the blue button as shown below.



Problem Description

Possible Cause

Possible Solution (Install Extension Component)

Possible Solution (Enable Extension Component)

Possible Solution (Install Local Application Component)

The problem may be fixed by (re)installing the Local Application Component of the Thales e-Security Smart C

1. Start the Control Panel Programs and Features via one of the following ways:
   - Run the command `control -name Microsoft.ProgramsAndFeatures`
   - Click on `Start` → `Control Panel` → `Programs` → `Programs and Features`
2. Locate the program named `Smartcard Bridge`. If it exists, then select it and uninstall it by clicking `Uninstall`
3. Click on this button to download the Local Application Component of the Thales e-Security Smart Card Bridge
4. When asked if you want to run `ThalesScBridge_ChromeFirefox.msi`, click `Run` to install it.

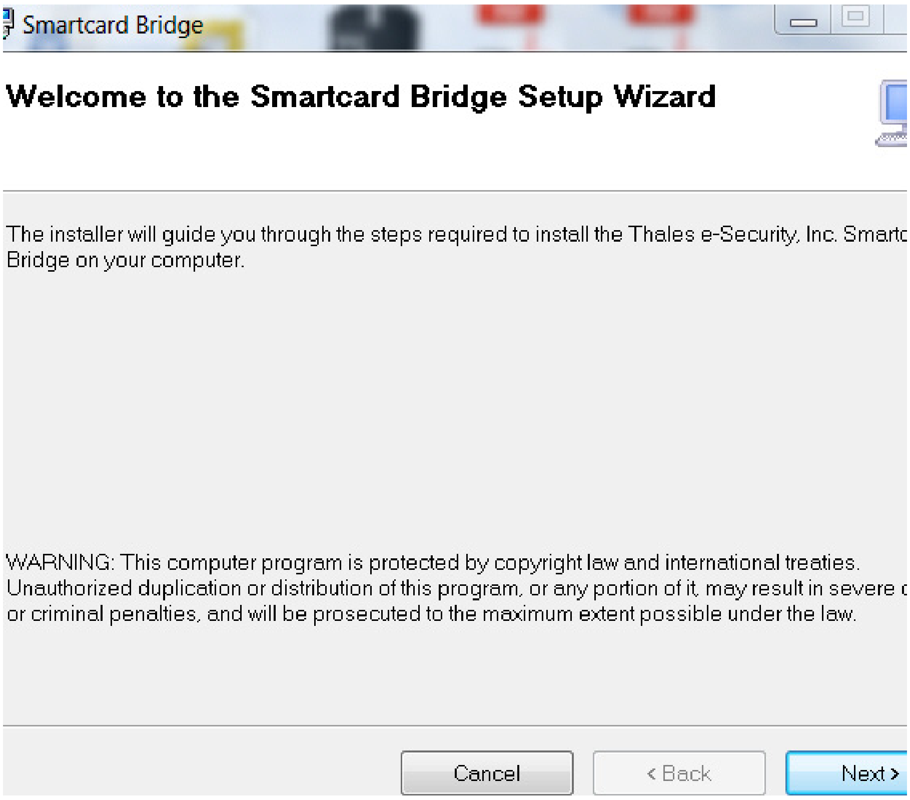
Afterwards, return to the login screen by clicking the 'Back' button on this page and try again.

The ThalesScBridge_ChromeFoxFire.msi downloads.

e) Click **Run**.

The Smart Card Bridge Setup Wizard Opens.

f) Click **Next**.



Smartcard Bridge

Welcome to the Smartcard Bridge Setup Wizard

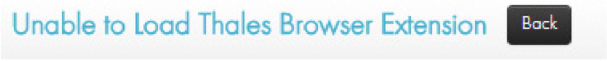
The installer will guide you through the steps required to install the Thales e-Security, Inc. Smartc Bridge on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe c or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

g) Click **Next** a second time to confirm.

h) Follow the instructions as prompted.

i) Click **Back** to return to the payShield landing page.

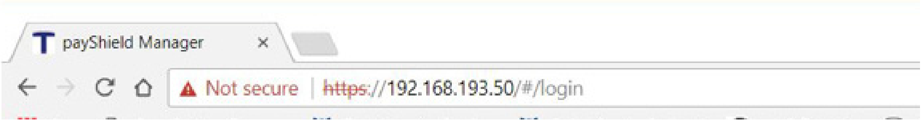


Unable to Load Thales Browser Extension

j) Close your payShield session.

6. From your Internet browser, enter the network name or IP address.

   Example:

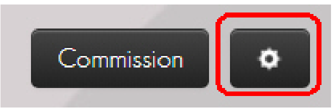


~~https~~://192.168.193.50/#/login

The landing page opens.

7.4.3 Configure the Smart Card reader

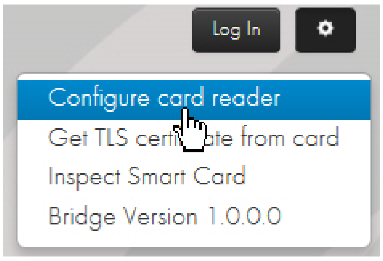
1. From the landing page, click on the **Settings** icon.



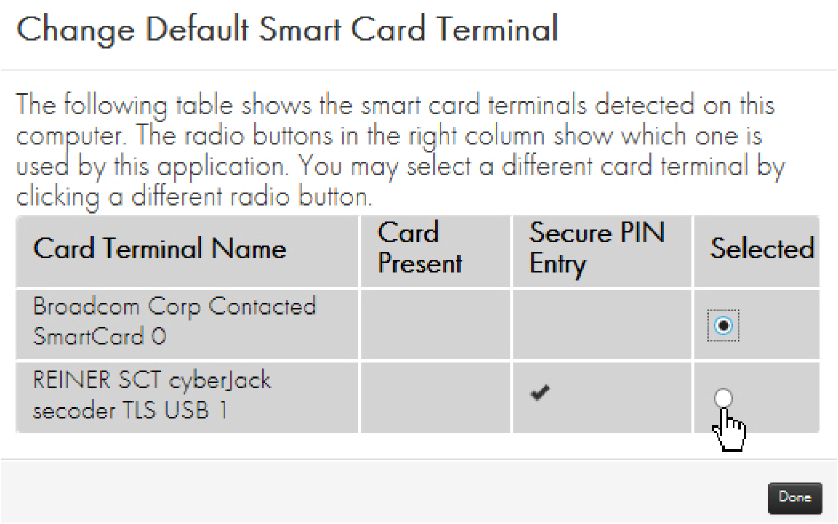
2. Confirm that the pop-up menu displays:

   Bridge Version 1.0.0.0

3. Click **Configure card reader**.



The Change Default Smart Card Terminal window opens.



Change Default Smart Card Terminal

The following table shows the smart card terminals detected on this computer. The radio buttons in the right column show which one is used by this application. You may select a different card terminal by clicking a different radio button.

Card Terminal Name	Card Present	Secure PIN Entry	Selected
Broadcom Corp Contacted SmartCard 0			●
REINER SCT cyberJack secoder TLS USB 1		✓	○

Note: In the image above, the PC has an internal Smart Card reader, for example: Smart Card 0. **Do not Click** this internal Smart Card reader. **It is not a trusted verification device**.

In the example above, **REINER SCT cyberJack secoder TLS USB1** is the trusted verification device.

Note: If after selecting the trusted verification Smart Card reader, you unplug the reader from your PC and/or reboot, you may need to come back and repeat this selection process.

4. Select the trusted verification device.

5. Click **Done**.

You are returned to the landing page.

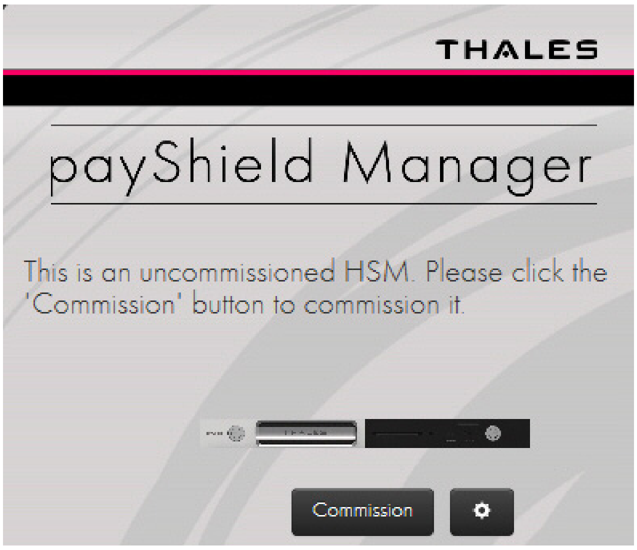
7.5 Commissioning payShield 10K

This section describes the steps required to complete the commissioning of the payShield 10K ready for LMK eneration / LMK installation and configuration.

Table 3 Commissioning Checklist

Step	Task	Go to Section	DONE
1.	Load a Security Domain: • Install an existing security domain. This can be a payShield 9000 domain. OR: • Create a new security domain.	• Section 7.5.3, “Load the Security Domain”, on page 73 • Section 7.5.2, “Create a new Security Domain”, on page 68	
2.	Set the HSM Recovery Key (HRK) passphrases.	Section 7.5.4, “Set HSM Recovery Key (HRK) passphrases”, on page 78	
3.	Create left and right key RACCs.	Section 7.5.5, “Create Left and Right Remote Access Control key cards”, on page 79	
4.	Create your trusted officers/authorizing officers.	Section 8.3.3, “Operational Tab”, on page 92	

7.5.1 Open the Commissioning Wizard page

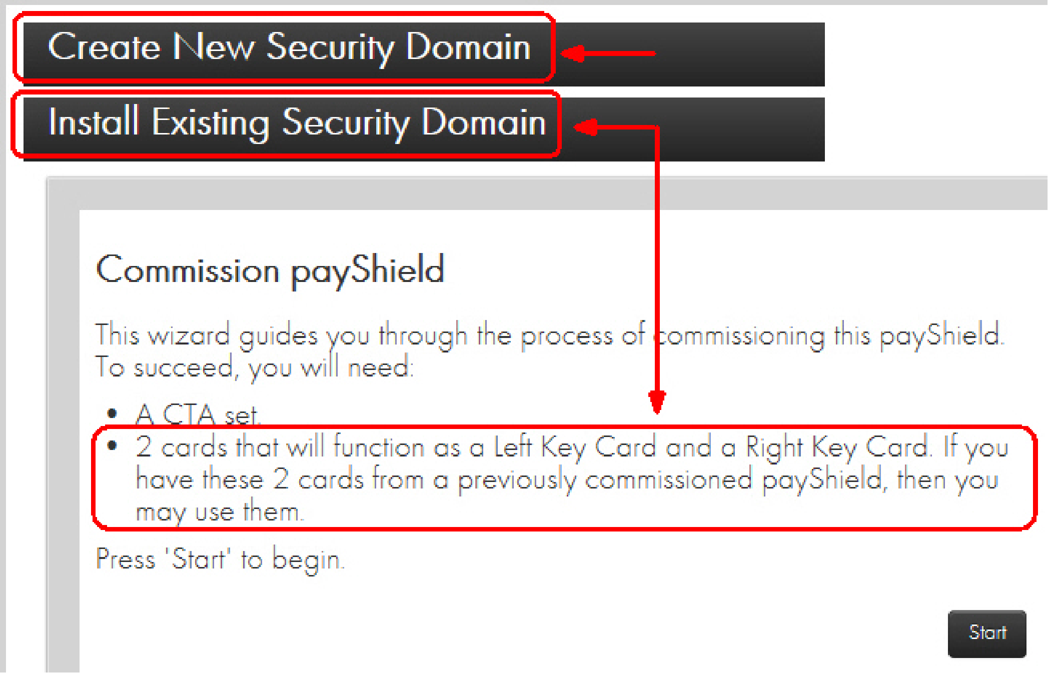


This is an uncommissioned HSM. Please click the 'Commission' button to commission it.

1. Click **Commission**.

   The payShield Manager's **Commission HSM** wizard landing page opens.

   From the landing page you have two options:



Commission payShield

This wizard guides you through the process of commissioning this payShield. To succeed, you will need:

- A CTA set.
- 2 cards that will function as a Left Key Card and a Right Key Card. If you have these 2 cards from a previously commissioned payShield, then you may use them.

Press 'Start' to begin.

- If you already have a Security Domain (i.e., you have previously created a security domain with these cards), you are ready to install, i.e., continue to Section 7.5.3, “Load the Security Domain”, on page 73.

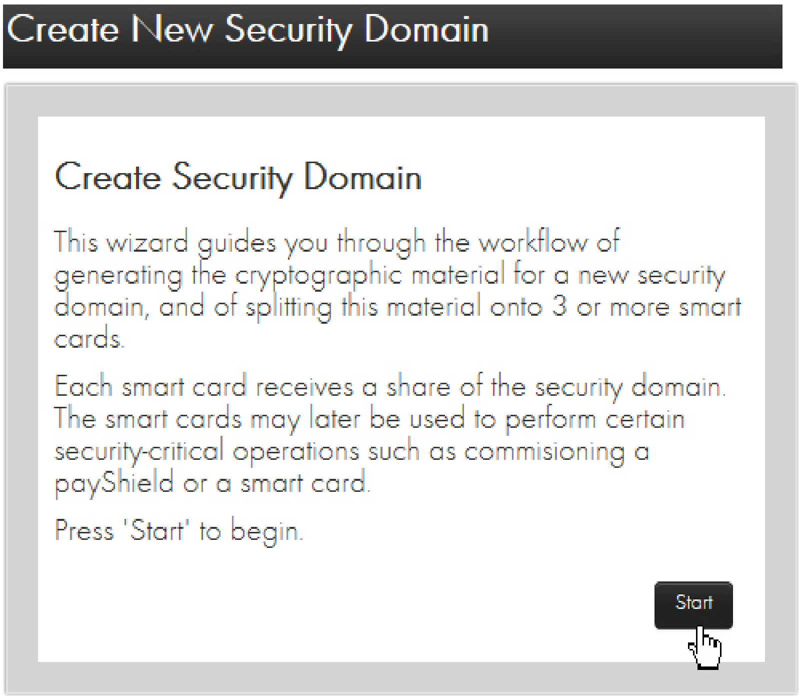
- If you are unsure of the status of your cards and prefer to create a new security domain, i.e., continue to Section 7.5.2, “Create a new Security Domain”, on page 68.

Note: When re-using existing Smart Cards, you must know the PIN. You will continue to use the existing PIN. The system will not prompt you to create a new PIN. The existing PIN is not erased.

7.5.2 Create a new Security Domain

Note: A Security Domain is made up of any number of HSMs and a set of Remote Access Cards.

1. Expand **Create New Security Domain**.



Create New Security Domain

Create Security Domain

This wizard guides you through the workflow of generating the cryptographic material for a new security domain, and of splitting this material onto 3 or more smart cards.

Each smart card receives a share of the security domain. The smart cards may later be used to perform certain security-critical operations such as commisioning a payShield or a smart card.

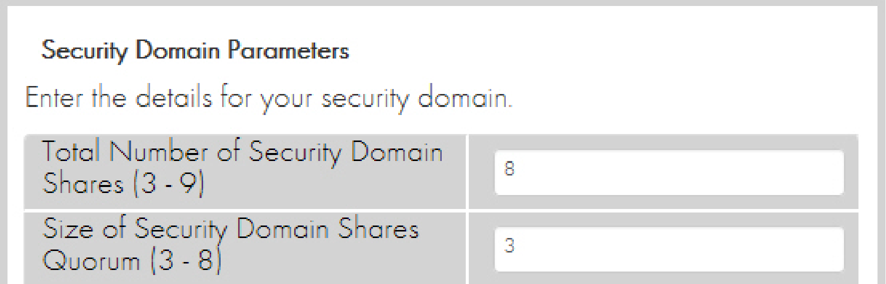
Press 'Start' to begin.

2. Click **Start**.

   The **Security Domain Parameters** window displays.

3. Enter your parameters.

   Attention: When determining the total number of security domain shares, carefully contemplate the size of the quorum.



Security Domain Parameters

Enter the details for your security domain.

Total Number of Security Domain Shares (3 - 9)	8
Size of Security Domain Shares Quorum (3 - 8)	3

For example, if the security domain is shared over 8 Smart Cards, and the quorum is set to 3, any three security officers out of the eight would need to be present to rebuild the Customer Trust Authority (CTA).

If the security domain is **shared over just 3 Smart Cards**, for example, there is less flexibility. The **same three security officers** would need to be readily available.

- Total Number of Security Domain Shares:

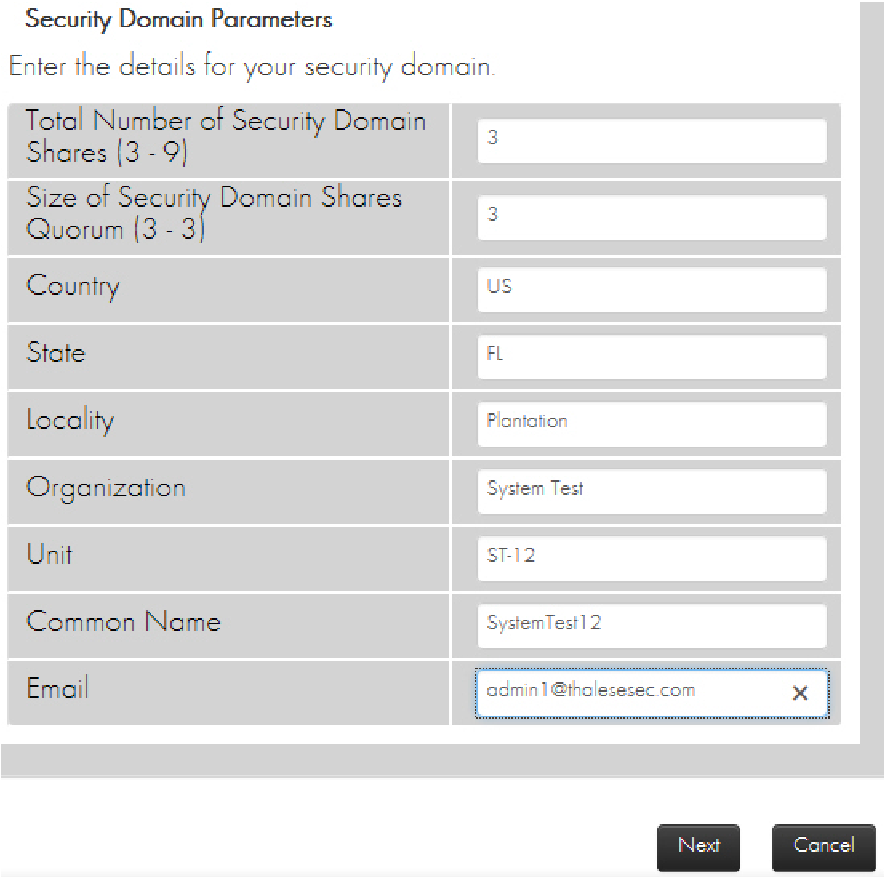
  This is the number of Smart Cards onto which the CTA shares will be distributed. Valid values are 3-9.

- Size of Security Domain Shares Quorum:

  This is the number of Smart Cards holding CTA shares that must be present in order to reassemble a CTA to perform various operations (including commissioning a payShield). The minimum value is 3.

- Country, State, Locality, Organization, Common Name, Unit, Email:

  These are parameters that are included in the X.509 certificate corresponding to the CTA. The Common Name is the only required parameter and should concisely describe the security domain.



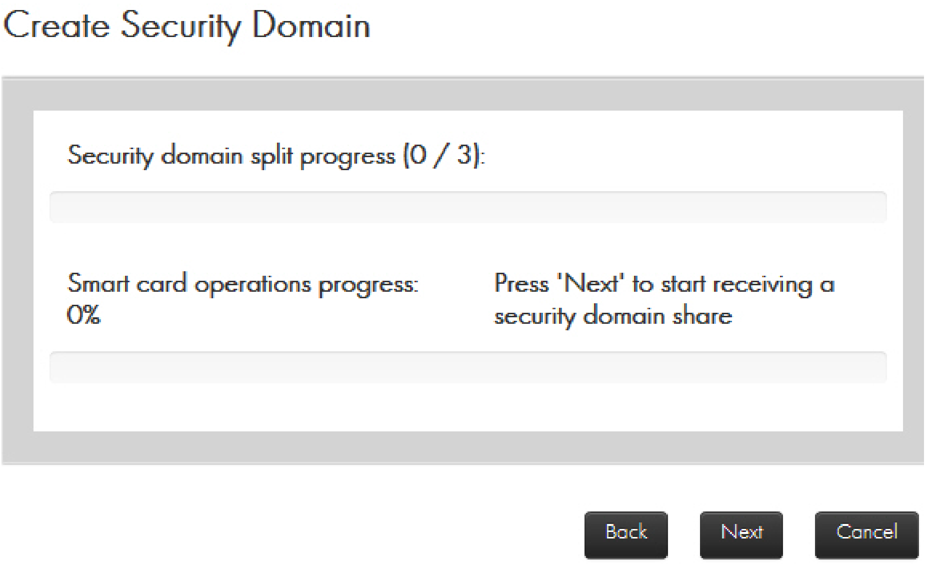
Security Domain Parameters

Enter the details for your security domain.

Total Number of Security Domain Shares (3 - 9)	3
Size of Security Domain Shares Quorum (3 - 3)	3
Country	US
State	FL
Locality	Plantation
Organization	System Test
Unit	ST-12
Common Name	SystemTest12
Email	admin1@thalesesec.com

4. Click **Next**.

5. Follow the wizard instructions to commission each Smart Card (i.e., assign key shares to each security officer's Smart Card).



Create Security Domain

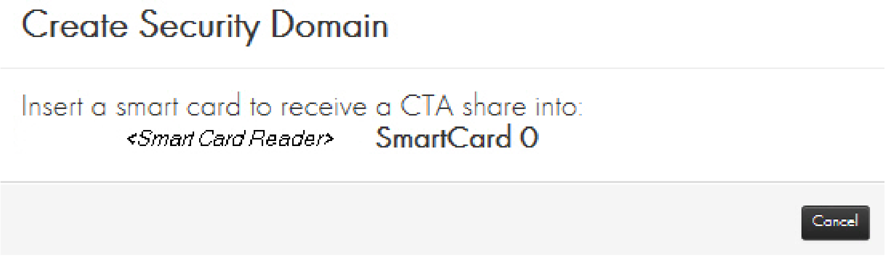
Security domain split progress (0 / 3):

Smart card operations progress: 0%

Press 'Next' to start receiving a security domain share

Note: Each Smart Card will hold a share of the CTA.

6. Click **Next.**
7. Follow the prompt and insert your Smart Card into your Smart Card reader.

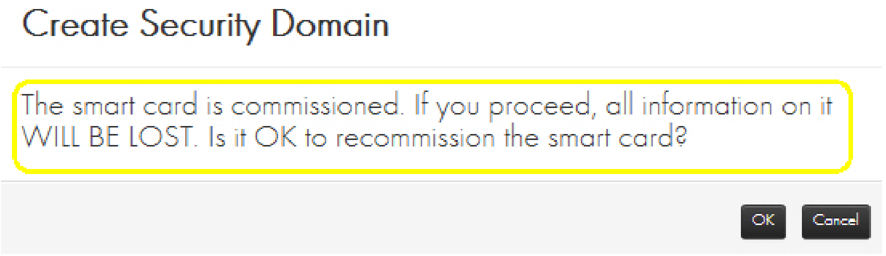


Create Security Domain

Insert a smart card to receive a CTA share into:
<Smart Card Reader> SmartCard 0

Note: If your Smart Card is brand new, continue to Step e.

a) If the system detects that you have **already commissioned the Smart Card**, you are alerted:



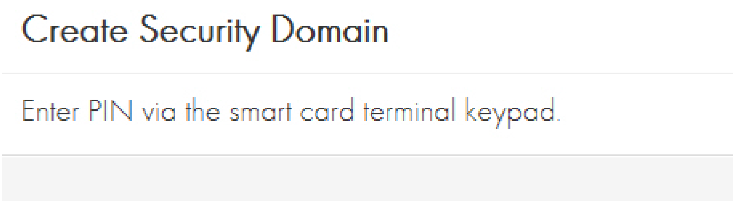
Create Security Domain

The smart card is commissioned. If you proceed, all information on it WILL BE LOST. Is it OK to recommission the smart card?

Attention: If you Click **OK**, information on the card will be lost **but the original PIN remains**. Clicking OK does not erase the PIN.

b) Click **OK**.

The system prompts for the **original PIN**.



Create Security Domain

Enter PIN via the smart card terminal keypad.

c) Enter the original PIN.

d) Press **OK** on the card reader.

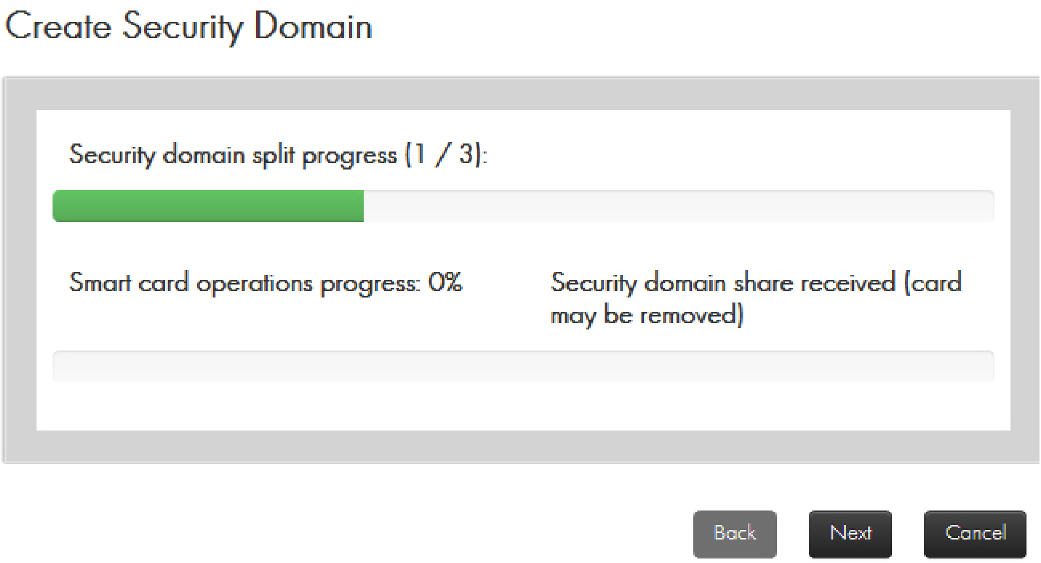
The system prompts for a new PIN.

e) Enter a new PIN (for example, a 6-digit PIN).

f) Press **OK** on the card reader.

g) Enter the new PIN again to confirm.

h) Press **OK** on the card reader.



Create Security Domain

Security domain split progress (1 / 3):

Smart card operations progress: 0%

Security domain share received (card may be removed)

The system will display **Security domain share received (card may be removed)**.

i) Click **Next**.

j) Remove the card and repeat the process for each card (i.e., for each security officer).

k) After the final security officer has confirmed a PIN, click **Finish**.

At this point a set of security domain credentials, i.e., a Customer Trust Authority (CTA), has been created and split into some number of Smart Cards with each trusted officer holding one share.

Note: This CTA can be loaded into any uncommissioned HSM.

It is important to note that these cards are critical in the remote management process. They are required each time an HSM or a Smart Card is added to the security domain.

Note: It is a best practice to back up these cards and store the backups in a secure off-site location.

7.5.3 Load the Security Domain

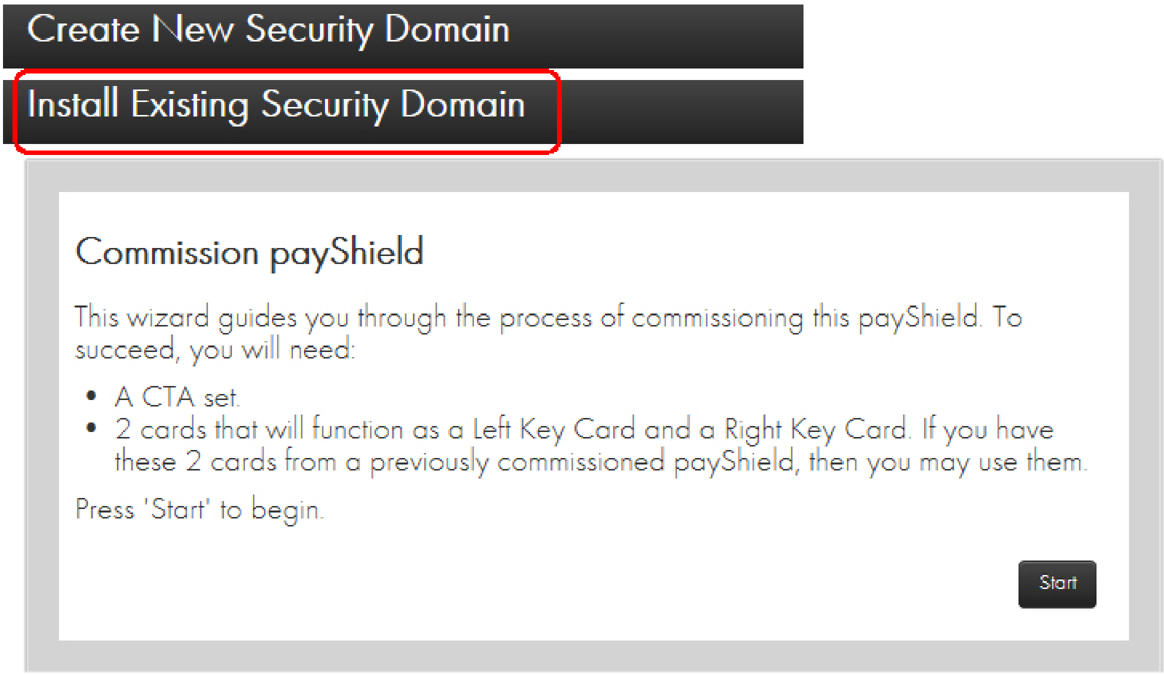
When you load a Security Domain, you are associating your payShield to that particular domain. You can associate the payShield with the newly created Security Domain (just created by following Section 7.5.2, “Create a new Security Domain”, on page 68) or you can add this payShield to an existing Security Domain of your choice.

Prerequisites:

- The Smart Cards that make up the Security Domain
- 2 Smart Cards (that will function as a Left Key Card and a Right Key Card)

Note: If you have these cards from a previously commissioned payShield, you may use them.

1. Expand the **Install Existing Security Domain** accordion.



Commission payShield

This wizard guides you through the process of commissioning this payShield. To succeed, you will need:

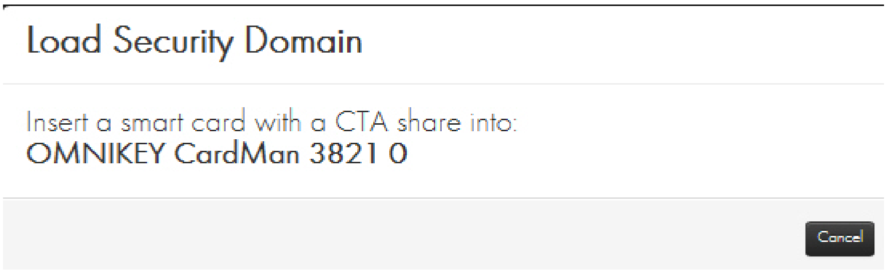
- A CTA set.
- 2 cards that will function as a Left Key Card and a Right Key Card. If you have these 2 cards from a previously commissioned payShield, then you may use them.

Press 'Start' to begin.

2. Click **Start**.

3. Each security officer performs the following:

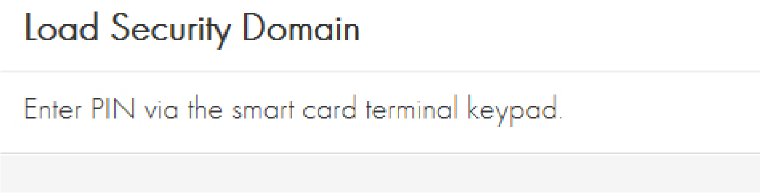
- Place their Smart Card in the reader.



Load Security Domain

Insert a smart card with a CTA share into:
OMNIKEY CardMan 3821 0

System prompts:

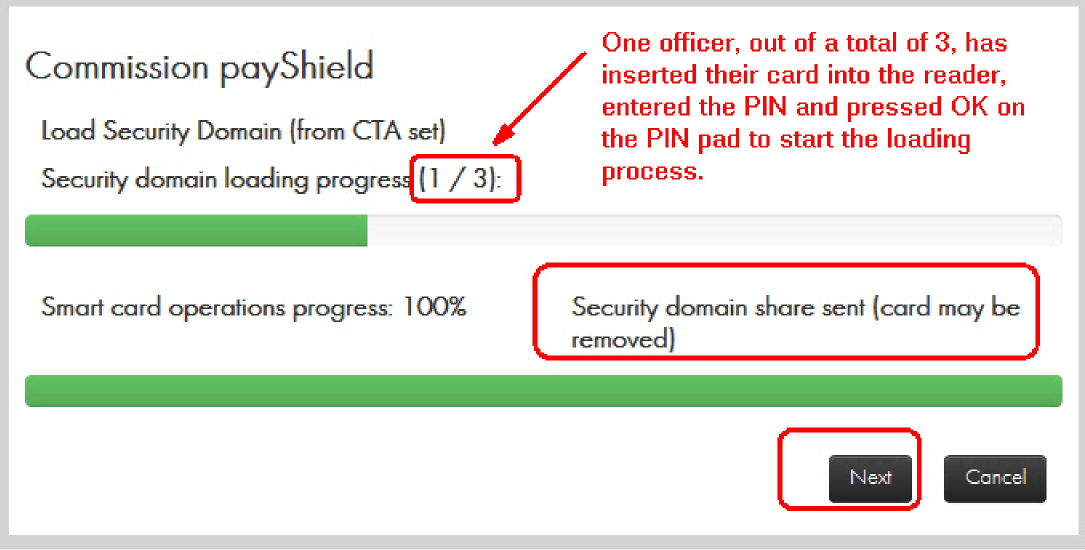


Load Security Domain

Enter PIN via the smart card terminal keypad.

- Enter PIN.
- Click **OK** on the PIN pad.

The system displays:



Commission payShield

Load Security Domain (from CTA set)

Security domain loading progress (1 / 3):

Smart card operations progress: 100%

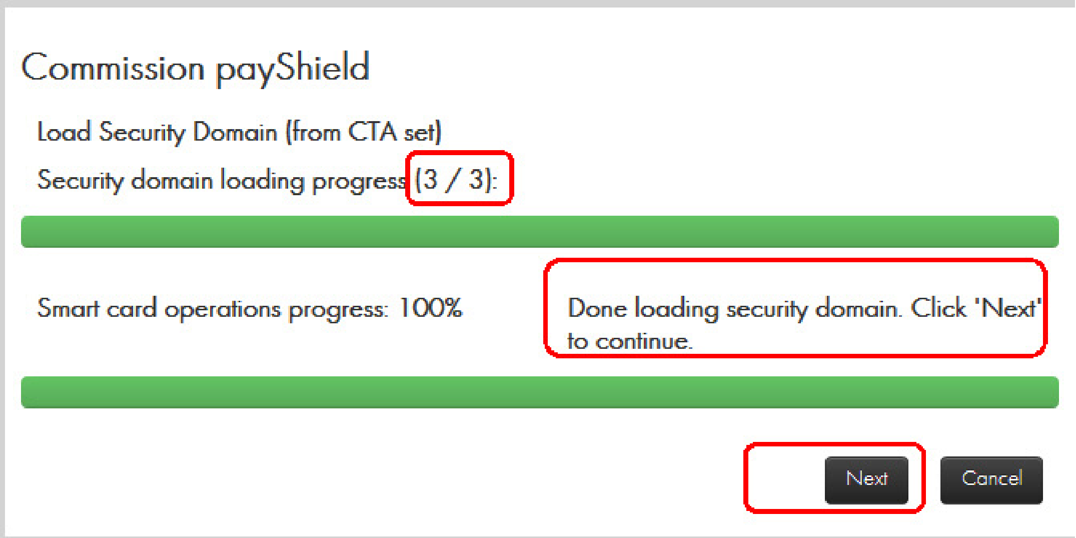
Security domain share sent (card may be removed)

One officer, out of a total of 3, has inserted their card into the reader, entered the PIN and pressed OK on the PIN pad to start the loading process.

4. Remove card and click **Next**.

5. Repeat the steps above for security officer.

   Note: As each officer enters their Smart Card, a key share is loaded into the domain.



Commission payShield

Load Security Domain (from CTA set)

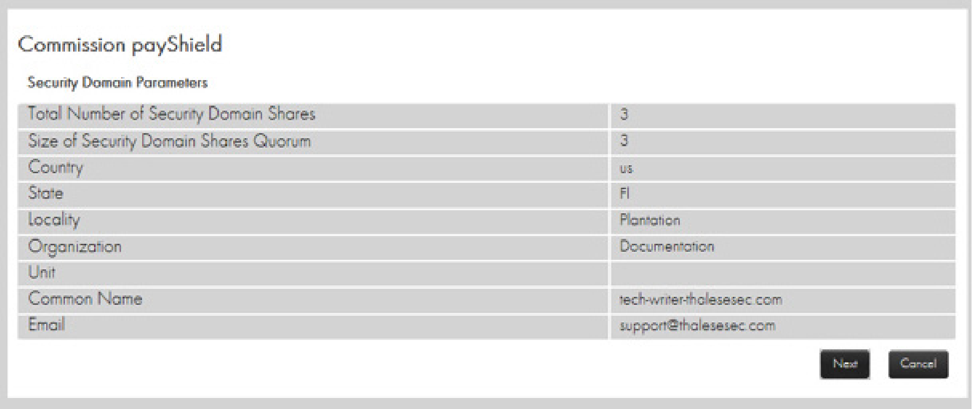
Security domain loading progress (3 / 3):

Smart card operations progress: 100%

Done loading security domain. Click 'Next' to continue.

6. When done, click **Next**.

   The system displays:



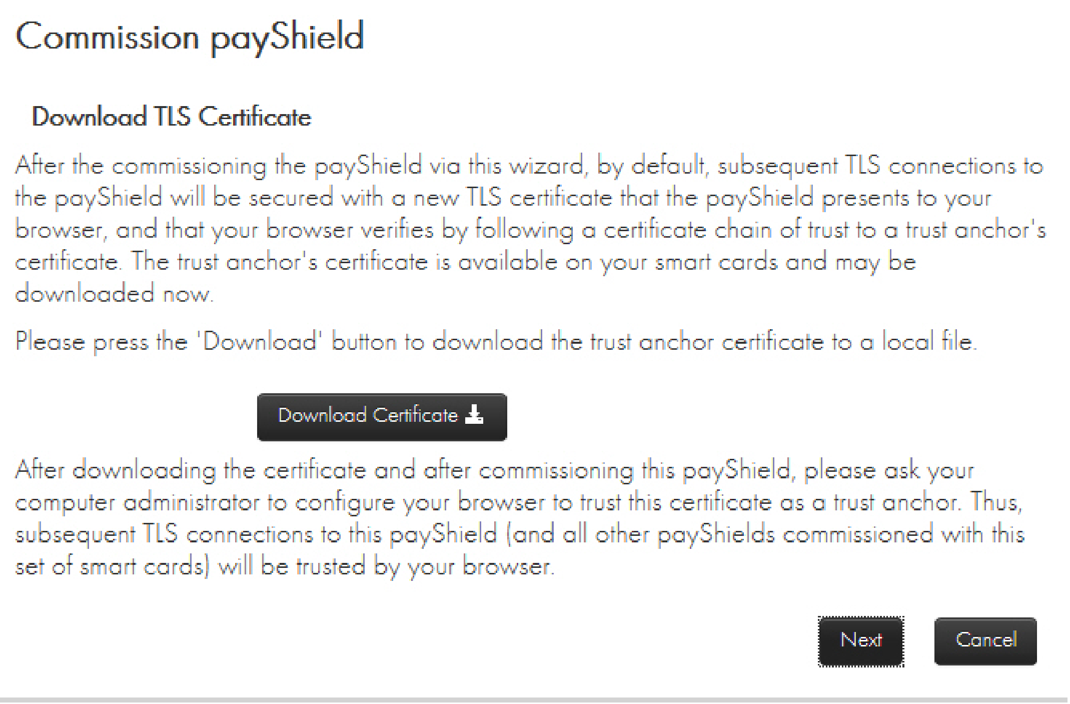
Commission payShield

Security Domain Parameters

Total Number of Security Domain Shares	3
Size of Security Domain Shares Quorum	3
Country	us
State	Fl
Locality	Plantation
Organization	Documentation
Unit	
Common Name	tech-writer-thalesesec.com
Email	support@thalesesec.com

7. Click **Next**.

   The system displays:



Commission payShield

Download TLS Certificate

After the commissioning the payShield via this wizard, by default, subsequent TLS connections to the payShield will be secured with a new TLS certificate that the payShield presents to your browser, and that your browser verifies by following a certificate chain of trust to a trust anchor's certificate. The trust anchor's certificate is available on your smart cards and may be downloaded now.

Please press the 'Download' button to download the trust anchor certificate to a local file.

After downloading the certificate and after commissioning this payShield, please ask your computer administrator to configure your browser to trust this certificate as a trust anchor. Thus, subsequent TLS connections to this payShield (and all other payShields commissioned with this set of smart cards) will be trusted by your browser.

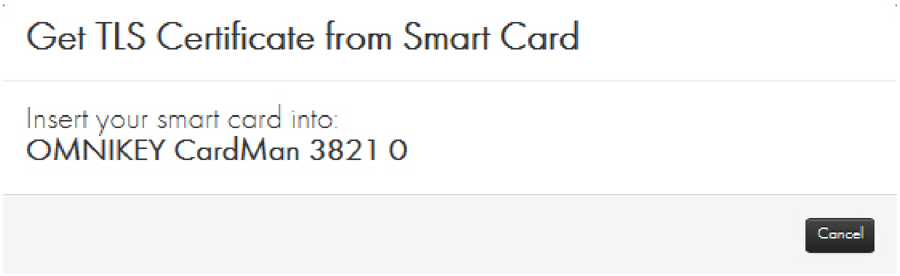
This certificate can then be imported into the browser in order to trust subsequent TLS connections to the commissioned payShield. Depending on your organization's IT policy, a PC administrator may be required to perform this configuration.

Note: If you do not need to Download the Certificate:

- Continue to Section 7.5.5, “Create Left and Right Remote Access Control key cards”, on page 79**.**

8. Click **Download Certificate to download the certificate.**

   The system displays:



Get TLS Certificate from Smart Card

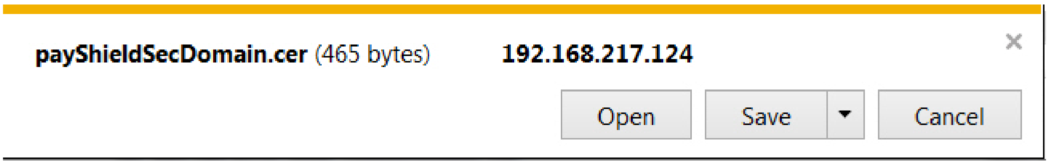
Insert your smart card into:
OMNIKEY CardMan 3821 0

a) Insert your Smart Card.

b) Enter your PIN.

c) Press **OK**.

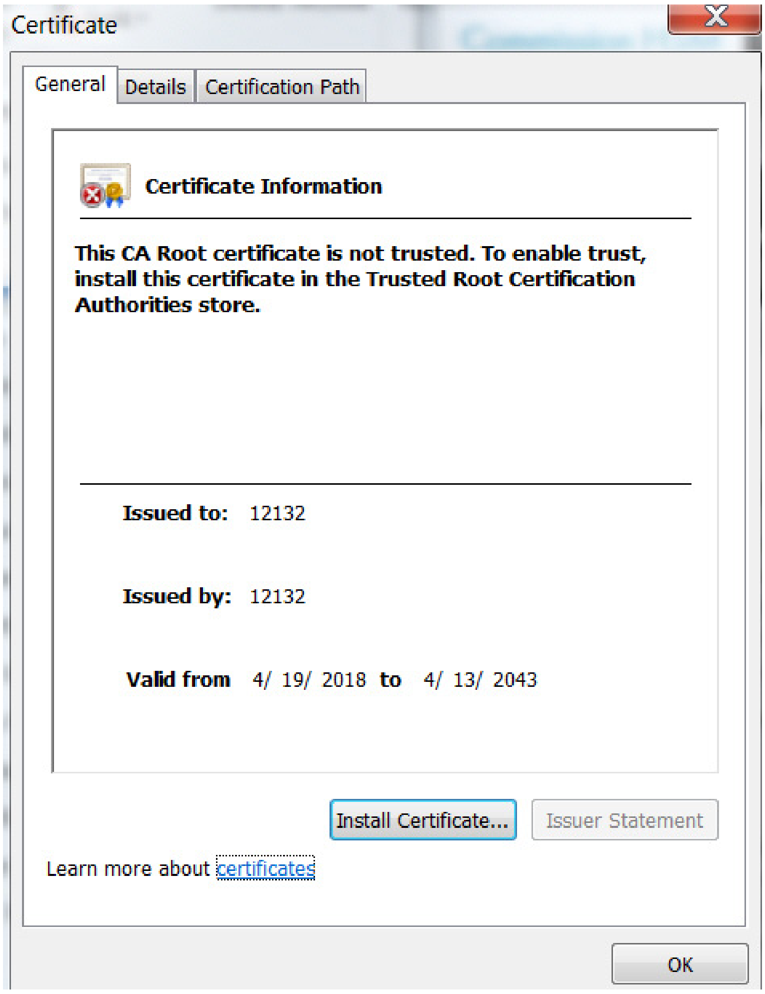
The system displays (example):



payShieldSecDomain.cer (465 bytes) **192.168.217.124**

d) Save your file to an appropriate location.

e) Open the certificate for details.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: 12132

Issued by: 12132

Valid from 4/ 19/ 2018 **to** 4/ 13/ 2043

Note: For additional data, open the **Details** tab and the **Certification Path** tab.

f) Click **Install Certificate**.

The Certificate Import Wizard opens.

g) Follow the prompts.

9. Click **OK**.

7.5.4 Set HSM Recovery Key (HRK) passphrases

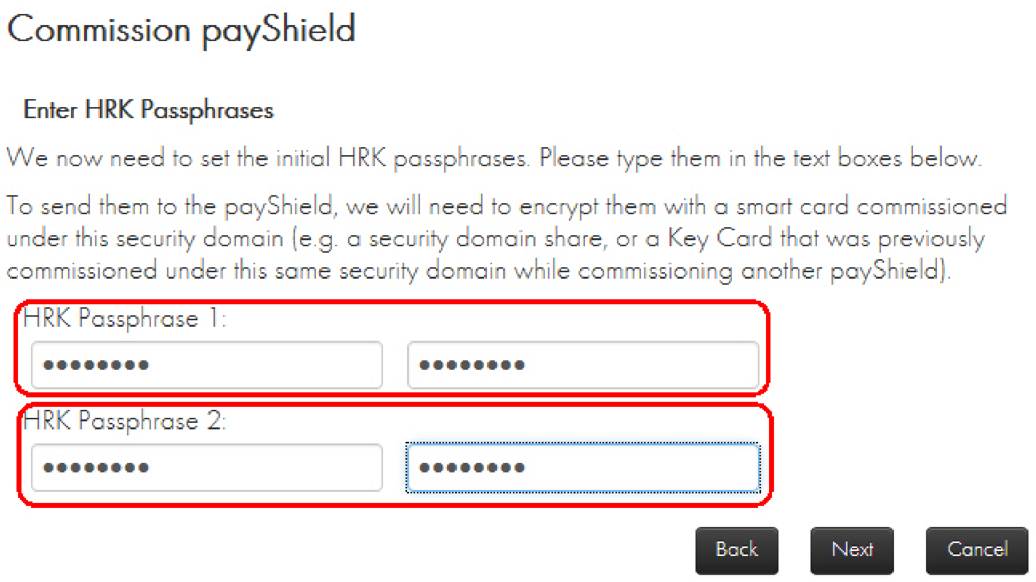
Note: You cannot use any HRK that was previously attempted to be set within the last 10 attempts. This encompasses all attempts.

- If you do not have HRK passphrases:
  - The system prompts you to create them. Continue to Step 1 below.
- If you already have HRK passphrases:
  - The system prompts you to create your Left Key Card. Continue to Section 7.5.5, “Create Left and Right Remote Access Control key cards”, on page 79.

1. Enter the HRK passphrases two times.

   The HRK passphrase must contain at least:

   - 2 uppercase characters
   - 2 lowercase characters
   - 2 digits
   - 2 symbols



Commission payShield

Enter HRK Passphrases

We now need to set the initial HRK passphrases. Please type them in the text boxes below.

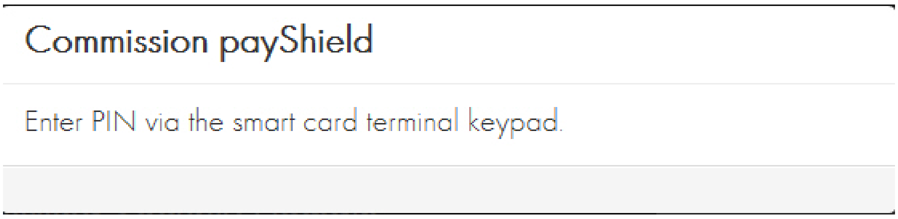
To send them to the payShield, we will need to encrypt them with a smart card commissioned under this security domain (e.g. a security domain share, or a Key Card that was previously commissioned under this same security domain while commissioning another payShield).

HRK Passphrase 1: •••••••• ••••••••

HRK Passphrase 2: •••••••• ••••••••

2. Click **Next**.

   The system displays:



Commission payShield

Enter PIN via the smart card terminal keypad.

3. Enter a PIN.

   Note: Although the system will accept a minimum PIN length of 6 digits, PINs MUST consist of 8 or more digits to align with the practices identified in the *payShield 10K Security Manual*.

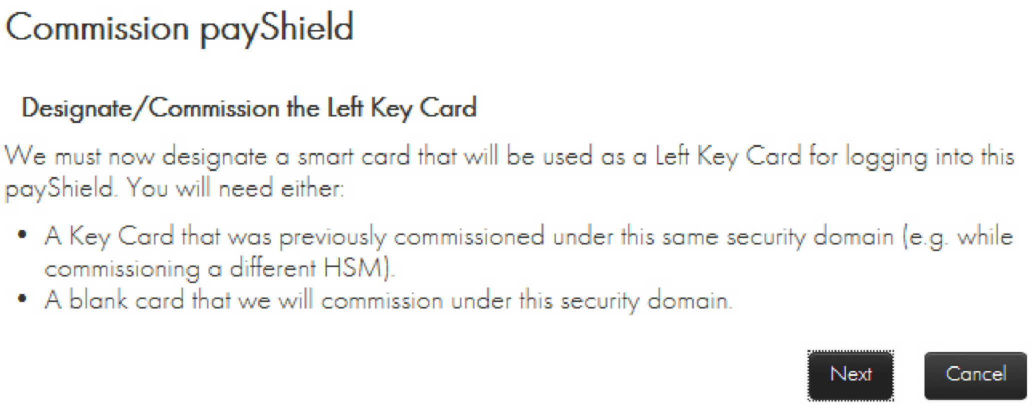
4. Remove the Smart Card.

   The system prompts you to Designate/Commission the Left Key Card.

7.5.5 Create Left and Right Remote Access Control key cards

If you already have Left and Right key cards, i.e., cards that have been created on a payShield 9000, you may use them.

1. Insert a Smart Card into the Smart Card reader.



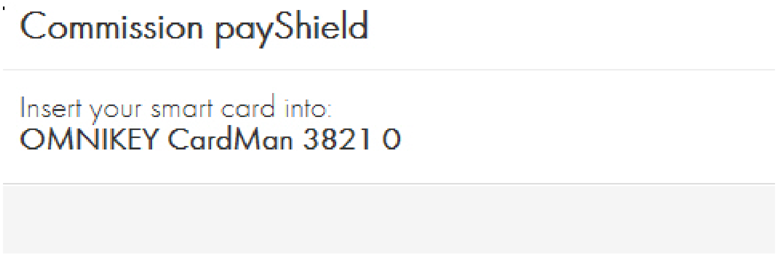
Commission payShield

Designate/Commission the Left Key Card

We must now designate a smart card that will be used as a Left Key Card for logging into this payShield. You will need either:

- A Key Card that was previously commissioned under this same security domain (e.g. while commissioning a different HSM).
- A blank card that we will commission under this security domain.

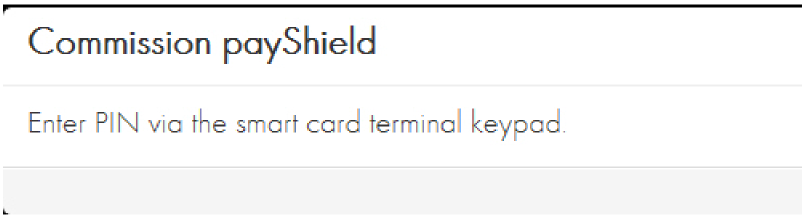
2. Click **Next**.



Commission payShield

Insert your smart card into:
OMNIKEY CardMan 3821 0

The system displays:



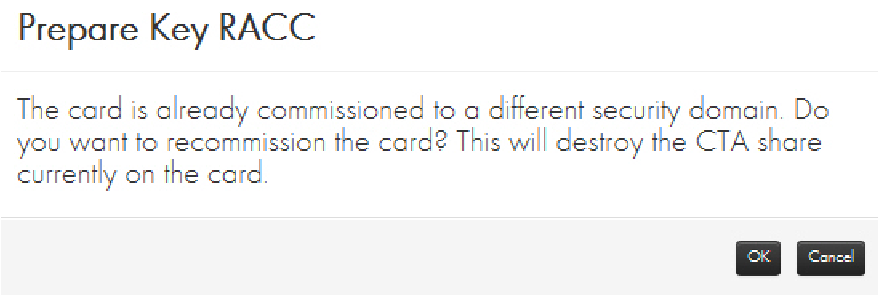
Commission payShield

Enter PIN via the smart card terminal keypad.

Note: PINs are entered via the Smart Card terminal keypad. Remember to press **OK** after entering a PIN.

3. Enter the PIN.
4. Press **OK**.

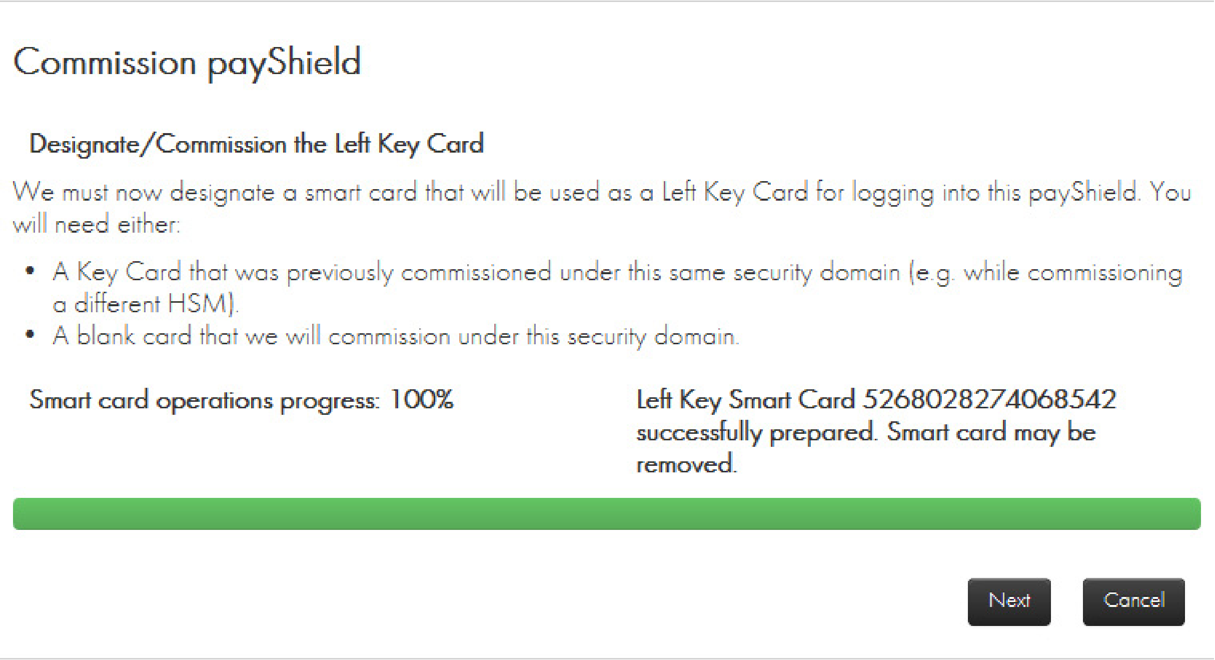
   The system displays:



Prepare Key RACC

The card is already commissioned to a different security domain. Do you want to recommission the card? This will destroy the CTA share currently on the card.

5. Click **OK**.



Commission payShield

Designate/Commission the Left Key Card

We must now designate a smart card that will be used as a Left Key Card for logging into this payShield. You will need either:

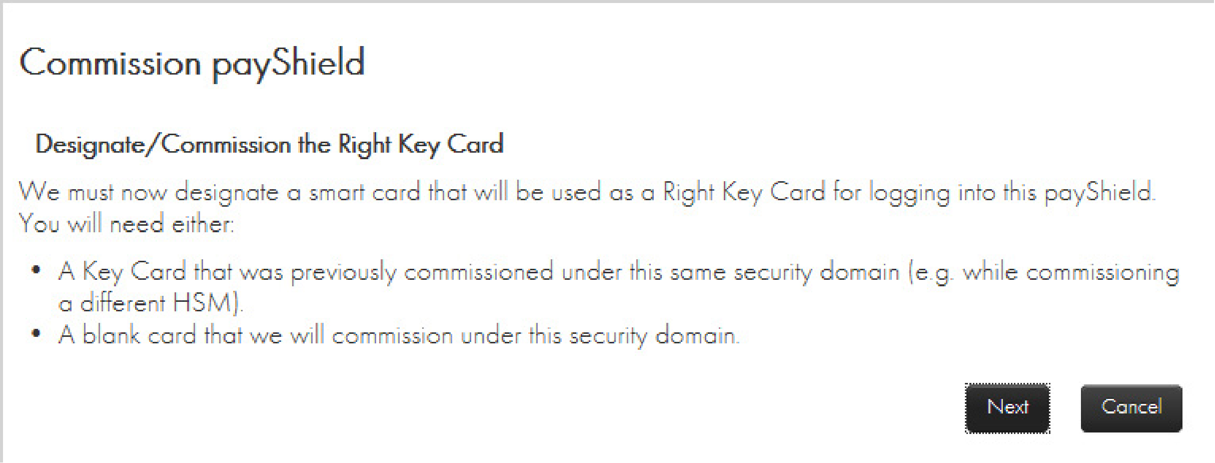
- A Key Card that was previously commissioned under this same security domain (e.g. while commissioning a different HSM).
- A blank card that we will commission under this security domain.

Smart card operations progress: 100%

Left Key Smart Card 5268028274068542 successfully prepared. Smart card may be removed.

6. Enter a new PIN.
7. Press **OK**.
8. Click **Next**.

   The system is ready to create the right key card.



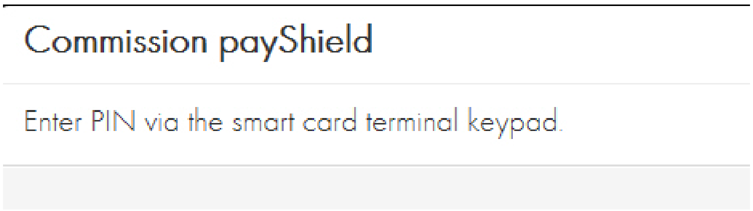
Commission payShield

Designate/Commission the Right Key Card

We must now designate a smart card that will be used as a Right Key Card for logging into this payShield. You will need either:

- A Key Card that was previously commissioned under this same security domain (e.g. while commissioning a different HSM).
- A blank card that we will commission under this security domain.

9. Click **Next**.
10. Insert the Smart Card into the reader.



Commission payShield

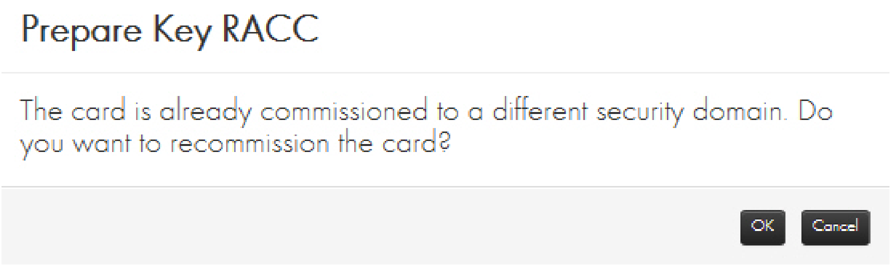
Enter PIN via the smart card terminal keypad.

11. Enter the PIN.

12. Press **OK**.

13. Insert the card into the Smart Card reader.

    The system prompts

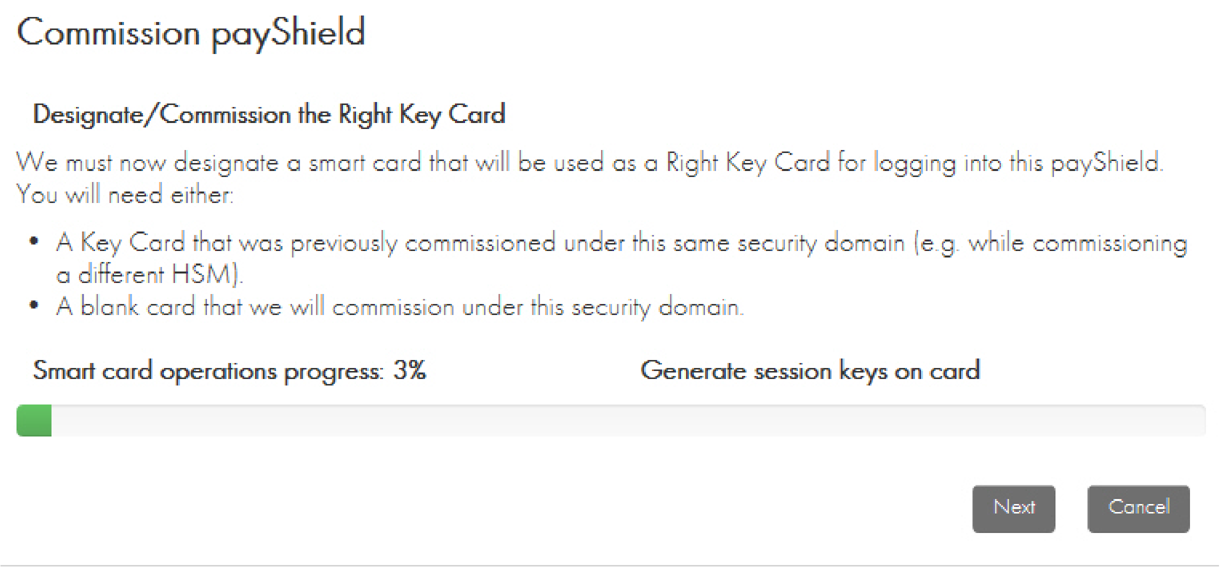


Prepare Key RACC

The card is already commissioned to a different security domain. Do you want to recommission the card?

14. Click **OK**.

    The system starts to process.



Commission payShield

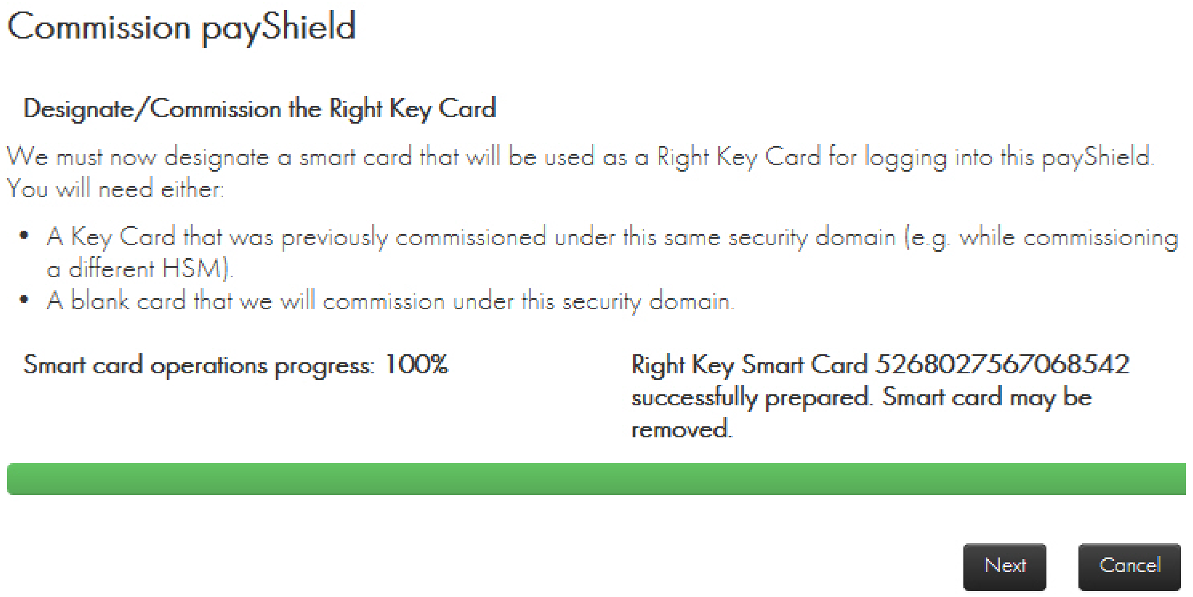
Designate/Commission the Right Key Card

We must now designate a smart card that will be used as a Right Key Card for logging into this payShield. You will need either:

- A Key Card that was previously commissioned under this same security domain (e.g. while commissioning a different HSM).
- A blank card that we will commission under this security domain.

Smart card operations progress: 3% Generate session keys on card

The system prompts completion.



Commission payShield

Designate/Commission the Right Key Card

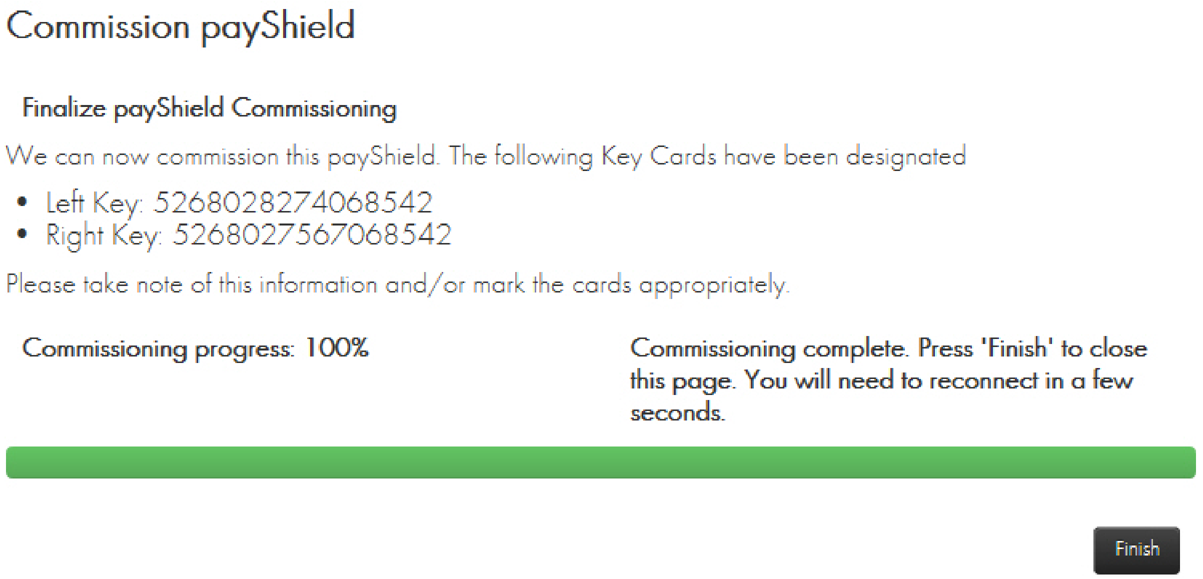
We must now designate a smart card that will be used as a Right Key Card for logging into this payShield. You will need either:

- A Key Card that was previously commissioned under this same security domain (e.g. while commissioning a different HSM).
- A blank card that we will commission under this security domain.

Smart card operations progress: 100%

Right Key Smart Card 5268027567068542 successfully prepared. Smart card may be removed.

15. Remove the Smart Card.
16. Click **Next**.



Commission payShield

Finalize payShield Commissioning

We can now commission this payShield. The following Key Cards have been designated

- Left Key: 5268028274068542
- Right Key: 5268027567068542

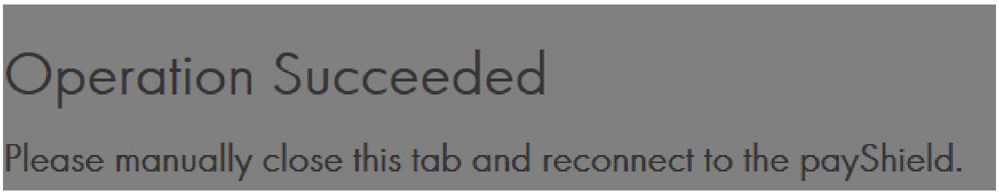
Please take note of this information and/or mark the cards appropriately.

Commissioning progress: 100%

Commissioning complete. Press 'Finish' to close this page. You will need to reconnect in a few seconds.

17. Click **Finish**.

    The system displays:

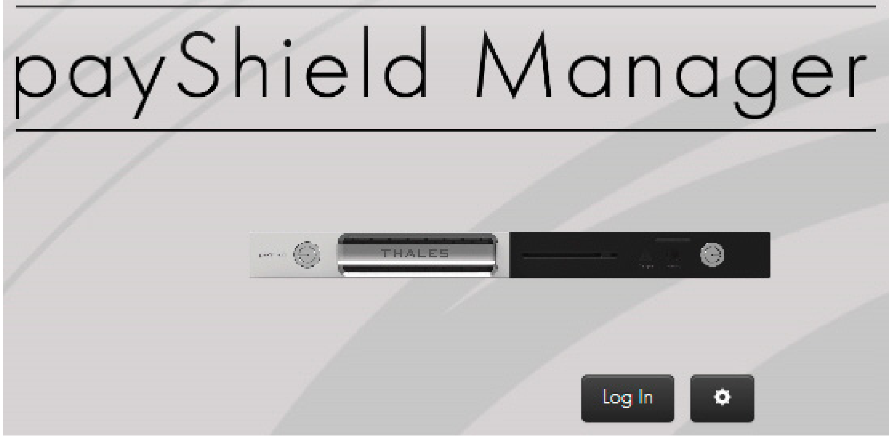


Operation Succeeded

Please manually close this tab and reconnect to the payShield.

18. Restart your Internet browser, enter the IP address associated with your HSM.

    The system displays:



7.5.6 Adding Additional Warranted HSMs to the Security Domain

New payShield HSMs that have Thales warranting on them can be added by using the instructions for Remote Commissioning of a warranted payShield.

1. Log into payShield Manager using the address of the new HSM to be commissioned.
2. Select the **Commission** when it comes up on the browser.
3. Remotely load the security domain (CTA) when prompted by the wizard.
4. Set the HRK passphrase for the HSM, when prompted by the wizard.

   Passphrases require the following:

   - At least 2 upper case characters
   - At least 2 lower case characters
   - At least 2 numbers
   - At least 2 special characters

5. Create (or sign existing) left and right key RACCs. If a set of cards is used for each individual HSM, then they will be commissioned first.
6. Restart the web-browser.

Follow this link for additional information: Chapter 8, “Using payShield Manager”.

7.6 Additional Information

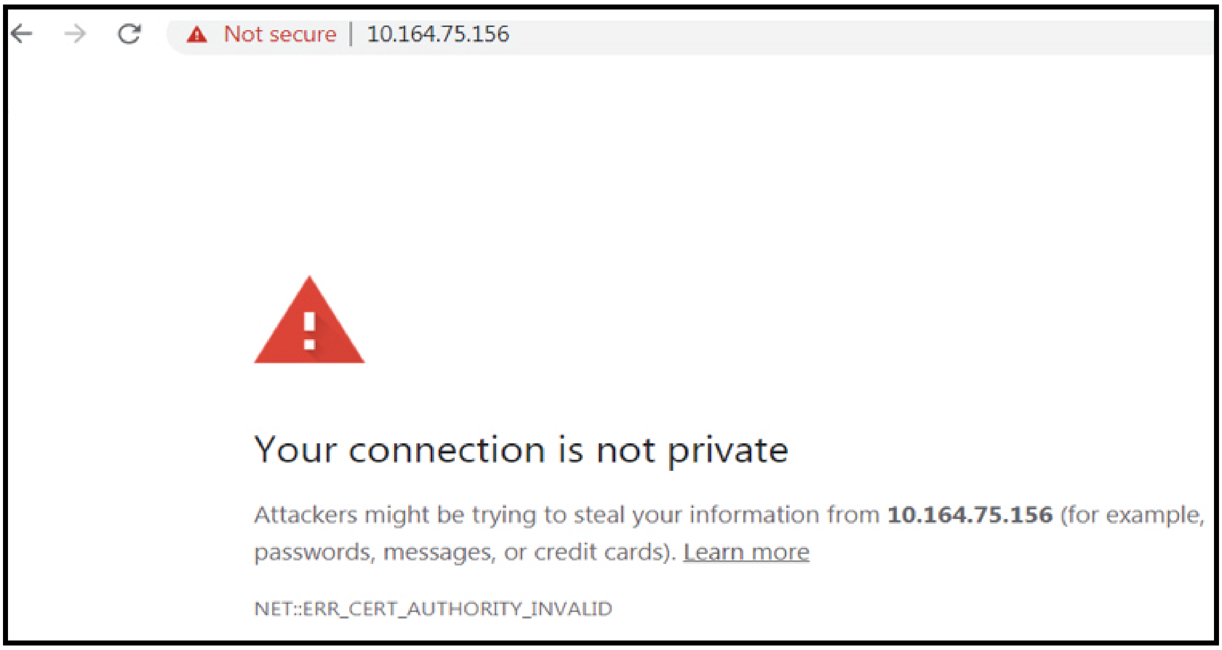
This section includes additional information on commissioning payShield Manager.

7.6.1 Using payShield Manager with MacOS Catalina

The following steps are required to be undertaken when using payShield Manager with MacOS Catalina Version 10.15.7 and above.

The procedure describes the steps required using Google Chrome Version 86.0.4240.111. The procedure may vary when using other versions of Chrome or other browsers.

When accessing the landing page, if the following message is shown by the browser, carry out the following steps:



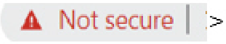
Your connection is not private

Attackers might be trying to steal your information from **10.164.75.156** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

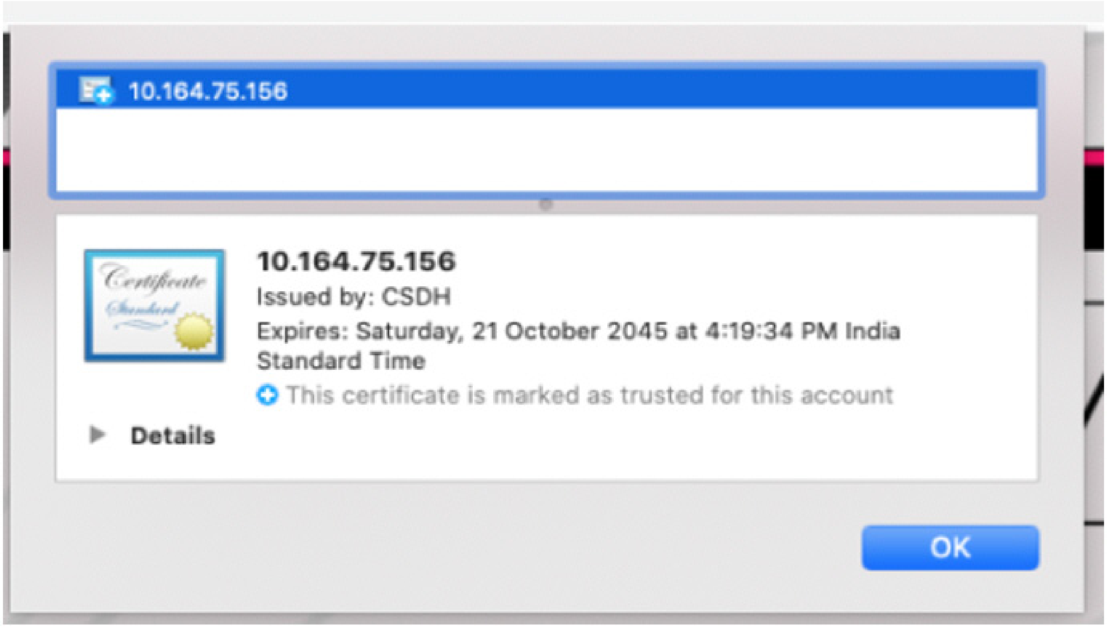
1. Save the Certificate to the Desktop.

- Click on:



> Certificate

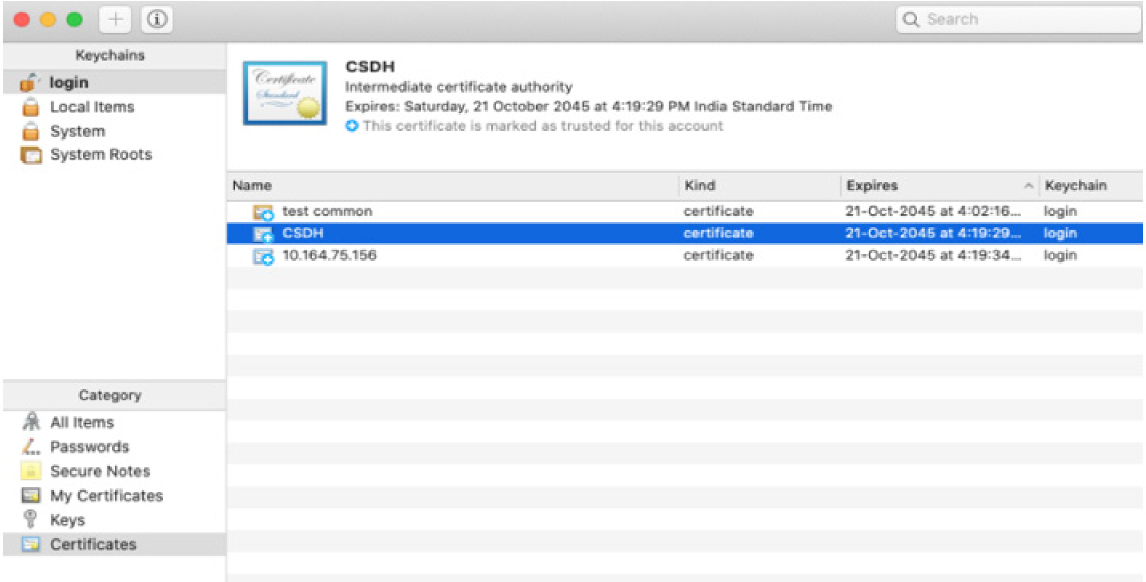
- The following dialogue is displayed which allows the certificate to be saved. Click the certificate icon and literally drag the icon to the desktop.



10.164.75.156

10.164.75.156
Issued by: CSDH
Expires: Saturday, 21 October 2045 at 4:19:34 PM India Standard Time
This certificate is marked as trusted for this account

2. Add the Certificate to Keychain Access.

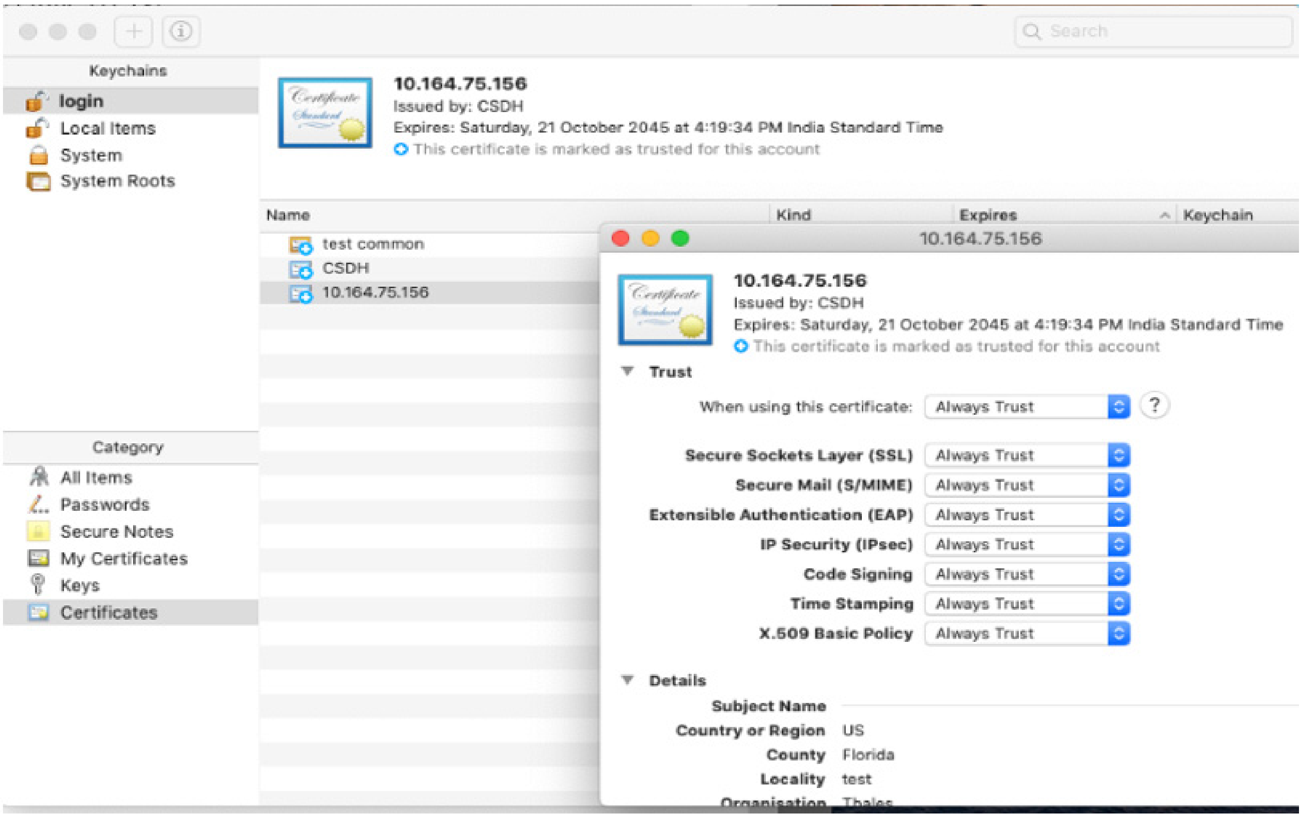


CSDH
Intermediate certificate authority
Expires: Saturday, 21 October 2045 at 4:19:29 PM India Standard Time
This certificate is marked as trusted for this account

Name	Kind	Expires	Keychain
test common	certificate	21-Oct-2045 at 4:02:16...	login
CSDH	certificate	21-Oct-2045 at 4:19:29...	login
10.164.75.156	certificate	21-Oct-2045 at 4:19:34...	login

- Open the Keychain Access Application and Navigate to the Certificates panel.
- Drag the certificate into the Certificates panel.
- The certificate is now installed and recognizable to Keychain Access.

3. Trust the Certificate.



10.164.75.156
Issued by: CSDH
Expires: Saturday, 21 October 2045 at 4:19:34 PM India Standard Time
This certificate is marked as trusted for this account

Trust

When using this certificate:	Always Trust
Secure Sockets Layer (SSL)	Always Trust
Secure Mail (S/MIME)	Always Trust
Extensible Authentication (EAP)	Always Trust
IP Security (IPsec)	Always Trust
Code Signing	Always Trust
Time Stamping	Always Trust
X.509 Basic Policy	Always Trust

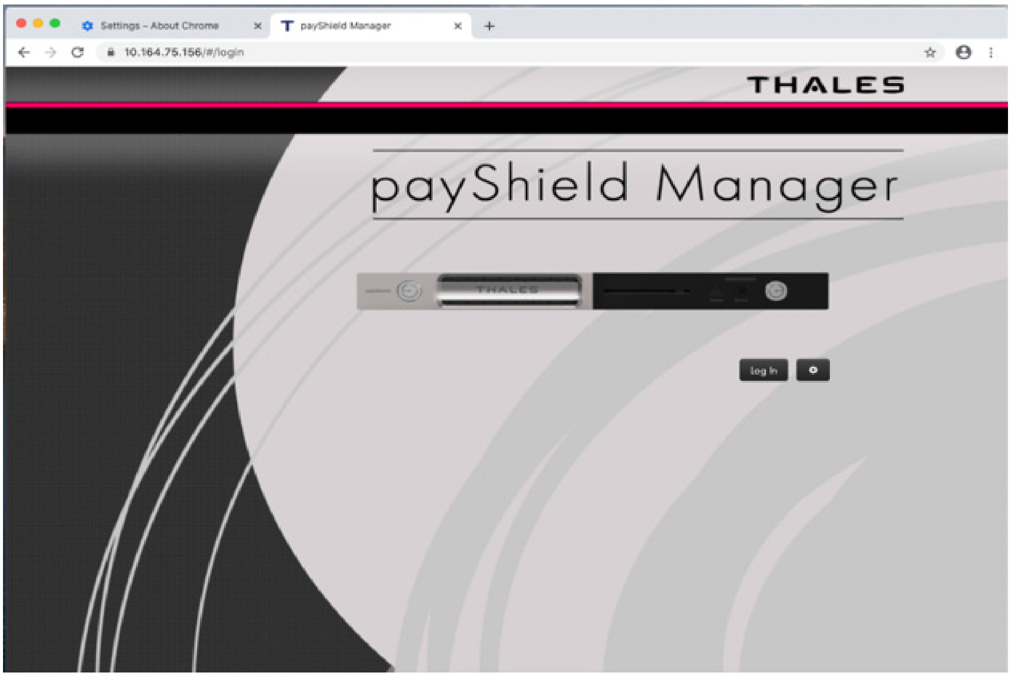
Details

Subject Name

Country or Region	US
County	Florida
Locality	test
Organisation	Thales

- Double-click on the certificate in order to manage the system preferences for handling the certificate.
- Expand the Trust panel and set the preference to “Always Trust” the certificate.

4. Restart the Browser/System.
   - Restart the browser of the system.
5. Open payShield Manager.
   - Open payShield Manager.


Settings – About Chrome
payShield Manager
10.164.75.156/#/login
THALES
payShield Manager
Log In

8 Using payShield Manager

8.1 Introduction to payShield Manager

This Chapter describes in detail the functionality provided by payShield Manager. It assumes the commissioning process has been completed as described in Chapter 7, “Commission using payShield Manager”. A description of how the Local Master Key (LMK) is generated and installed and the configuration is updated is included.

payShield Manager provides the following features:

- HSM Configuration – communication port settings, security settings, etc.
- HSM Installation – generation and installation of LMKs from Smart Cards
- HSM Key Management – generate keys, import keys, export keys, etc.
- HSM Maintenance – viewing, printing, and erasing of audit logs, error logs, version info, etc.
- HSM State Changes – transitions between Online, Offline, Secure and Authorized.
- HSM Firmware and license loading

Please note:

- Only one payShield Manager session is allowed at a time.
- When accessing the payShield 10K via the payShield Manager, the local console is disabled. Once the payShield Manager session ends, local console access is restored.
- If the physical keys on the front panel are changed from the online position, the payShield Manager session terminates abruptly and the local console is restored.

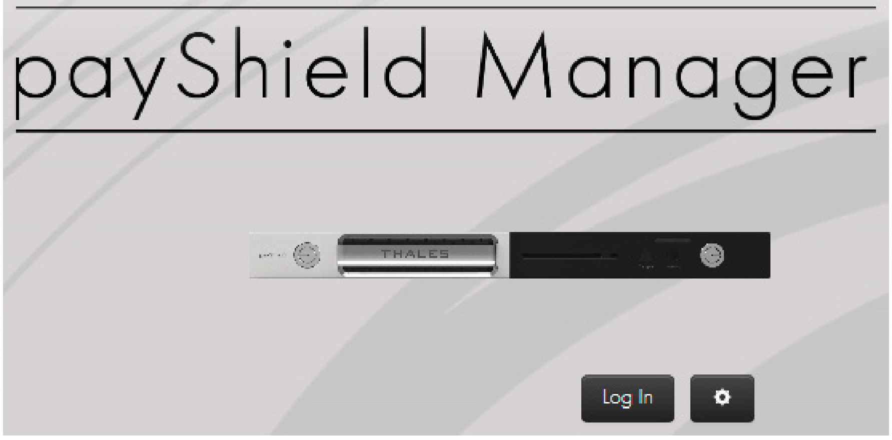
8.2 Logging into payShield Manager

1. Enter the IP address of your payShield 10K into your Internet browser and click enter.

   Note: Only one tab in one browser window may be connected to the payShield 10k. To monitor multiple 10ks within the same browser, each should be loaded into a separate browser tab.

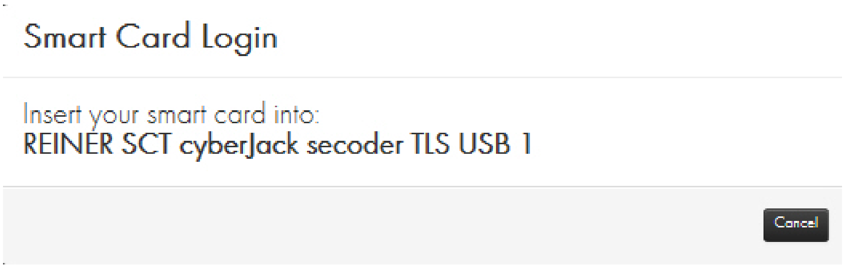
   The payShield Manager welcome page displays.

   Note: When using MacOS Catalina there are a few additional steps to be carried out before the landing page can be accessed. These are described in Section 7.6.1, “Using payShield Manager with MacOS Catalina”, on page 85.



2. Click **Log In**.

   The system prompts you to insert your Smart Card into the Smart Card reader.



Smart Card Login

Insert your smart card into:
REINER SCT cyberJack secoder TLS USB 1

Note: To reach the Secure state, both Right and Left Administrators must perform steps 3 through 5 below.

3. Insert your Administrator Smart Card into the Smart Card reader.

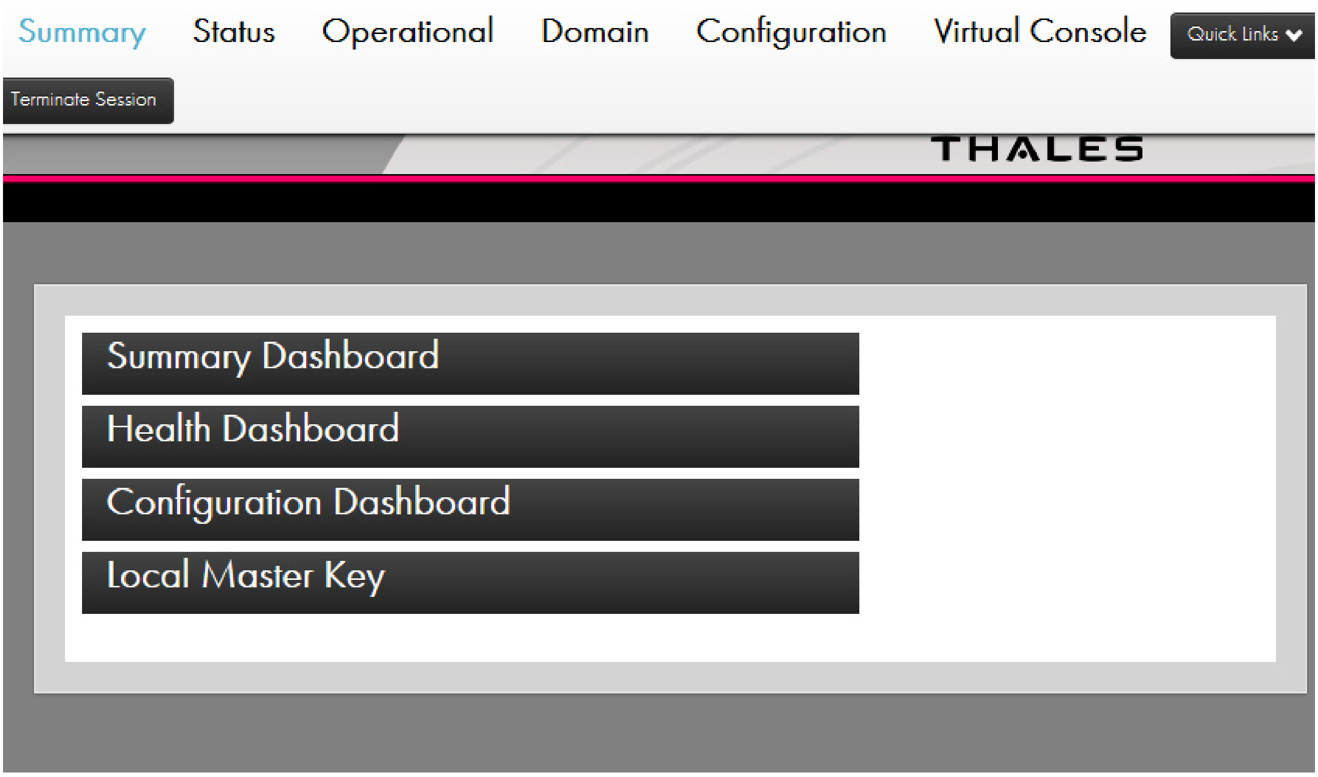
   Note: If the system does not appear to be reading your Smart Card, check your Smart Card reader configuration.

   Section 6.1.3.3, “Configure the smart card reader”, on page 56.

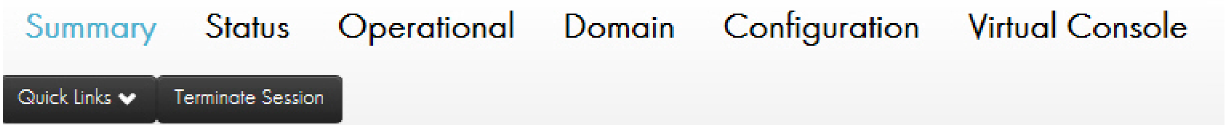
4. Enter your PIN.

5. Select **OK**.

   The main page opens.



8.3 Top Tab descriptions



8.3.1 Summary Tab

Selecting this tab causes the UI to transition to the Summary Perspective (shown). In this perspective, you can view summary information about your HSM.

8.3.2 Status Tab

Selecting this tab causes the UI to transition to the Status Perspective. In this perspective, you can:

- View detailed device information
- Cause a reboot of the HSM

- View/download/reset utilization statistics and configure their collection
- View/download/reset health statistics, configure their collection and reset the fraud detection
- Run diagnostics and configure the automated run-time
- View/download the error log and clear it
- View/download the audit log and clear it
- View detailed software versions
- Upgrade the software
- View detailed license information
- Install licenses
- View details on the FIPS validated algorithms
- Import a TLS certificate for Host connections

8.3.3 Operational Tab

Selecting this tab causes the UI to transition to the Operational Perspective. In this perspective, you can:

- For each individual LMK
  - Replace an LMK
  - Delete an LMK
  - Set an LMK as the default LMK
  - Set an LMK as the default Management LMK
  - Set Authorized Activities
- For each individual LMK in Key Change Storage
  - Replace an LMK
  - Delete an LMK
- Verify LMK Smart Card shares
- Create Authorizing Officer Smart Cards
- Duplicate LMK Smart Card shares
- Generate LMKs
- Install LMKs

  Note: Installing an LMK loads an old LMK component set into the Key Change Storage. This then allows you to translate key material from encryption under one LMK to encryption under another LMK. The current LMK must be installed before an “old” LMK can be installed. Note that attempts to load both Live and Test into the same slot (as new and old LMKs) will be rejected.

- Install LMKs into the Key Change Storage (old LMKs)

  Note: “Old” LMKs are stored in a table within the secure memory of the HSM, with each “old” LMK occupying a different “slot” within the table.

8.3.4 Domain Tab

Selecting this tab causes the UI to transition to the Domain Perspective. In this perspective, you can:

- View and manage the payShield Security Group’s Smart Card whitelist
- View and manage the Security Domain
  - View the certificate chain and its fields
  - Commission a Smart Card for this security domain
  - Decommission a Smart Card
  - Copy a Domain Smart Card
  - Create a new Security Domain (CTA)
- Change the HRK passphrases
- Migrate Legacy Cards (if the payShield is a migrated unit)

8.3.5 Configuration Tab

Selecting this tab causes the UI to transition to the Configuration Perspective. In this perspective, you can:

- View and manage the HSM’s Host Interface Settings including:
  - Setting the Host message header length
  - Setting and configuring the interface type (Ethernet/FICON)
  - Setting the IP, ACL, TCP/UDP, and TLS parameters for Ethernet
  - Configuring the connection settings for FICON
- View and manage the console interface settings
- View and manage the printer settings
- View and manage the security settings
- View and manage the management interface settings
  - IP settings
  - Timeouts
  - View the TLS certificate
- View and select the PIN block formats that the HSM should process

- View and manage the alarm settings
- View and manage the fraud settings
- View and set the HSM’s date and time
- View and set the HSM’s system name and description
- Set audit operations and set the audit counter value
- Select audit-able console, Host, and management commands
- View and manage the SNMP settings
- Load/save the HSM’s settings to a Smart Card
- Reset the HSM’s settings to factory default state

8.4 Virtual Console Tab

Selecting this tab causes the UI to open a virtual console window. Commands can be entered as if you were on the local console at the HSM. Note that not all commands are available. Commands that require the use of the integrated Smart Card reader are not available.

8.4.1 Quick Links

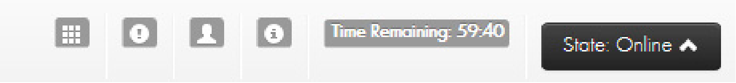
Provides shortcuts to Host interface settings, security settings, load/save settings, and LMK Operations.

8.4.2 Terminate Session

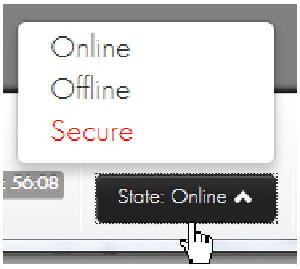
Logs out all users and ends the current session.

8.5 Lower screen icons

The icons are described from right to left.



8.5.1 payShield 10K States



The allowed state transitions are based on the type of users logged in.

For example:

- If only a left **or** only a right RACC are logged into the HSM, then the available states are Online and Offline.
- If at least one left **and** one right RACC are logged into the HSM, then all three state transitions are allowed.

8.5.1.1 Online

In the Online state, the HSM permits communication with a Host computer system by way of the HSM's Host port.

8.5.1.2 Offline

In the Offline state, the HSM prevents communication with the Host computer system. Usually this state is required when changing configuration parameters.

8.5.1.3 Secure

In the Secure state, the HSM prevents communication with the Host computer system. This state is required for certain highly sensitive functions (for example, generating or loading LMKs into the HSM).

8.5.1.4 Switching to Online or Offline State

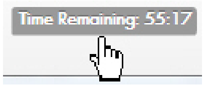
To switch the HSM into the Online or Offline state, simply click the appropriate option from the State button's menu list.

8.5.1.5 Switching to Secure State

Switching the HSM into its Secure state requires one left and one right RACC (both belonging to the HSM in which you wish to switch to secure state) to be authenticated. The action is similar to providing both the left and right physical keys locally and turning them to the secure position.

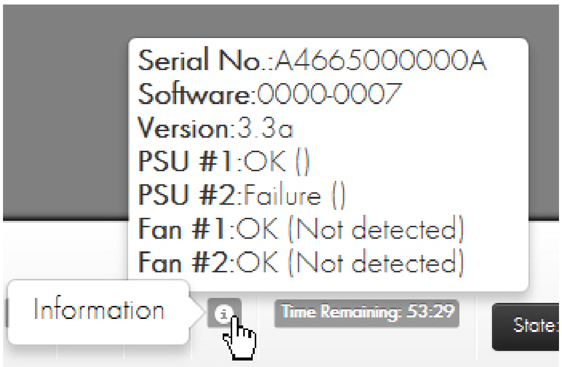
Assuming you logged in with a left RACC, you would simply have to login the right RACC before the “State” button would present the option to move to the “Secure” state.

8.5.2 Time Remaining



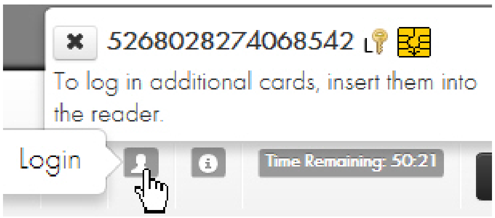
Shows the amount of time left before the automatic termination of the session.

8.5.3 Information



Serial No.:A4665000000A
Software:0000-0007
Version:3.3a
PSU #1:OK ()
PSU #2:Failure ()
Fan #1:OK (Not detected)
Fan #2:OK (Not detected)

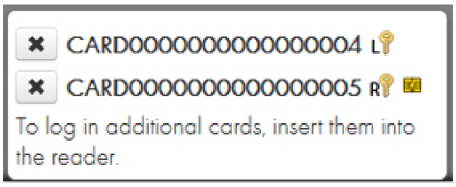
8.5.4 User



✖ 5268028274068542 L

To log in additional cards, insert them into the reader.

Selecting this button shows information on card user(s) and **allows an individual user to logout of the session** by selecting the ✖ next to their card’s serial number.

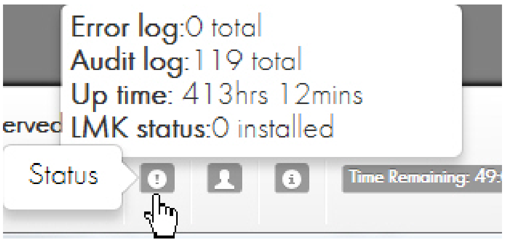


✖ CARD0000000000000004 L
✖ CARD0000000000000005 R

To log in additional cards, insert them into the reader.

The L🔑 icon next to a card serial number indicates that you is a Left RACC. While the R🔑 icon next to a card serial number indicates that you is a Right RACC. The ▣ symbol next to the card serial number indicates that the card is currently inserted into the reader.

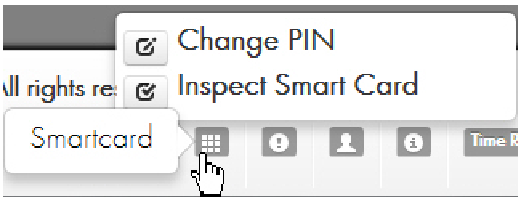
8.5.5 Status



Error log:0 total
Audit log:119 total
Up time: 413hrs 12mins
LMK status:0 installed

Selecting this button displays the number of error and audit log entries, the system up time, and number of LMKs installed.

8.5.6 Smart Card Operations



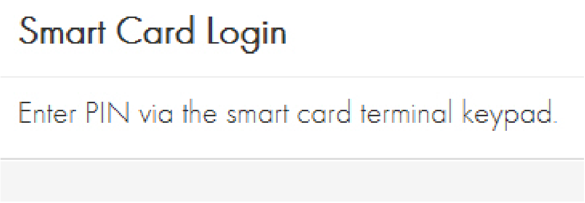
Selecting this button allows you to do Smart Card operations such as Change PIN and Inspect Smart Card.

To change the PIN on a Smart Card, select the “Change PIN” operation and follow the wizard which requires that you insert your Smart Card, enter the current PIN, and finally enter the new PIN.

To view the Smart Card details including **getting the Certificate Number** on the Smart Card, click the “Inspect Smart Card” operation. The Certificate Number is required to manually enter Smart Cards into the whitelist from the **Domain > payShield Security Group** tab.

8.5.7 Login/Logout of Users

8.5.7.1 Login Additional Users



Smart Card Login

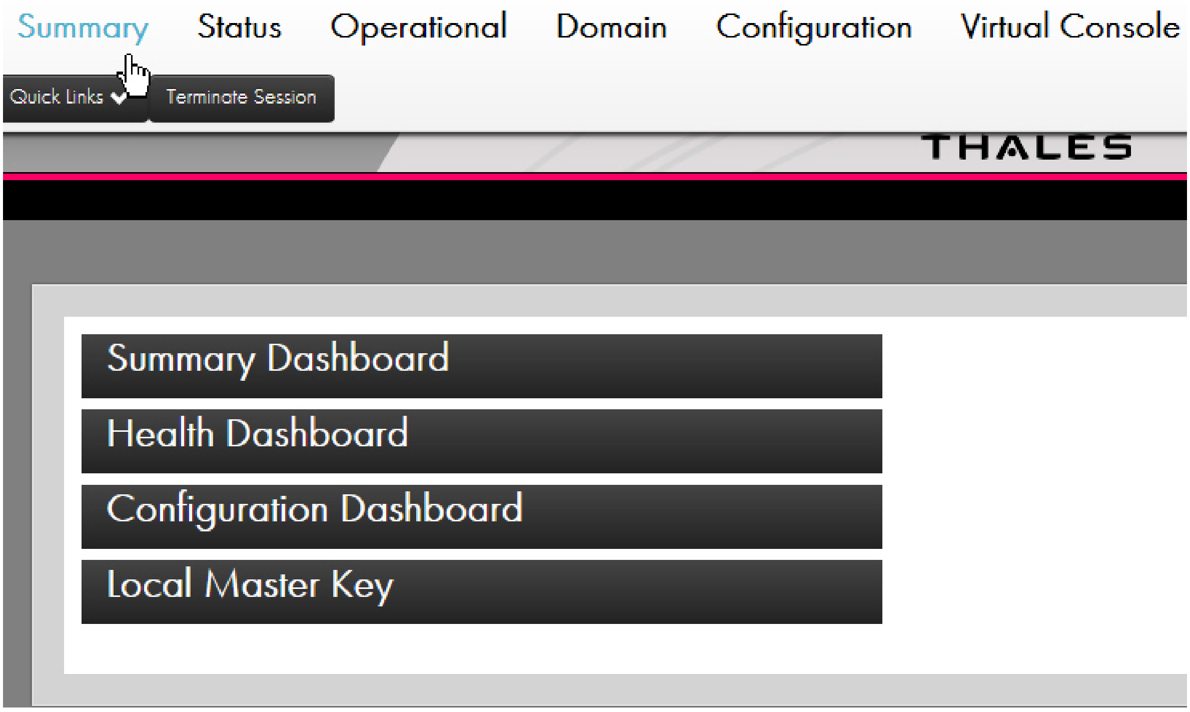
Enter PIN via the smart card terminal keypad.

To login additional users, insert the new user's Smart Card into the Smart Card reader after the initial login (and when not in the middle of a wizard that calls for a Smart Card to be inserted – e.g., Loading an LMK). The system will automatically prompt you for you's PIN and begin the authentication process. Once the authentication has completed successfully, the allowed Host interface state transitions) and logged in users will be updated.

8.5.7.2 User Logout

To logout a logged in user, press the 👤 button at the bottom right of the main page, find you in the list, and press the ✖ button next to it.

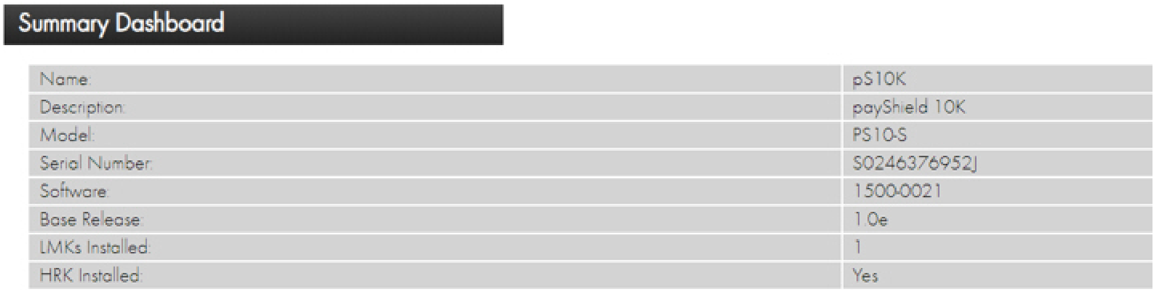
8.6 Summary Page



After a successful login, you will be greeted with the main page as shown below. Each element will be described next.

The four collapsible sections contained on this page are the following:

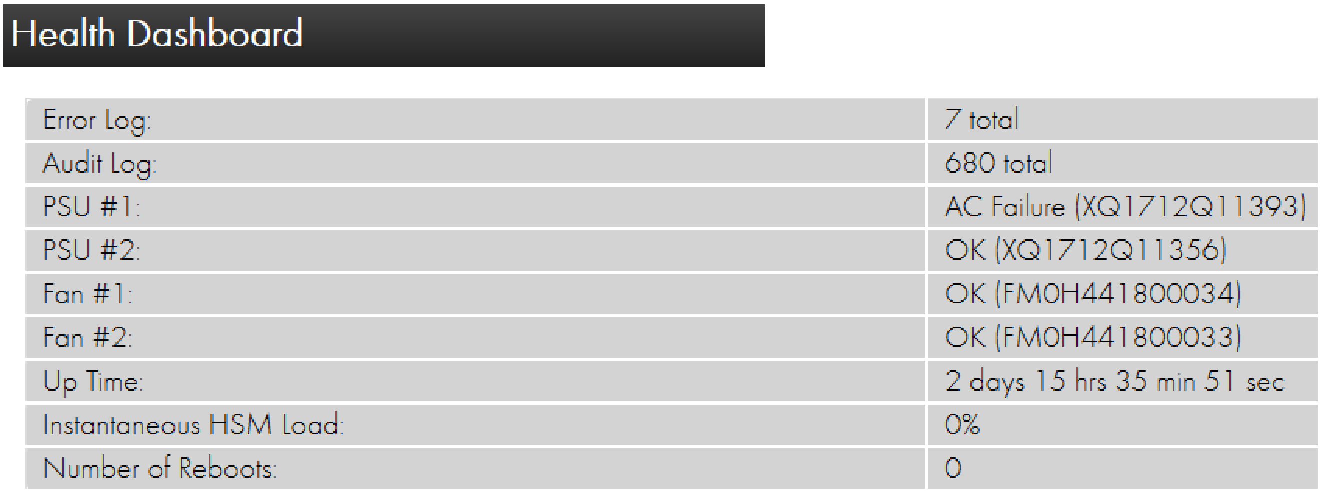
8.6.1 Summary Dashboard


Summary Dashboard

Name:	pS10K
Description:	payShield 10K
Model:	PS10-S
Serial Number:	S0246376952J
Software:	1500-0021
Base Release:	1.0e
LMKs Installed:	1
HRK Installed:	Yes

When expanded, this section displays a table containing Model Number, Serial Number, Software Version, Base Release, the number of LMKs Installed, and the presence of an Installed HRK.

8.6.2 Health Dashboard



Health Dashboard

Error Log:	7 total
Audit Log:	680 total
PSU #1:	AC Failure (XQ1712Q11393)
PSU #2:	OK (XQ1712Q11356)
Fan #1:	OK (FM0H441800034)
Fan #2:	OK (FM0H441800033)
Up Time:	2 days 15 hrs 35 min 51 sec
Instantaneous HSM Load:	0%
Number of Reboots:	0

When expanded this section displays a table containing an Error Log counter, an Audit Log counter, Power Supply Unit status (#1 and #2), System Up-Time, Instantaneous HSM Load (%), and the number of Reboots.

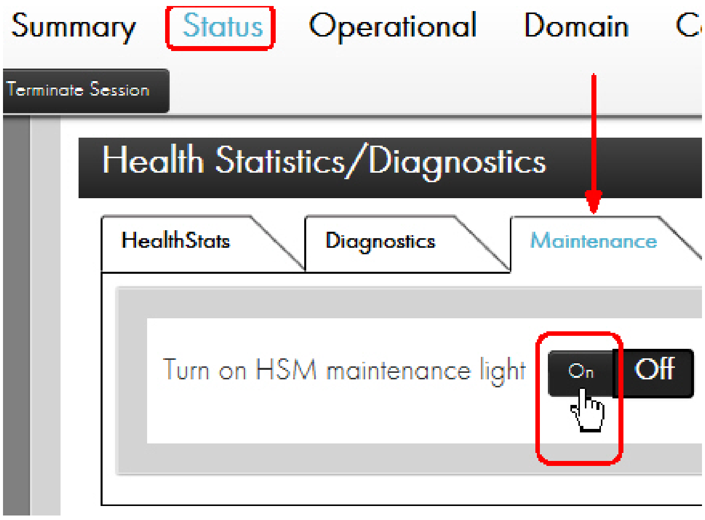
8.6.2.1 How to resolve reported errors

In the example above, the dashboard identifies Failure with Power Supply #2.

The payShield 10K handle light is red.

Follow these steps to resolve:

1. Navigate to **Status > Maintenance**.



2. Click **On**.

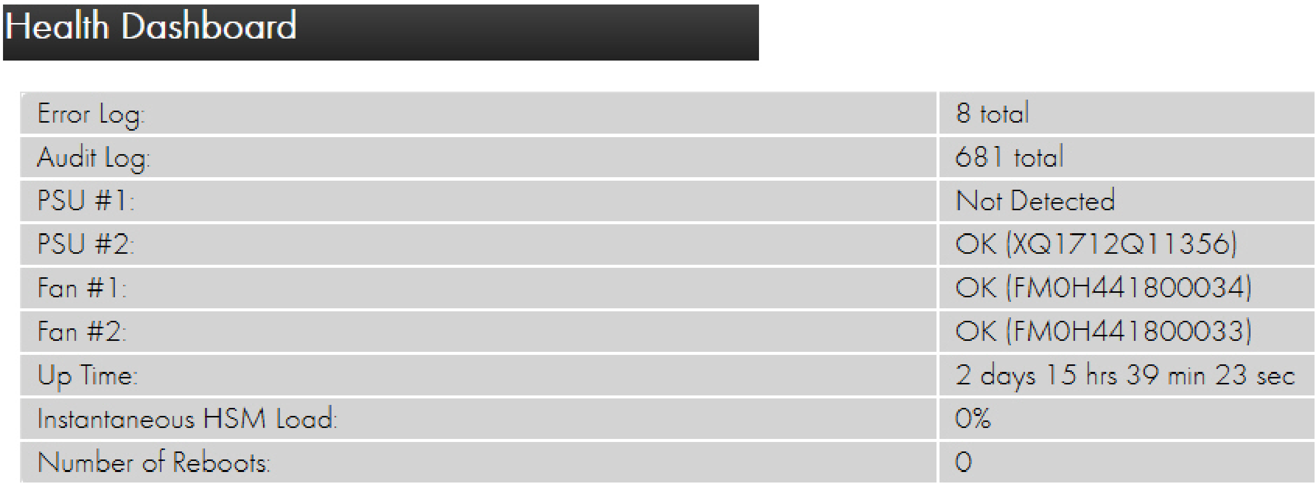
Lights on the payShield 10K turn blue (lights in two locations: front and rear of the panel).

Note: The HSM Maintenance light can be switched to blue via two means: via payShield Manager, as documented above, or manually by a Security Officer who is at the unit.

This light is for informational purposes only and does not impact the status of the payShield 10K in any manner other than turning on the blue service light in on the front and rear panels of the payShield. If the service light is turned on or off, it will be recorded as an event in the Audit Log.

3. Review the error code.

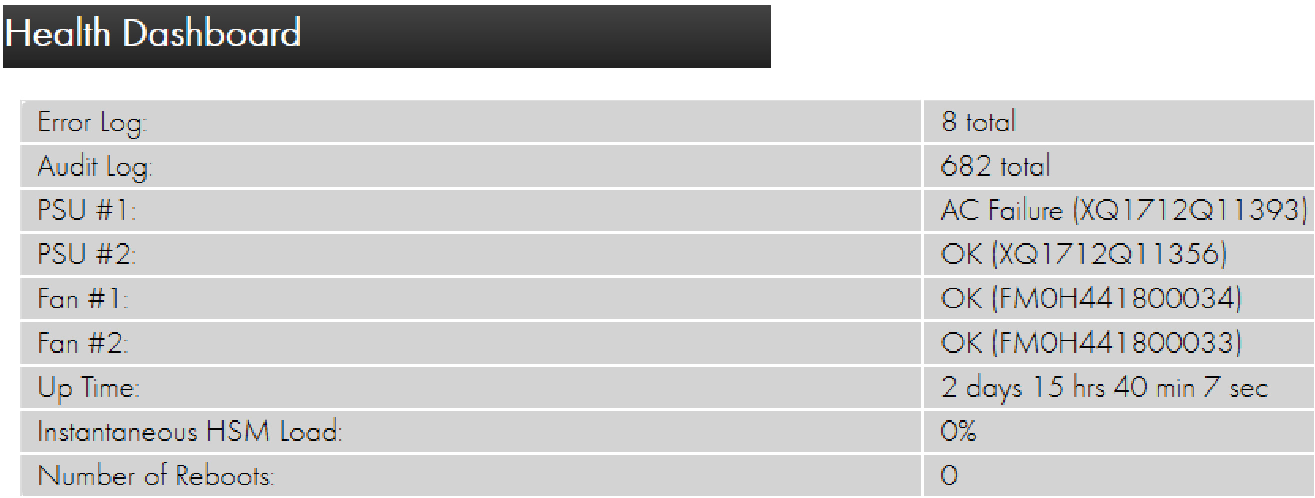
   The Health dashboard reports “NotDetected” when the power supply is removed.



Health Dashboard

Error Log:	8 total
Audit Log:	681 total
PSU #1:	Not Detected
PSU #2:	OK (XQ1712Q11356)
Fan #1:	OK (FM0H441800034)
Fan #2:	OK (FM0H441800033)
Up Time:	2 days 15 hrs 39 min 23 sec
Instantaneous HSM Load:	0%
Number of Reboots:	0

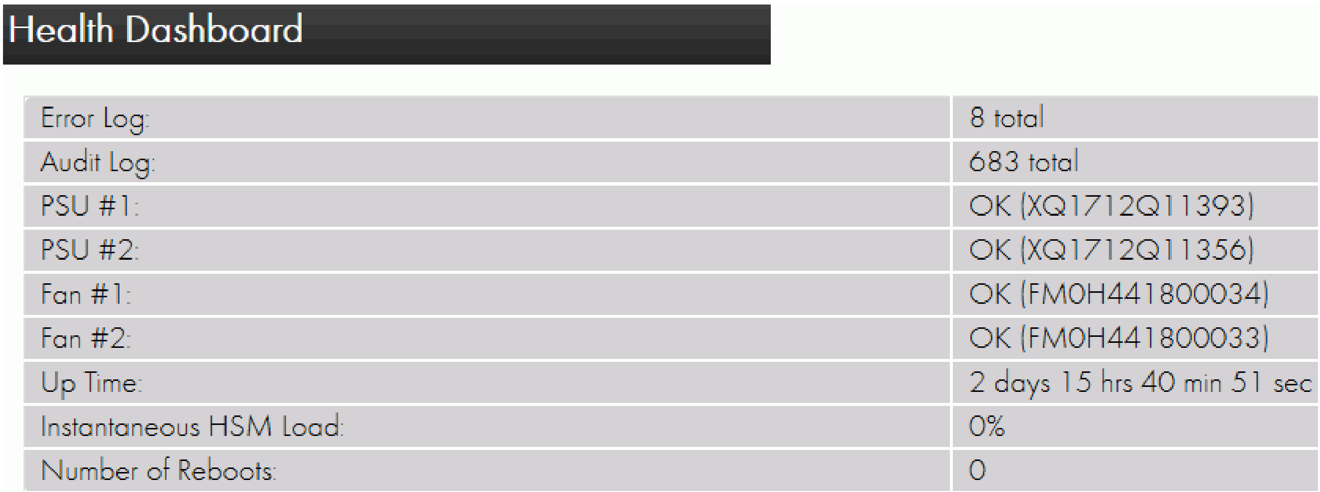
Versus reporting a fault code indicating no electrical power.



Health Dashboard

Error Log:	8 total
Audit Log:	682 total
PSU #1:	AC Failure (XQ1712Q11393)
PSU #2:	OK (XQ1712Q11356)
Fan #1:	OK (FM0H441800034)
Fan #2:	OK (FM0H441800033)
Up Time:	2 days 15 hrs 40 min 7 sec
Instantaneous HSM Load:	0%
Number of Reboots:	0

4. Repair appropriately, i.e., physically replace the power supply / restore lost power.

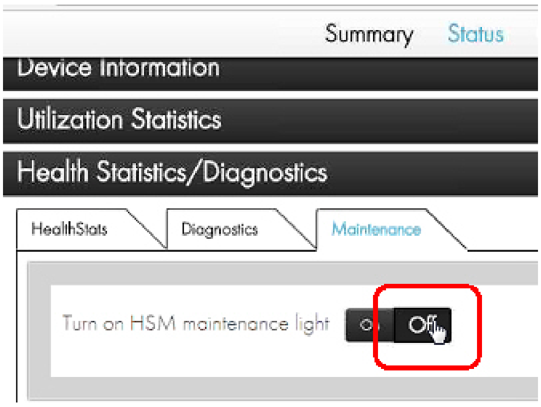


Health Dashboard

Error Log:	8 total
Audit Log:	683 total
PSU #1:	OK (XQ1712Q11393)
PSU #2:	OK (XQ1712Q11356)
Fan #1:	OK (FM0H441800034)
Fan #2:	OK (FM0H441800033)
Up Time:	2 days 15 hrs 40 min 51 sec
Instantaneous HSM Load:	0%
Number of Reboots:	0

5. Navigate to **Status > Health Statistics/Diagnostics > Maintenance**.

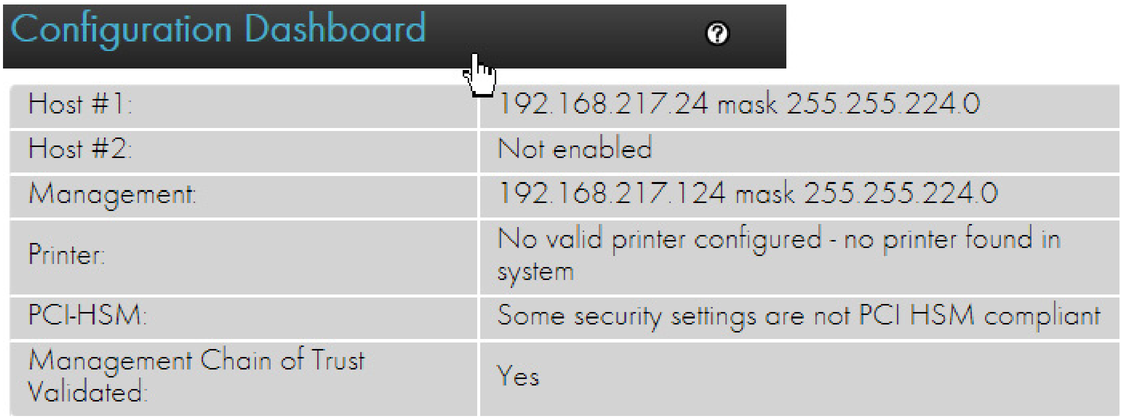
6. Set the maintenance light to **Off**.



Turn on HSM maintenance light On [✓ Off]

Note: Turning the maintenance light to off can also be performed manually at the unit.

8.6.3 Configuration Dashboard

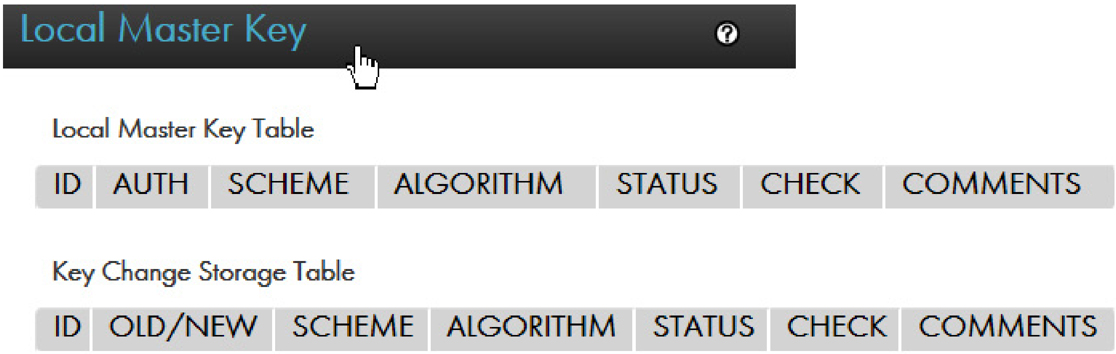


Configuration Dashboard

Host #1:	192.168.217.24 mask 255.255.224.0
Host #2:	Not enabled
Management:	192.168.217.124 mask 255.255.224.0
Printer:	No valid printer configured - no printer found in system
PCI-HSM:	Some security settings are not PCI HSM compliant
Management Chain of Trust Validated:	Yes

When expanded this section displays a table containing Host 1 IP address, Host 2 IP addresses, the management IP address, a summary of the printer configuration, PCI-HSM compliance, and Management Chain of Trust Validation status.

8.6.4 Local Master Key



Local Master Key

Local Master Key Table

ID	AUTH	SCHEME	ALGORITHM	STATUS	CHECK	COMMENTS

Key Change Storage Table

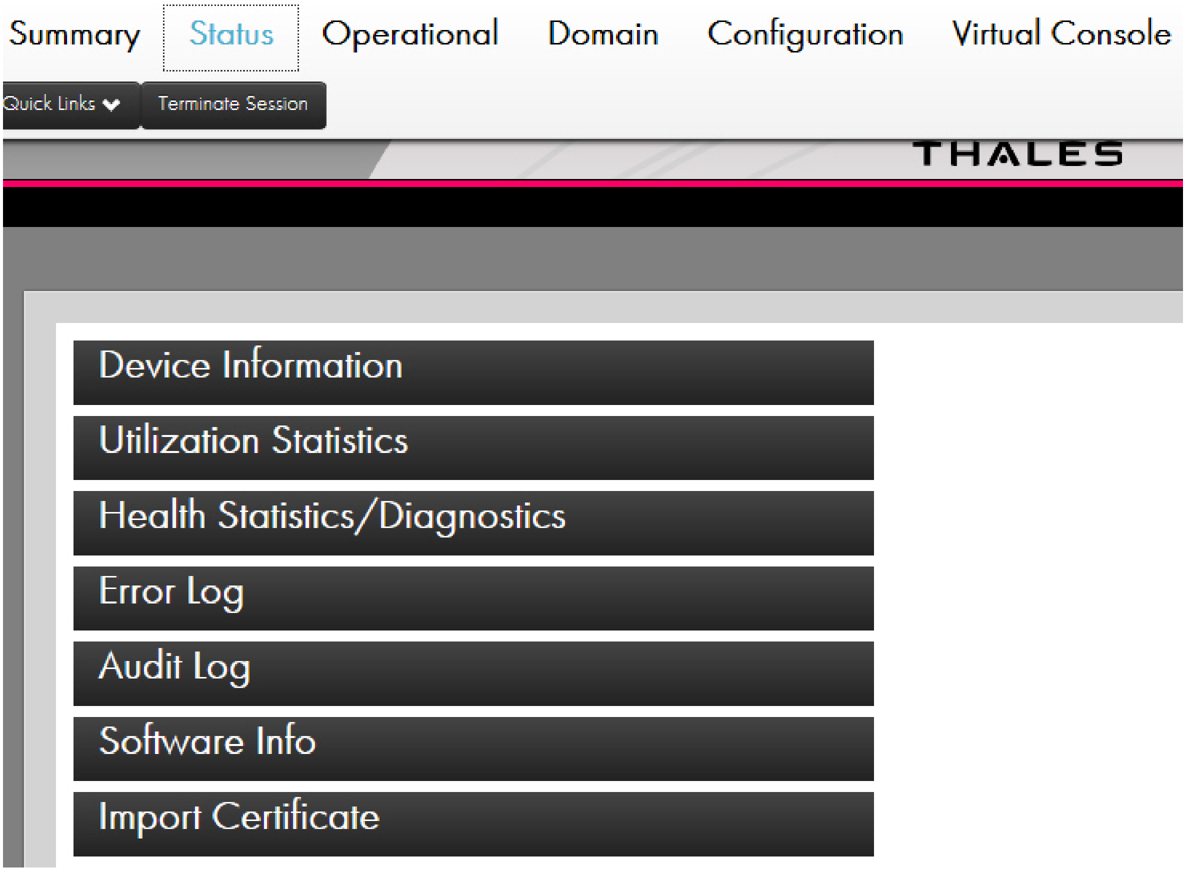
ID	OLD/NEW	SCHEME	ALGORITHM	STATUS	CHECK	COMMENTS

When expanded, this section displays two tables. The first is the Local Master Key Table showing ID, AUTH, SCHEME, ALGORITHM, STATUS, CHECK, and COMMENTS.

The second table shown is the Key Change Storage Table. This table displays ID, SCHEME, ALGORITHM, STATUS, CHECK, and COMMENTS.

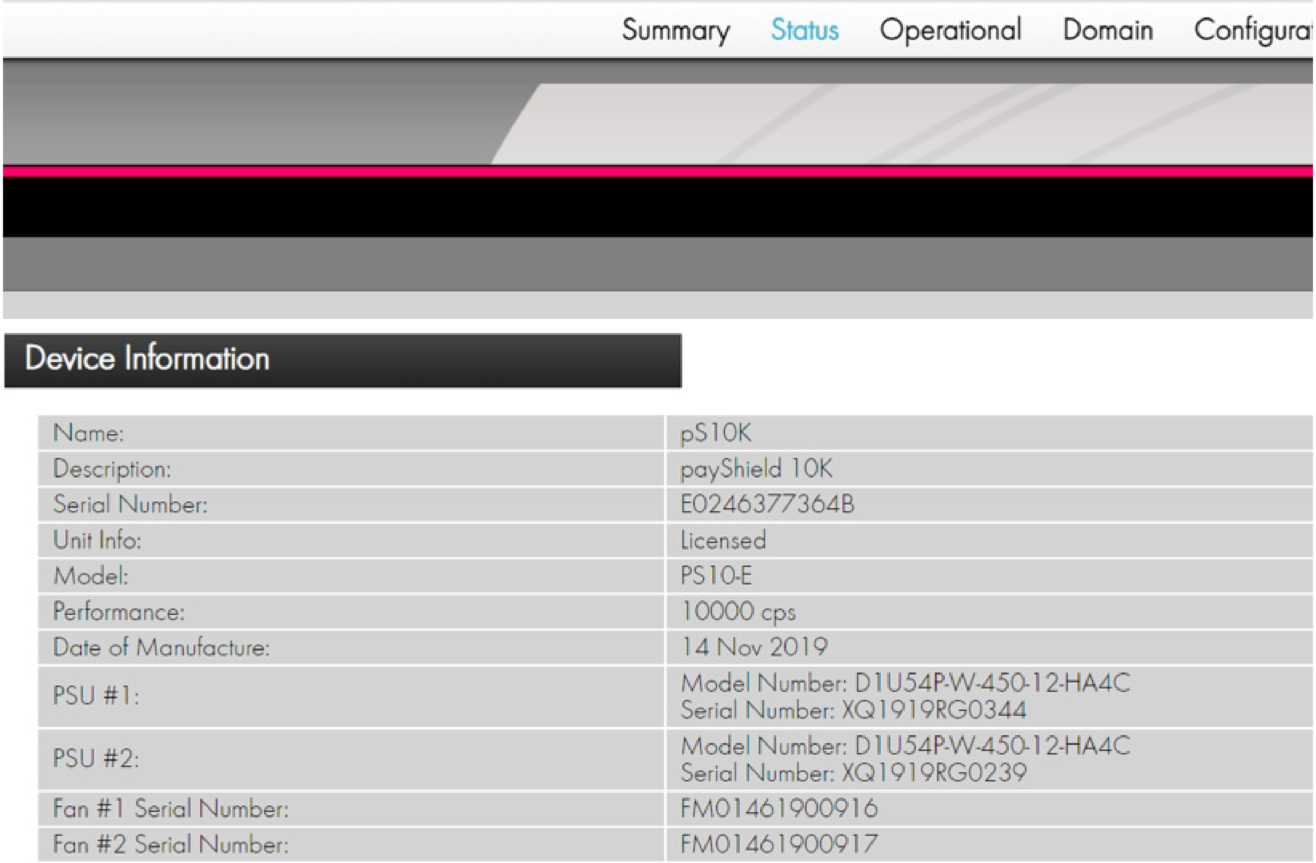
Note: These collapsible menus and the content within are designed to give a quick overview of the current status of the HSM. The values cannot be interacted with or changed from the Summary page.

8.7 Status page



The Status Page can be reached by selecting the “Status” button which is the second button from the left at the top of the frame.

8.7.1 Device Information

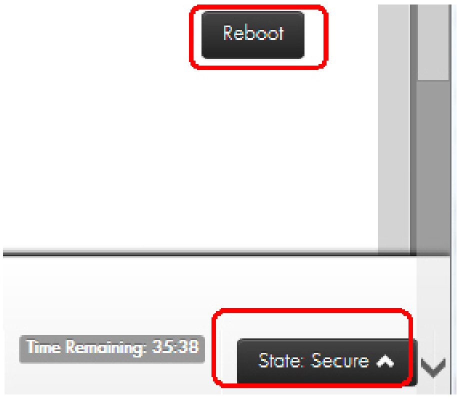


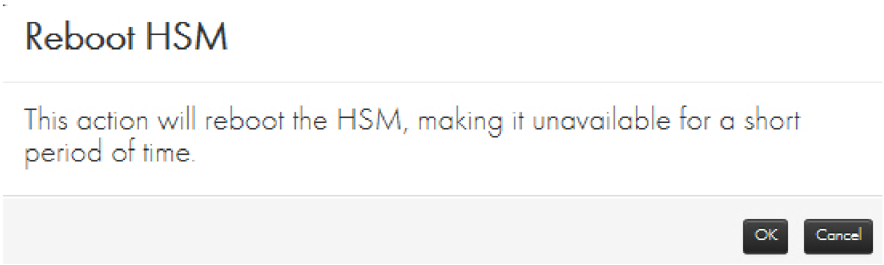
Device Information

Name:	pS10K
Description:	payShield 10K
Serial Number:	E0246377364B
Unit Info:	licensed
Model:	PS10-E
Performance:	10000 cps
Date of Manufacture:	14 Nov 2019
PSU #1:	Model Number: D1U54P-W-450-12-HA4C Serial Number: XQ1919RG0344
PSU #2:	Model Number: D1U54P-W-450-12-HA4C Serial Number: XQ1919RG0239
Fan #1 Serial Number:	FM01461900916
Fan #2 Serial Number:	FM01461900917

The Device Information section contains a table that displays the System Name of the HSM Unit, the Unit Description, Serial Number, Unit Info, Model number, Performance in calls per seconds (cps), the Date of Manufacture, PSU serial numbers, and Fan serial numbers.

Note: These fields are for easy viewing and are not editable.

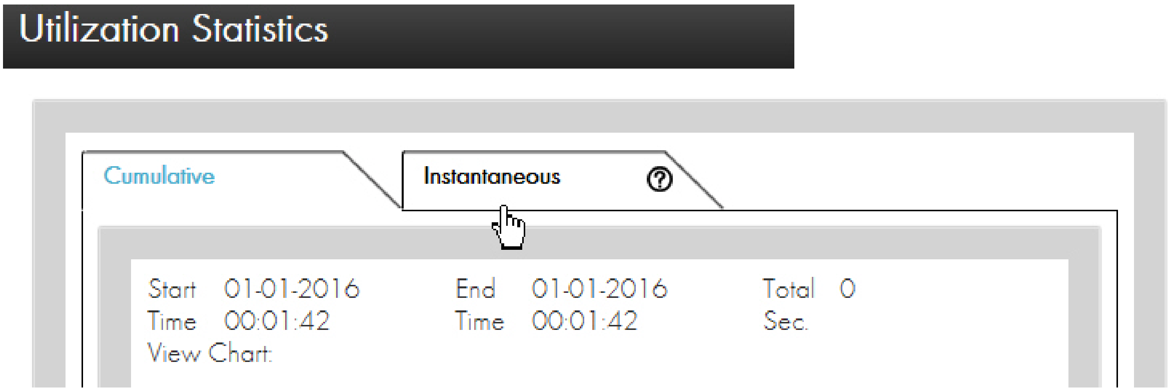




Reboot HSM

This action will reboot the HSM, making it unavailable for a short period of time.

8.7.2 Utilization Statistics



Utilization Statistics

Start Time 01-01-2016 00:01:42
End Time 01-01-2016 00:01:42
Total Sec. 0
View Chart:

The Utilization Statistics section contains a set of click-able tabs. The first tab is titled “Cumulative” and the second tab is titled “Instantaneous”.

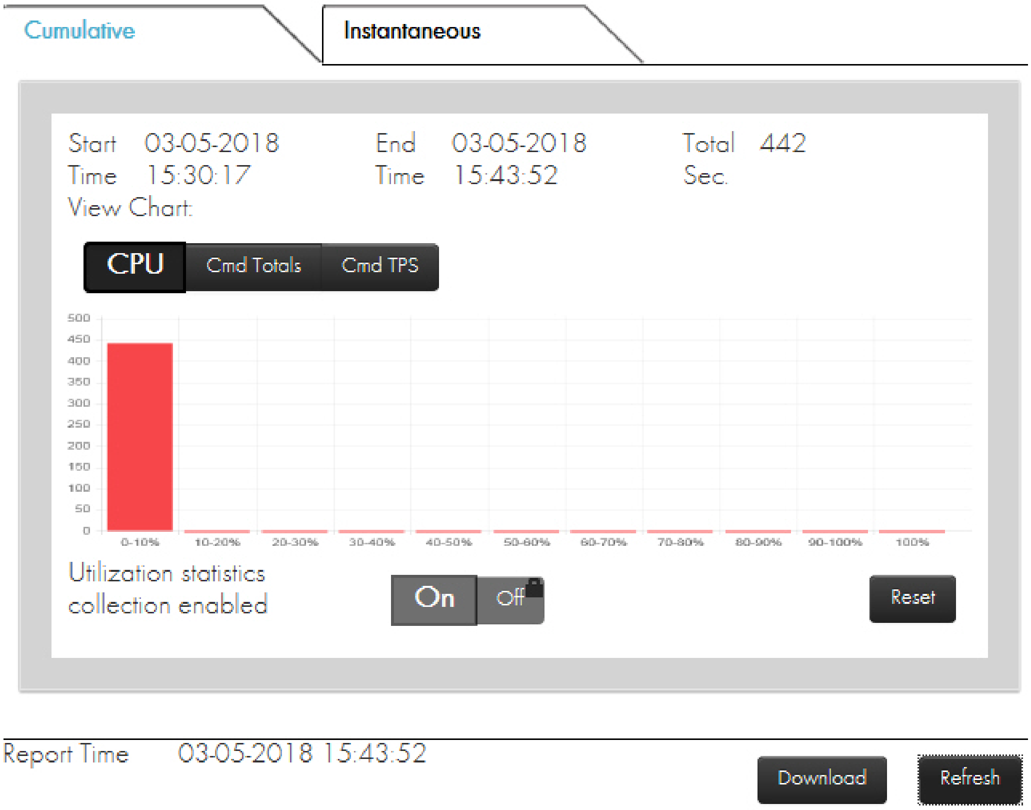
The two tabs provide information showing static statistics about CPU Load, Command Totals and Command TPS.

- Cumulative statistics:

  Displays data accumulated since the last time that you reset the utilization data. It will continue to accumulate until the next time that the data is explicitly reset. The collected data is persistent over re-starts and power being switched off.

- Instantaneous statistics:

  Displays data for the current loading of the HSM, helping administrators investigate throughput or performance issues as they occur.



Start Time 03-05-2018 15:30:17

End Time 03-05-2018 15:43:52

Total Sec. 442

View Chart:

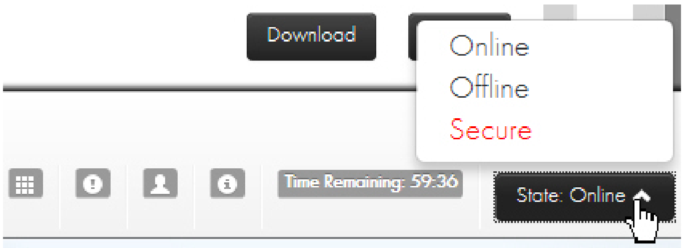
Utilization statistics collection enabled

Report Time 03-05-2018 15:43:52

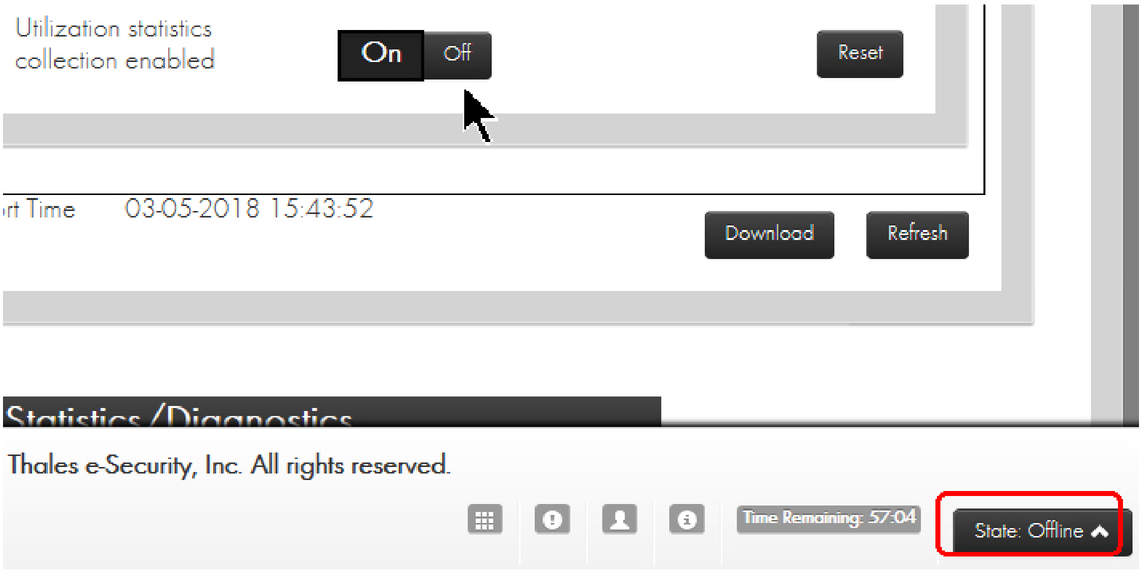
CPU: This data indicates how heavily the HSM is loaded.

Cmd Totals: This data indicates how many times each Host command has been processed.

Cmd TPS: This data indicates the average transactions per second (tps) for each command that has been processed. The rated performance of the HSM relates to how many CA Host commands the HSM could run in a second. The speed a command runs may depend on the options or payload associated with it.

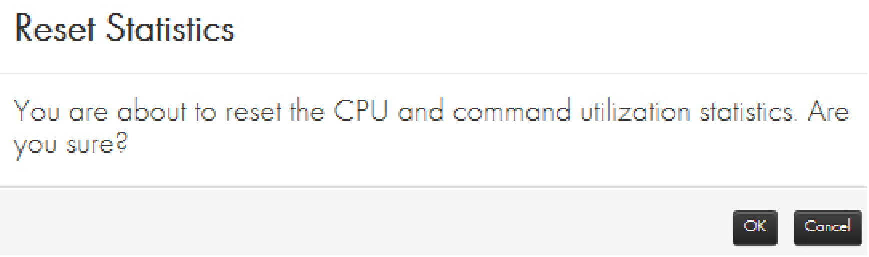


On/Off: In Offline or Secure state, the Utilization statistics collection may be turned on or off.



Additionally, while in the Offline or Secure state:

- Click **Refresh** to refresh statistics.
- Click **Reset** to reset the statistics.

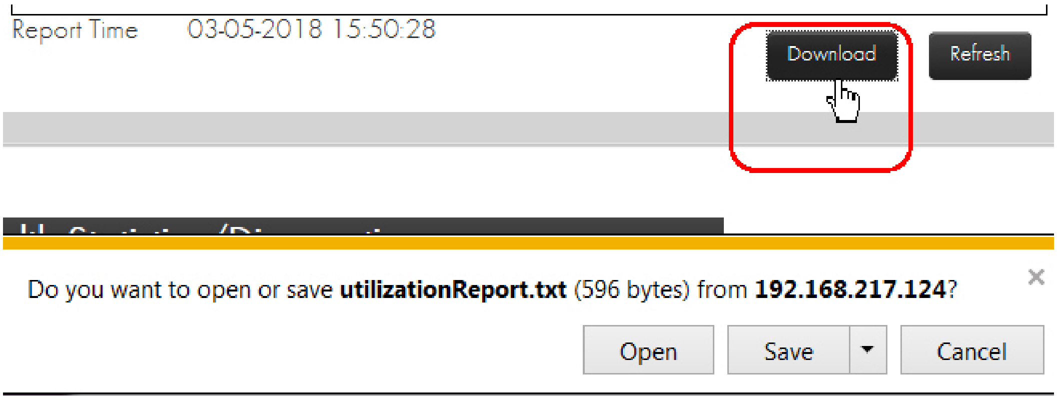


Reset Statistics

You are about to reset the CPU and command utilization statistics. Are you sure?

In any state:

- Click **Download** to save to a text file.

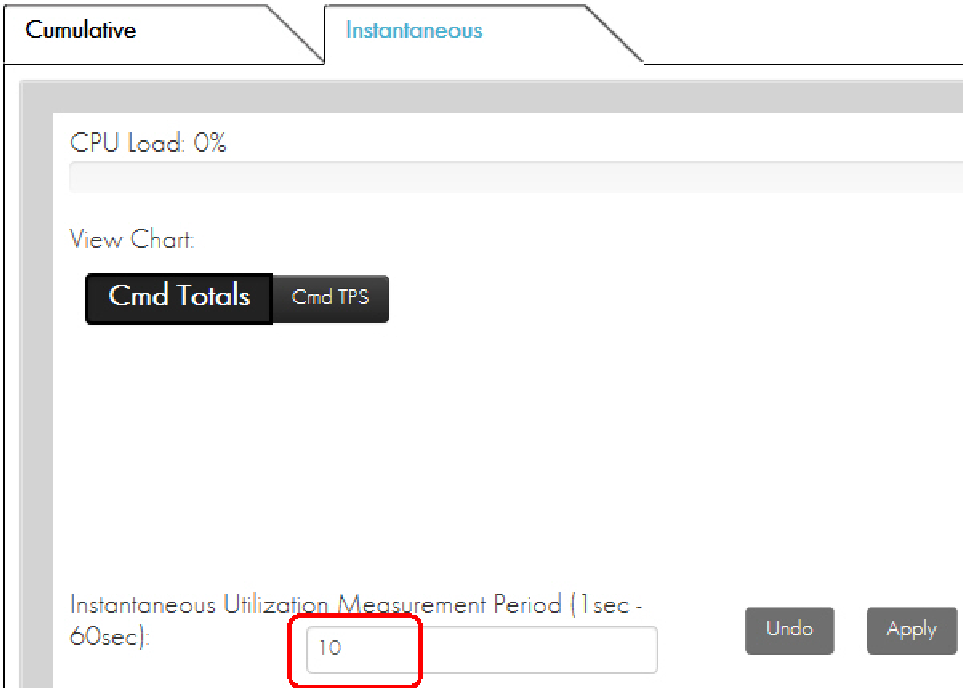


Do you want to open or save **utilizationReport.txt** (596 bytes) from **192.168.217.124**?

From the Instantaneous view, you may change the measurement period as follows:

1. Enter the new value in the Measurement Period field.
2. Click **Apply**.

   Clicking **Undo** restores the prior setting.



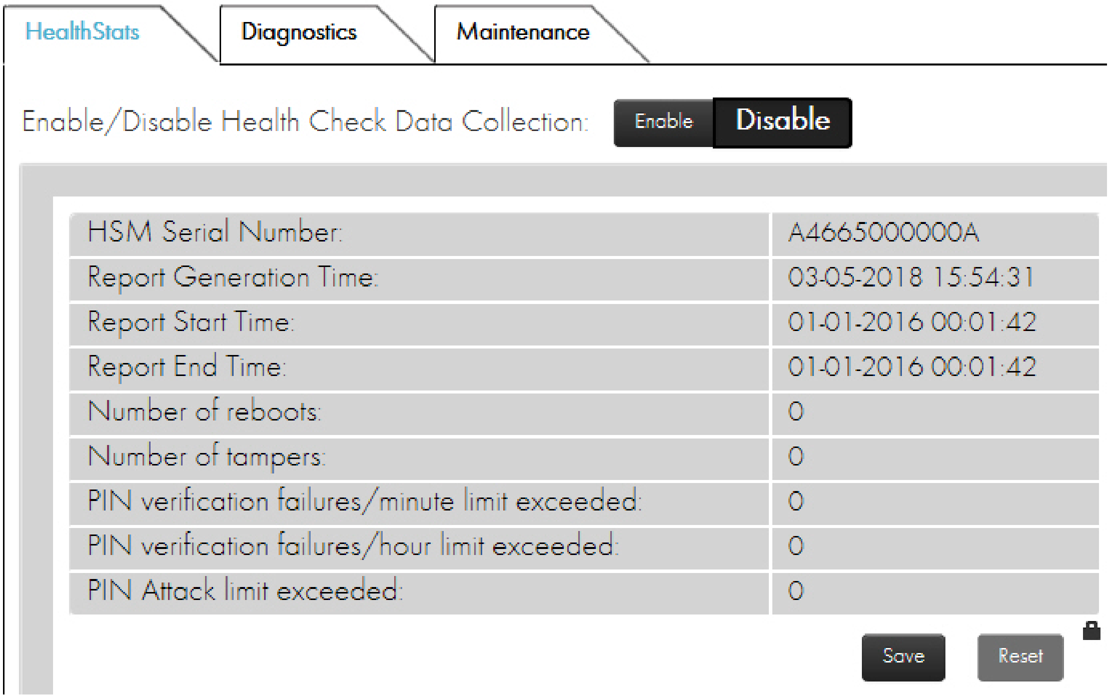
CPU Load: 0%

View Chart:

Instantaneous Utilization Measurement Period (1sec - 60sec): 10

8.7.3 Health Statistics/Diagnostics

8.7.3.1 Health/Stats



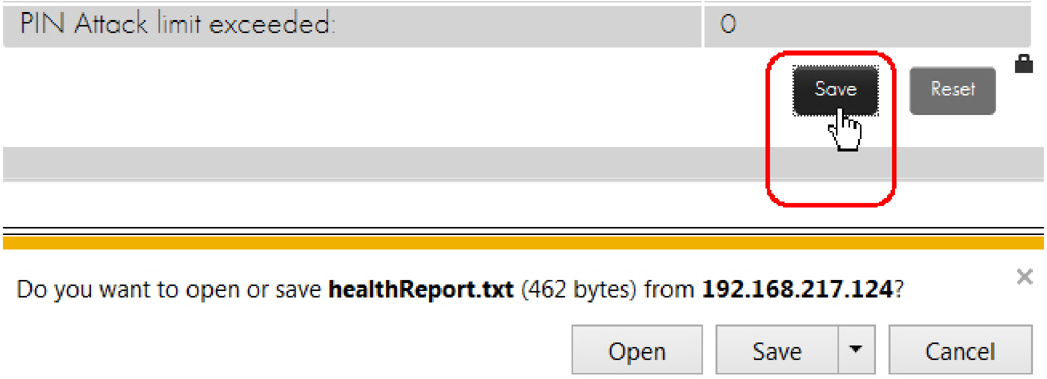
Enable/Disable Health Check Data Collection:

HSM Serial Number:	A4665000000A
Report Generation Time:	03-05-2018 15:54:31
Report Start Time:	01-01-2016 00:01:42
Report End Time:	01-01-2016 00:01:42
Number of reboots:	0
Number of tampers:	0
PIN verification failures/minute limit exceeded:	0
PIN verification failures/hour limit exceeded:	0
PIN Attack limit exceeded:	0

In this section, you can enable and disable the collection of health statistics as well as reset the currently gathered statistics.

In Offline or Secure state, the Health Check Data Collection can be turned on or off using the buttons presented on this page. You may reset the Health Check Data in Offline or Secure state when Authorized using the management LMK.

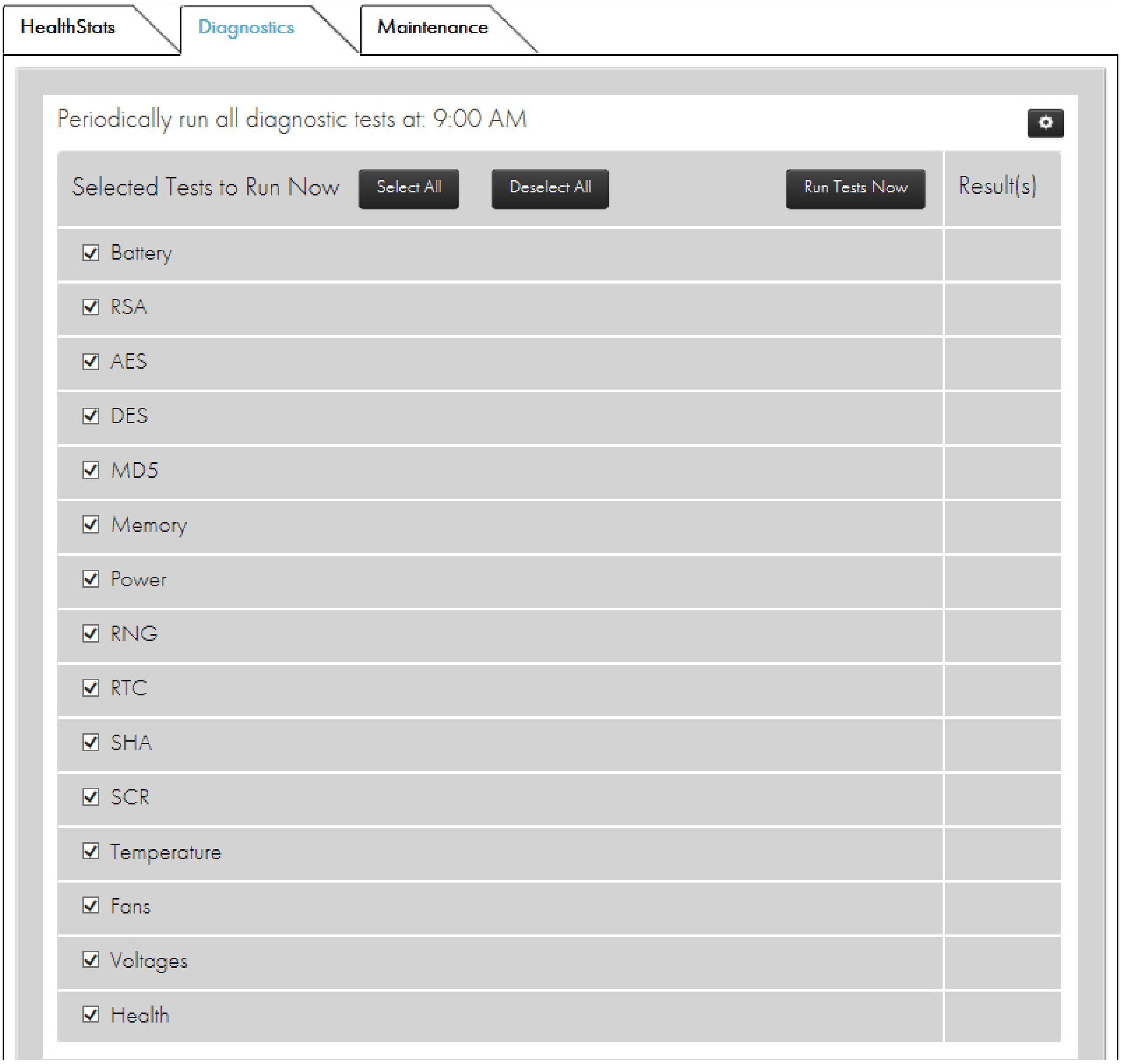
In any state, the Health Check Data can be saved to a text file by selecting **Save**.



PIN Attack limit exceeded:	0

Do you want to open or save **healthReport.txt** (462 bytes) from **192.168.217.124**?

8.7.3.2 Diagnostics



Periodically run all diagnostic tests at: 9:00 AM

Selected Tests to Run Now | Result(s)

☑ Battery
☑ RSA
☑ AES
☑ DES
☑ MD5
☑ Memory
☑ Power
☑ RNG
☑ RTC
☑ SHA
☑ SCR
☑ Temperature
☑ Fans
☑ Voltages
☑ Health

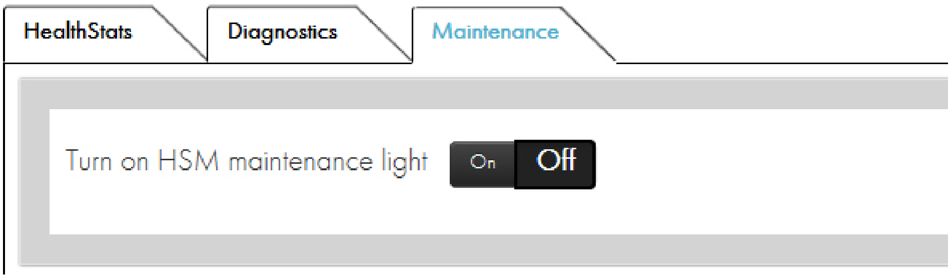
The Diagnostics tab contains a list of tests that are run periodically and can be run immediately. Tests that are run immediately will display their result(s) upon completion. Automated tests do not report results on this screen. (Failures of those results are placed in the error log. No entry means the tests passed.)

To run test(s) immediately, check the box next to the test and select the “Run Tests Now” button. After a short time, the results are displayed next to the test.

When in Offline or Secure state, you can change the automatic run time by selecting the ⚙ control to the right of the self-test time.

Note: For the self-tests to be run at the desired time, the HSM Date and Time must be correctly set.

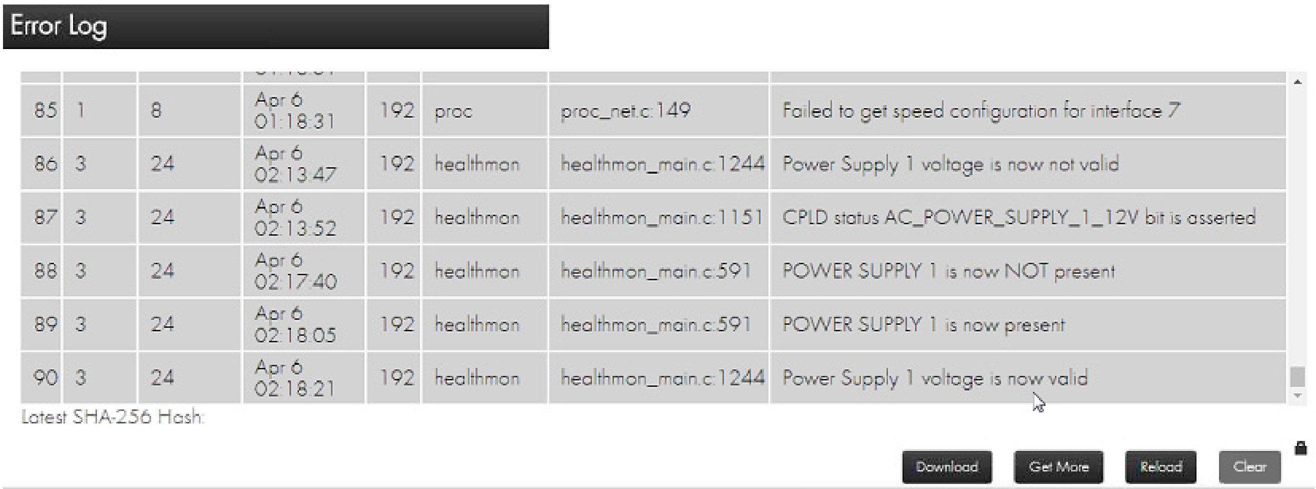
8.7.3.3 Maintenance



Turn on HSM maintenance light On [✓ Off]

The payShield 10K has a service light on the front and rear panel of the HSM. This light can be toggled on or off only through payShield Manager or directly in front of the payShield using the On/Off button. This light is for informational purposes only and does not impact the status of the payShield 10K in any manner other than turning on the blue service light in on the front and rear panels of the payShield. If the service light is turned on or off, it will be recorded as an event in the Audit Log.

8.7.4 Error Log



85	1	8	Apr 6 01:18:31	192	proc	proc_net.c:149	Failed to get speed configuration for interface 7
86	3	24	Apr 6 02:13:47	192	healthmon	healthmon_main.c:1244	Power Supply 1 voltage is now not valid
87	3	24	Apr 6 02:13:52	192	healthmon	healthmon_main.c:1151	CPLD status AC_POWER_SUPPLY_1_12V bit is asserted
88	3	24	Apr 6 02:17:40	192	healthmon	healthmon_main.c:591	POWER SUPPLY 1 is now NOT present
89	3	24	Apr 6 02:18:05	192	healthmon	healthmon_main.c:591	POWER SUPPLY 1 is now present
90	3	24	Apr 6 02:18:21	192	healthmon	healthmon_main.c:1244	Power Supply 1 voltage is now valid

Latest SHA-256 Hash:

The Error Log stores fault information for use by Thales eSecurity support personnel. The Error log is used to log unexpected software errors, hardware failures, and alarm events. Only catastrophic errors cause the HSM to reboot.

For each entry in the log, the following information is displayed:

- ID

- System
- Subsystem
- Time
- User
- Process
- File
- Message

Below the log table there are options to Download, Get More, Reload, and Clear.

Selecting Download retrieves a Comma-Separated-File (CSV) text file (which can be directly imported into a spreadsheet, for example) of all the log entries. Upon completion of the download, the UI displays the SHA-256 Hash of the downloaded file. You can use offline tools to compute the hash yourself and compare it with the value displayed in the UI to ensure that the log is accurate. The hash is computed over the file itself, not the value of its contents. Copy/Pasting the contents into a hash function will give incorrect results.

Note: If the log is very long, it may take a while to retrieve and can impact performance of the HSM.

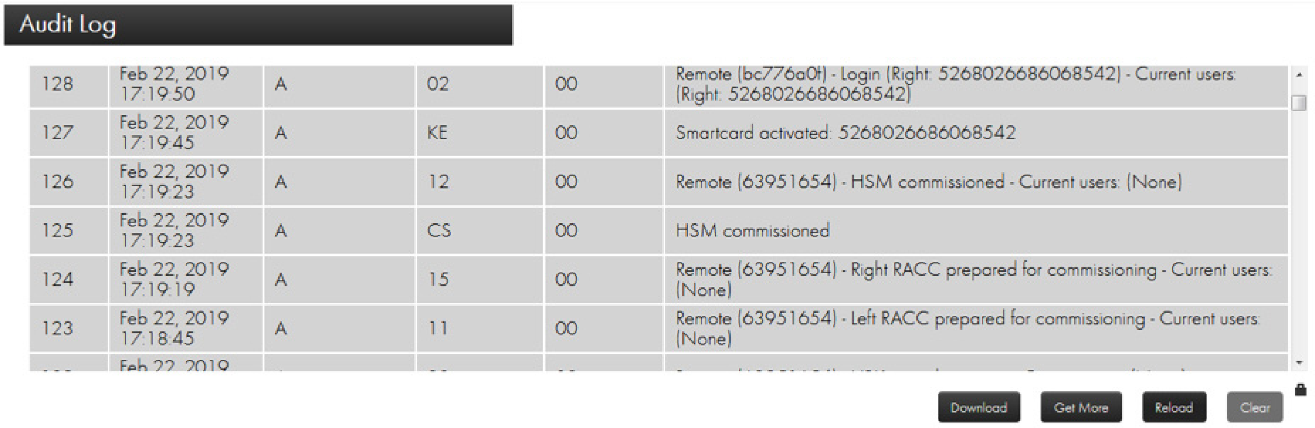
- Selecting **Get More** returns the next batch of log entries.
- Selecting **Reload** gets the first batch of log entries.
- Selecting **Clear**, which is only available in secure state, clears all error log entries.

8.7.5 Audit Log

Note: The items in the Audit Log includes both:

- Items identified via configuration settings page (i.e., **Configuration > Audit Settings)** and
- Items that are included automatically.

Certain sensitive functions, such as key management, authorizations, configuration and diagnostic tests are always automatically recorded in the audit log.



Audit Log

128	Feb 22, 2019 17:19:50	A	02	00	Remote (bc776a0f) - Login (Right: 5268026686068542) - Current users: (Right: 5268026686068542)
127	Feb 22, 2019 17:19:45	A	KE	00	Smartcard activated: 5268026686068542
126	Feb 22, 2019 17:19:23	A	12	00	Remote (63951654) - HSM commissioned - Current users: (None)
125	Feb 22, 2019 17:19:23	A	CS	00	HSM commissioned
124	Feb 22, 2019 17:19:19	A	15	00	Remote (63951654) - Right RACC prepared for commissioning - Current users: (None)
123	Feb 22, 2019 17:18:45	A	11	00	Remote (63951654) - Left RACC prepared for commissioning - Current users: (None)
	Feb 22, 2019				

The Audit Log can contain up to 100,000 entries for audit records. The audit records are added to the log until it is full and for each subsequent record, the oldest record in the log is deleted to make room for the new one.

Whenever the HSM state is altered through power-up, state changes, or payShield Manager commands, the Audit Log is updated with the Time/Date, the Command Code Type, the Command Code, the Response Code, and a Text field with a brief description.

The Audit Log can be configured to record the execution of any payShield Manager, console or Host command. Configure the Audit Log in the “Audit Settings” menu on the “Configuration” page. Refer to Section 8.10, “Configuration”, on page 154.

Note: Some events are always audited, even if you has not specified auditing activity.

Below the log table there are options to **Download**, **Get More**, **Reload**, and **Clear**.

The Download option retrieves a Comma-Separated-File (CSV) text file (which can be directly imported into a spreadsheet, for example) of all the log entries. Upon completion of the download, the UI displays the SHA-256 Hash of the downloaded file. Using offline tools, you can manually compute the hash and compare your calculation with the value displayed in the UI, to ensure that the log is accurate.

Note: The hash is computed over the file itself, not the value of its contents. Copy/Pasting the contents into a hash function will give incorrect results.

Note: If the log is very long, it may take a while to retrieve and can impact performance of the HSM.

- Selecting **Get More** returns the next batch of log entries.
- Selecting **Reload** gets the first batch of log entries.
- Selecting **Clear**, which is only available in secure state, clears all error log entries.

The following table lists all of the audit log messages.

Category	Audit Log Messages	Notes
Access Control List (ACL)	TCP/TLS connection from x.x.x.x to y.y.y.y refused due to ACL UDP traffic from x.x.x.x to y.y.y.y refused due to ACL	*Optional (controlled by “Audit ACL connection failures” audit option; Disabled by default)* x.x.x.x - source IP address y.y.y.y - destination IP address (Host 1 or Host 2)
Audit log	Audit log was cleared Cleared all retrieved audit logs Cleared all archived audit logs	
Authentication	Authentication cmd XX executed	“XX” is the authentication related console command (such as CO, KD, SP, XD, XH, XR) that was executed

Table 4 Audit Log Messages

Category	Audit Log Messages	Notes
Authorization	Activity A was authorized for LMK id 0-19 Activity A:T was authorized for LMK id 0-19 Authorization activity A:T was cancelled Authorization activity A was cancelled for LMK id 0-19 Authorization activity A:T has expired for LMK id 0-19 HSM was authorized for LMK id 0-19 HSM authorization was cancelled for LMK id 0-19	A - activity list, T - timeout
Bootup	System Restarted	
Console command	Console command XX	"XX" is the console command that was executed Audit of desired console commands is done via "auditoptions" console command or via payShield Manager Security sensitive console commands are always audited.
Commissioning	HSM commissioned HSM decommissioned HSM commission failed; error "error message"	
Diagnostics	Diagnostic self tests passed Diagnostic self test failure: "test name"	*Optional (controlled by "Audit diagnostic self tests" audit option; Disabled by default)* "test name" is name of the failed diagnostic self test
Firmware update	Firmware update attempted Firmware update package validation failed Firmware update failed Firmware update to revision XXXX-XXXX and bootstrap version y.y.y successful/failed	"Firmware update failed" is generated when firmware update fails and version info is not available (such as package validation failure) Where XXXX-XXXX is the firmware revision If bootstrap was present in the update package, "and bootstrap version y.y.y" is included in the log (where y.y.y is the bootstrap version)
Fraud	Fraud event detected executing Host command XX - Limit of number of PIN verification failures per minute exceeded Fraud event detected executing Host command XX - Limit of number of PIN verification failures per hour exceeded Fraud event detected executing Host command XX - PIN attack limit exceeded	"XX" is the Host command that was executed

Table 4 Audit Log Messages (Continued)

Category	Audit Log Messages	Notes
FRU (Field Replaceable Units - fans, PSUs)	FAN 1/2 removed FAN 1/2 restored Fan 1/2 replaced: “fru serial number” Power Supply 1/2 removed Power Supply 1/2 restored Power Supply 1/2 replaced: “fru serial number” Power Supply 1/2 AC outage Power Supply 1/2 AC restored	“fru serial number” is the FRU serial number
Health	Health Check Statistics reset to 0	
Host command	Host command XX Host command XX, response EE	Audit of desired Host commands is done via “auditoptions” console command or via payShield Manager *Optional (controlled by “Audit Error Responses to Host Commands” audit option; Disabled by default)* XX is the Host command EE is the error response to the Host command
Key Management	Smartcard activated: “card serial number” Smartcard PIN changed Key management command XX executed Loaded CTA share from smartcard Stored CTA share on smartcard Smartcard serial number read error	“card serial number” is the smartcard serial number XX is the key management command that was executed
Keylock	Keylock turned to Online/Offline/Secure	
Licensing	New license file loaded License file load failed	
LMK	LMKs loaded LMKs erased Keychange LMKs loaded Keychange LMKs erased	
Maintenance	payShield “device serial number” maintenance light switch ON/OFF	“device serial number” is the 10K device serial number

Table 4 Audit Log Messages (Continued)

Category	Audit Log Messages	Notes
Management	Format of the audit logs for payShield Manager commands is as follows: Remote (xxxxxxxx) - “command string” - Current users: (None / Left: SSSS / Right: SSSS / Guest: SSSS) xxxxxxxx is the session cookie id SSSS is the card serial number **Below are the various management command strings/ messages when the command is successful. A few of these are configurable (enabled/disabled via payShield Manager Audit Settings).** HSM state changed to Online/Offline/Secure Login / Logout Session terminated Single authorized state entered Single authorized state cancelled ***<continued next page>***	Security sensitive management actions/ commands are always audited. “Current Users:” will list all the logged in users.

Table 4 Audit Log Messages (Continued)

Category	Audit Log Messages	Notes
Management	CTA generated CTA share read from smartcard (optional - disabled by default) CTA share loaded from smartcard (optional - disabled by default) CTA share created on smartcard CTA share stored on smartcard RACC commissioned Left RACC prepared for commissioning Right RACC prepared for commissioning Key RACC for commissioning prepared HSM commissioned Periodic self diagnostic tests schedule changed Diagnostic tests executed Alarm settings modified HSM date and time updated PIN block settings modified Fraud settings modified Fraud detection re-enabled Enabled Host commands modified Enabled console commands modified Audit settings modified Host commands audit modified Console commands audit modified Remote management commands audit modified Health statistics report generated (optional - disabled by default) Health statistics reset (optional - disabled by default) HRK passphrase set HRK passphrase 1 changed HRK passphrase 2 changed General Host settings modified Ethernet Host settings modified ACL Host settings modified Error log cleared Error log retrieved (optional - disabled by default) Error log downloaded (optional - disabled by default) Audit log cleared ***<continued on next page>***	

Table 4 Audit Log Messages (Continued)

Category	Audit Log Messages	Notes
Management (continued)	Audit log retrieved (optional - disabled by default) Audit log downloaded (optional - disabled by default) New LMK installed / deleted Keychange old LMK installed Keychange new LMK installed Keychange LMK deleted LMK generated LMK copied LMK verified Authorizing officer card created Management interface settings modified Printer settings modified (optional - disabled by default) Test page printed (optional - disabled by default) General security settings modified Initial security settings modified SNMP state changed (optional - disabled by default) SNMP port changed (optional - disabled by default) SNMP user added (optional - disabled by default) SNMP user deleted VR info retrieved (optional - enabled by default) Licensing info retrieved (optional - disabled by default) Firmware update attempted License updated (optional - enabled by default) Utilstats settings modified (optional - disabled by default) Utilstats state changed (optional - disabled by default) Utilstats reset (optional - disabled by default) Miscellaneous settings modified (optional - disabled by default) Multiple authorized state changed Whitelist modified Session timeout settings modified Management TLS certificate imported Host TLS certificate imported LMK share loaded LMK share stored LMK split LMK reassembled LMK password loaded LMK password stored HSM settings loaded from smartcard HSM settings saved to Smart Card (optional - enabled by default) HSM settings reset to factory state HSM rebooted **Failure audit logs are generated for most of the above commands/actions when the command fails:** Login / Logout failed Failed to generate CTA Failed to read CTA share from smartcard Failed to load CTA share from smartcard Failed to create CTA share on smartcard Failed to store CTA share on smartcard Failed to commission RACC Failed to prepare left RACC for commissioning Failed to prepare right RACC for commissioning ***<continued next page>***	

Category	Audit Log Messages	Notes
Management (Continued)	Failed to commission HSM Failed to update license Failed to set HRK passphrases Failed to change HRK passphrase 1 Failed to change HRK passphrase 2 Failed to update HSM date and time Failed to install keychange old LMK Failed to delete new LMK Failed to generate LMK Failed to copy LMK Failed to verify LMK Failed to load LMK share Failed to store LMK share Failed to split LMK Failed to reassemble LMK Failed to create authorizing officer card Failed to import management TLS certificate Failed to import Host TLS certificate Failed to load HSM settings from smartcard Failed to save HSM settings to smartcard Failed to reset to HSM settings to factory state Failed to enter single authorized state Failed to modify whitelist	
Reboot	System rebooted due to firmware update System rebooted due to management request System rebooted due to critical diagnostic test failure - “failed test name”	
Secure Host Comms	Certificate not yet valid. Unique ID: “Cert ID” Certificate has expired. Unique ID: “Cert ID” Error in Cert. Not Before Field. Unique ID: “Cert ID” Error in Cert. Not After Field. Unique ID: “Cert ID”	“Cert ID” is the certificate's unique ID
Settings	HSM settings saved to smartcard HSM settings loaded from smartcard HSM settings saved to smartcard (remote) HSM settings loaded from smartcard (remote)	“(remote)” refers to settings save/restore from payShield Manager
SNMP	SNMP user added/deleted SNMP trap receiver added/deleted	
Tamper	Tamper Detected “tamper text” High Tamper Detected “tamper text” Tamper Cleared	“tamper text” provides tamper details
Utilization	Utilization Statistics reset to 0	*Optional (controlled by “Audit utilization data resets” audit option; Enabled by default)*

Table 4 Audit Log Messages (Continued)

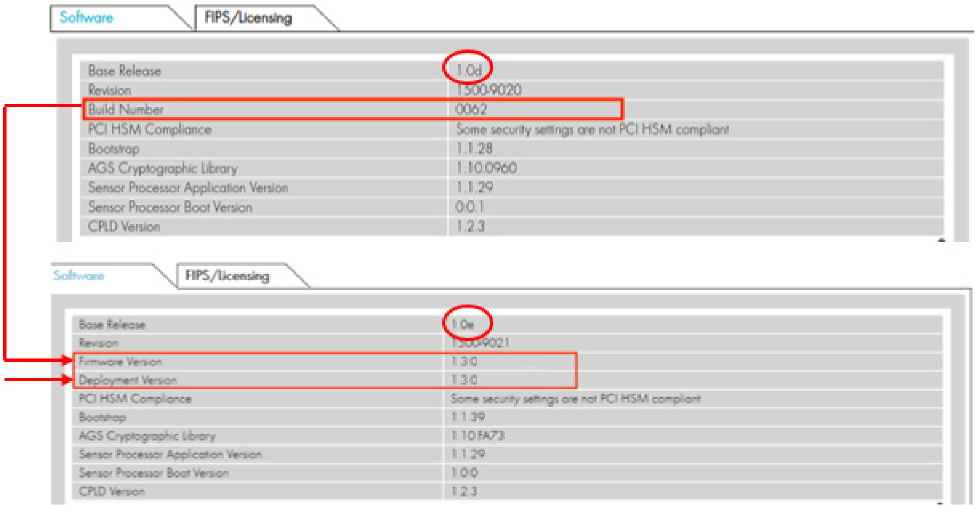
8.7.6 Software Info

The Software tab provides information on the versions of the currently installed software and allows new software to be loaded.

8.7.6.1 Software - how to update software

Note: With Release 1.0e, the Software tab has been updated. “Build Number” was changed to “Firmware Version” and a new entry “Deployment Version” has been added. Both fields are used only to assist Thales Support.

The figure below shows both 1.0d and 1.0e screens for clarification purposes.



Base Release	1.0d
Revision	1500-9020
Build Number	0062
PCI HSM Compliance	Some security settings are not PCI HSM compliant
Bootstrap	1.1.28
AGS Cryptographic Library	1.10.0960
Sensor Processor Application Version	1.1.29
Sensor Processor Boot Version	0.0.1
CPLD Version	1.2.3

Base Release	1.0e
Revision	1500-9021
Firmware Version	1.3.0
Deployment Version	1.3.0
PCI HSM Compliance	Some security settings are not PCI HSM compliant
Bootstrap	1.1.39
AGS Cryptographic Library	1.10.FA73
Sensor Processor Application Version	1.1.29
Sensor Processor Boot Version	1.0.0
CPLD Version	1.2.3

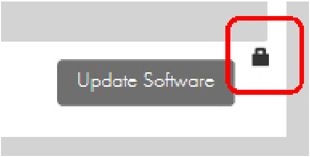
“Firmware Version” was formerly referred to as “Build Number” and is used to assist Thales Support only

“Deployment Version” was added to assist Thales Support only

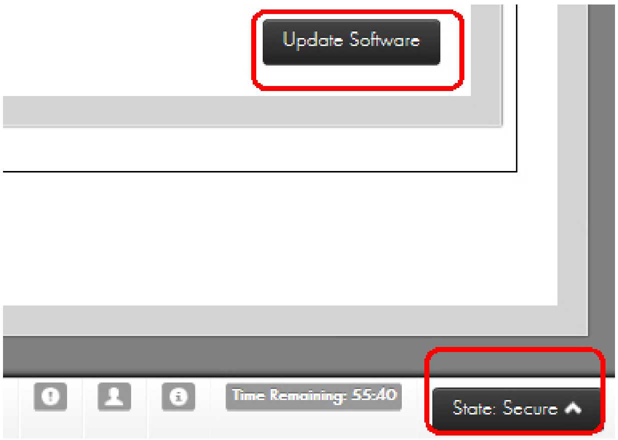
To update software:

1. Both Left and Right Administrators log on.
2. Click the **Secure State**.

   Once the state is Secure, the lock image is removed and the Update Software option is enabled.

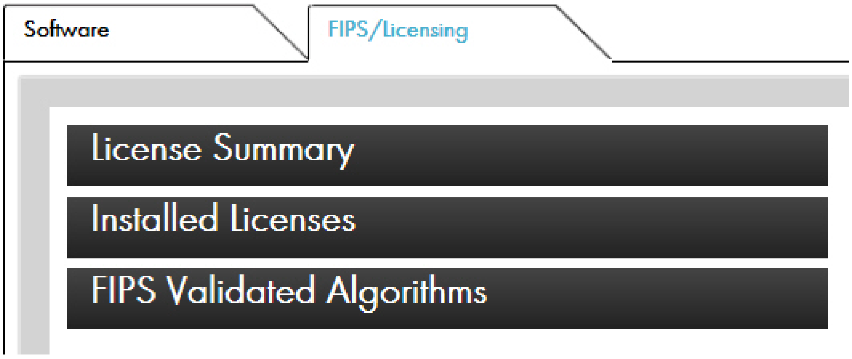


3. Click **Update Software**.



⚠ Software updates can take several minutes.

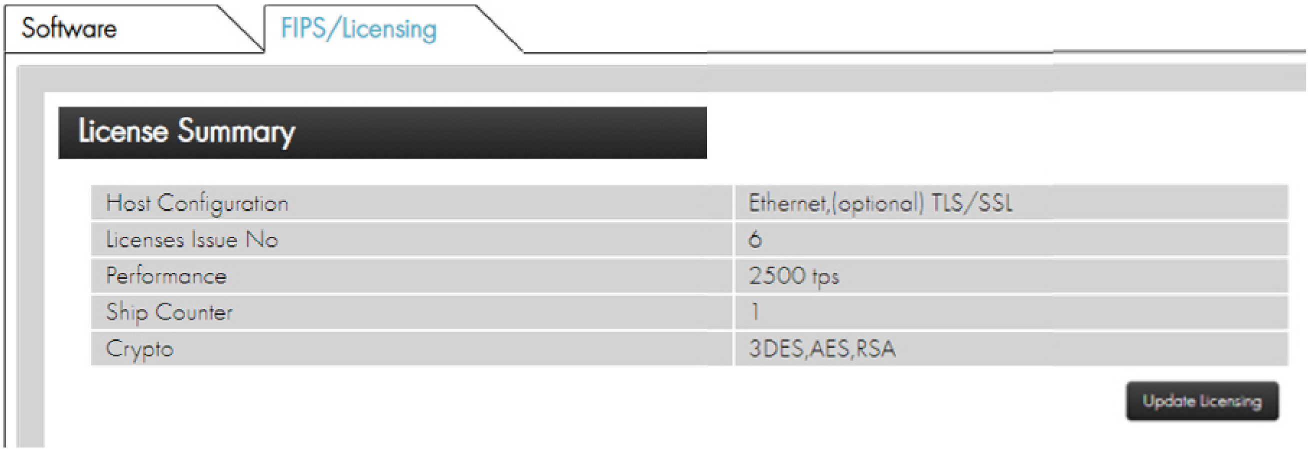
8.7.7 FIPS/Licensing



The FIPS/Licensing tab has three tabs.

8.7.7.1 License Summary - how to update Licensing

This tab displays data about the connected HSM license information including the performance number, the crypto algorithms licensed in the box, and the number of licensed LMKs.



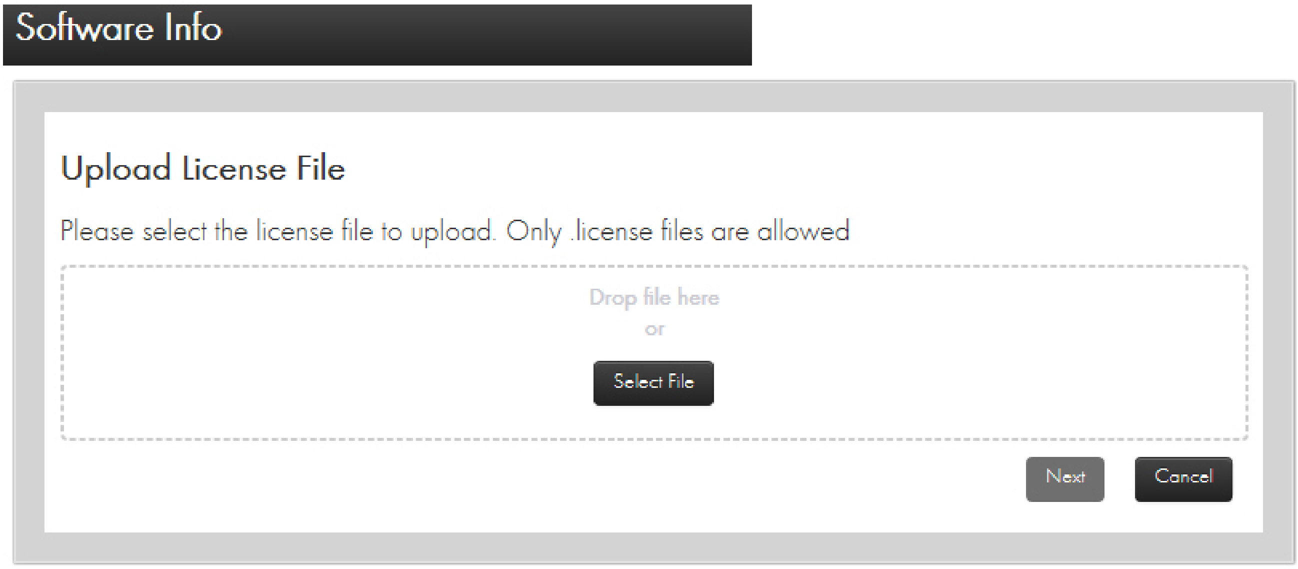
License Summary

Host Configuration	Ethernet,(optional) TLS/SSL
Licenses Issue No	6
Performance	2500 tps
Ship Counter	1
Crypto	3DES,AES,RSA

To update the license:

1. Click **Update License**.

   Note: This can be performed from the **offline or secure** state.



Upload License File

Please select the license file to upload. Only .license files are allowed

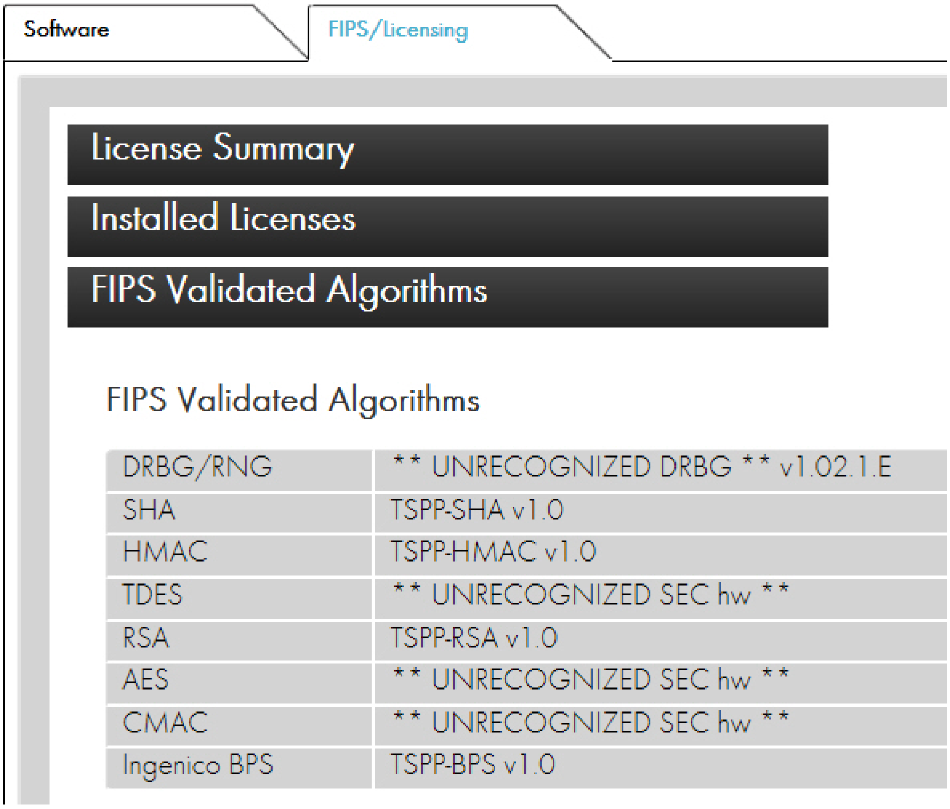
2. Select or drag and drop the file.
3. Click **Next**.
4. Continue as prompted.

8.7.7.2 Installed Licenses

This tab provides a list of all licenses currently installed on the HSM.

8.7.7.3 FIPS Validated Algorithms

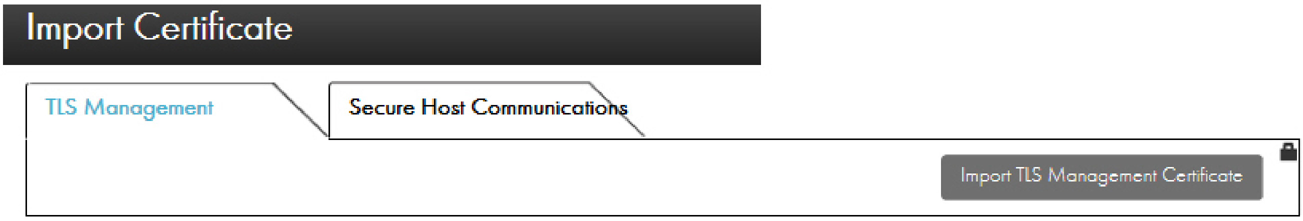
This tab lists all of the currently available FIPS Validated Algorithms.



FIPS Validated Algorithms

DRBG/RNG	** UNRECOGNIZED DRBG ** v1.02.1.E
SHA	TSPP-SHA v1.0
HMAC	TSPP-HMAC v1.0
TDES	** UNRECOGNIZED SEC hw **
RSA	TSPP-RSA v1.0
AES	** UNRECOGNIZED SEC hw **
CMAC	** UNRECOGNIZED SEC hw **
Ingenico BPS	TSPP-BPS v1.0

8.7.8 Import Certificate



From this tab, when in the secure state, you can load a TLS certificate into the payShield.

8.7.8.1 General Information

payShield 10K supports the use of TLS to secure traffic between Host applications and the HSM. TLS v1.2 is the preferred protocol.

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.

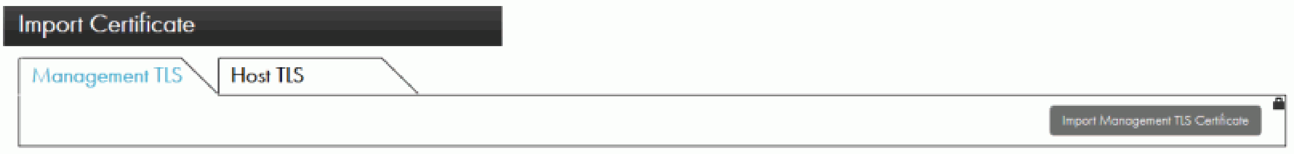
The following prerequisites apply to both TLS Management Certificates and Secure Host Communication Certificates:

1. The system time has to be set to 24 hour UTC format
2. A CSR needs to have been signed by an external CA to obtain the certificate to import
3. No more than 64 certificates can be imported onto the HSM
4. The maximum length (depth) for the Chain of Trust is 6

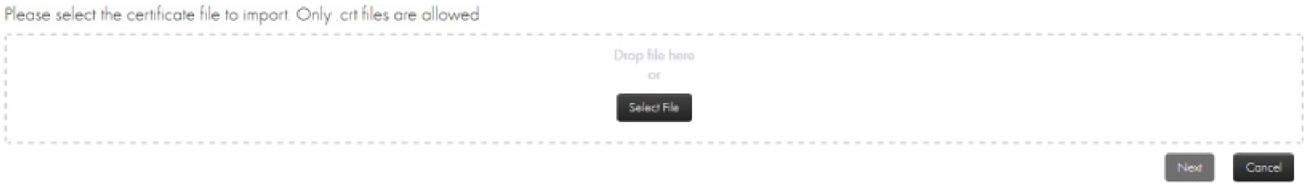
8.7.8.2 TLS Management

Follow the steps below to install a certificate for securing payShield Manager connections.

1. Both Left and Right Administrators log on.
2. Click the **Secure State**.
3. Click the **TLS Management** tab.
4. Click **Import TLS Management Certificate**.



5. Select or drag and drop the file.

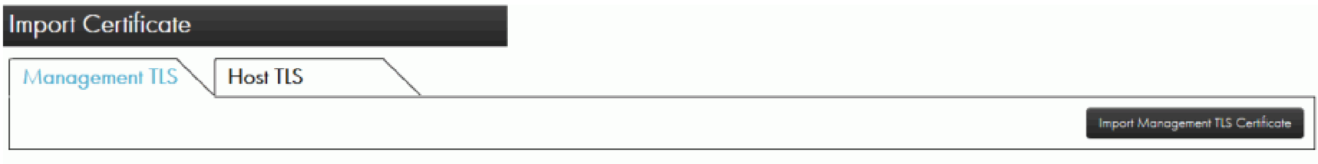

Please select the certificate file to import. Only .crt files are allowed

6. Click **Next**.
7. Continue as prompted.

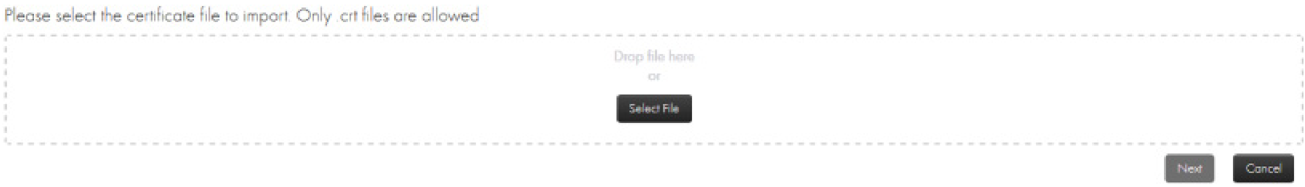
8.7.8.3 Secure Host Communications

Follow the steps below to install a certificate for securing Host connections.

1. Both Left and Right Administrators log on.
2. Click the **Secure State**.
3. Click the **TLS Management** tab.



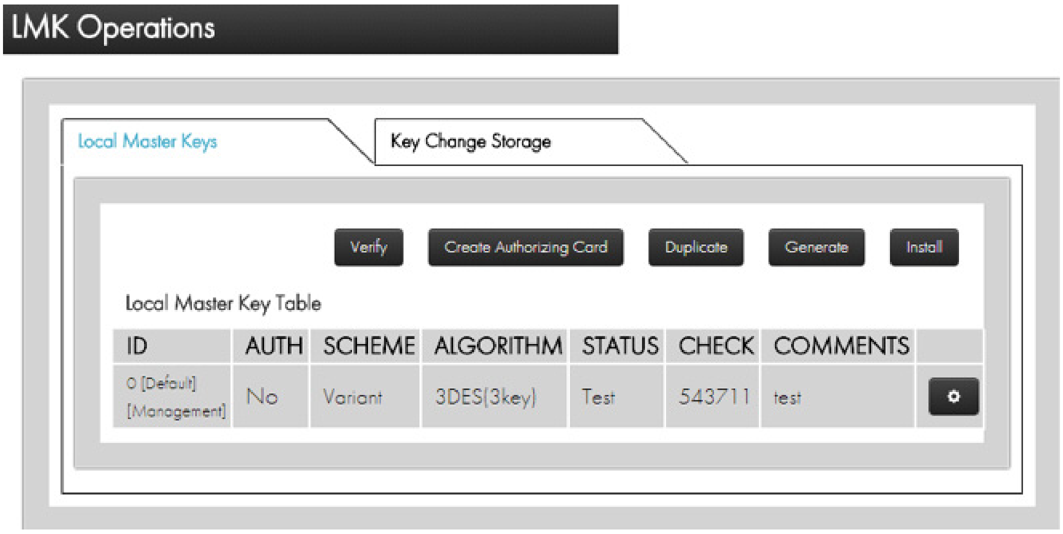
4. Select or drag and drop the file.


Please select the certificate file to import. Only .crt files are allowed

5. Click **Next**.
6. Continue as prompted.

8.8 Operational

The Operational section handles all functions relating to Local Master Keys.



Local Master Key Table

ID	AUTH	SCHEME	ALGORITHM	STATUS	CHECK	COMMENTS	
0 [Default] [Management]	No	Variant	3DES(3key)	Test	543711	test	⚙

8.8.1 Local Master Keys

Note: Each LMK has its own security setting.

LMKs are used to encrypt operational keys used for encryption, MACing, digital signing, etc. LMKs are secret, internal to the HSM, and do not exist outside of the HSM except as components or shares held in Smart Cards. Each HSM can have a unique LMK, or an organization can install the same LMKs on multiple HSMs within a logical system.

LMKs provide separation between different types of keys to ensure that keys can be used only for their intended purpose. The payShield 10K supports two types of LMK, both of which provide key separation:

- **Variant LMKs**. These are double- or triple-length Triple-DES keys and provide key separation by encrypting different types of key with different variants of the LMK. Double-length Variant LMKs have been in use for many years, and are the most widely used type of LMK. Triple-length Variant LMKs were introduced for later versions of the payShield.
- **Key Block LMKs**. These are either triple-length Triple-DES keys, or 256-bit AES keys, and key separation is provided by parameters in the key block which govern characteristics such as usage and exportability of the protected key.

  Key Block LMKs are newer technology than Variant LMKs and so are still less widely used, but provide security benefits.

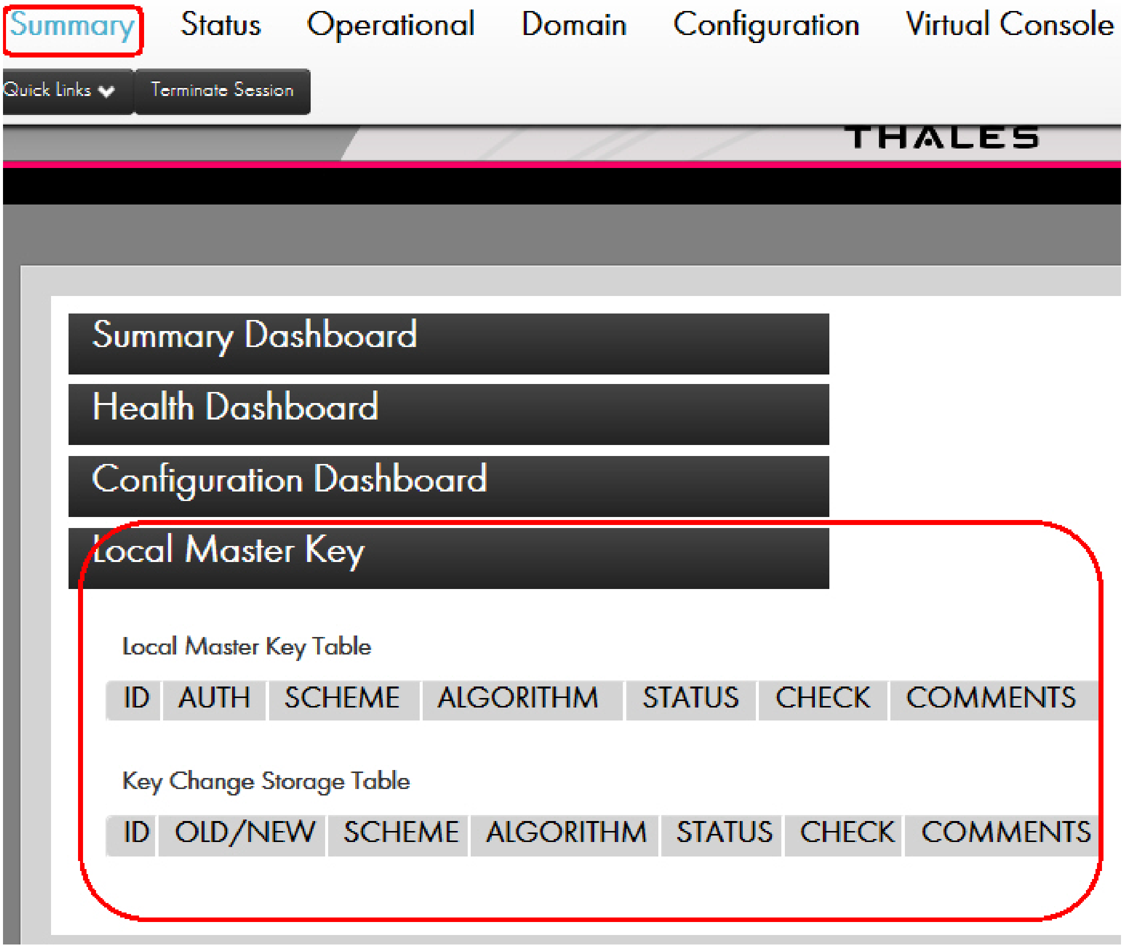
This tab provides a table that shows and allows the management of all loaded LMKs stored in the tamper-proof area of memory in the HSM.

The LMK holders become what are called the “**trusted officers**” because they hold components or shares of the Master Key that encrypts all other keys as well as two of the (up to 9 possible component holders). They also become “**authorizing officers**” (not to be confused with the administrators) and can authorize key management functions such as generating, importing or exporting keys. They can also authorize changes to configuration settings and other sensitive functions.

8.8.1.1 Generate LMK - create trusted officer

Prerequisite: Your Smart Card has already been commissioned, i.e., it already has the Security Domain stored on it.

To determine your status, navigate to **Summary > Local Master Key**. In the example below, you see that there are no LMKs listed.



Local Master Key Table

ID	AUTH	SCHEME	ALGORITHM	STATUS	CHECK	COMMENTS

Key Change Storage Table

ID	OLD/NEW	SCHEME	ALGORITHM	STATUS	CHECK	COMMENTS

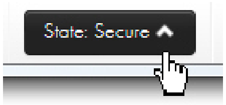
By design, when you created your Left and Right LMK cards, no data is stored on the cards. The Left and Right LMK cards are used for things that do store data on cards.

For example, they are used for creating:

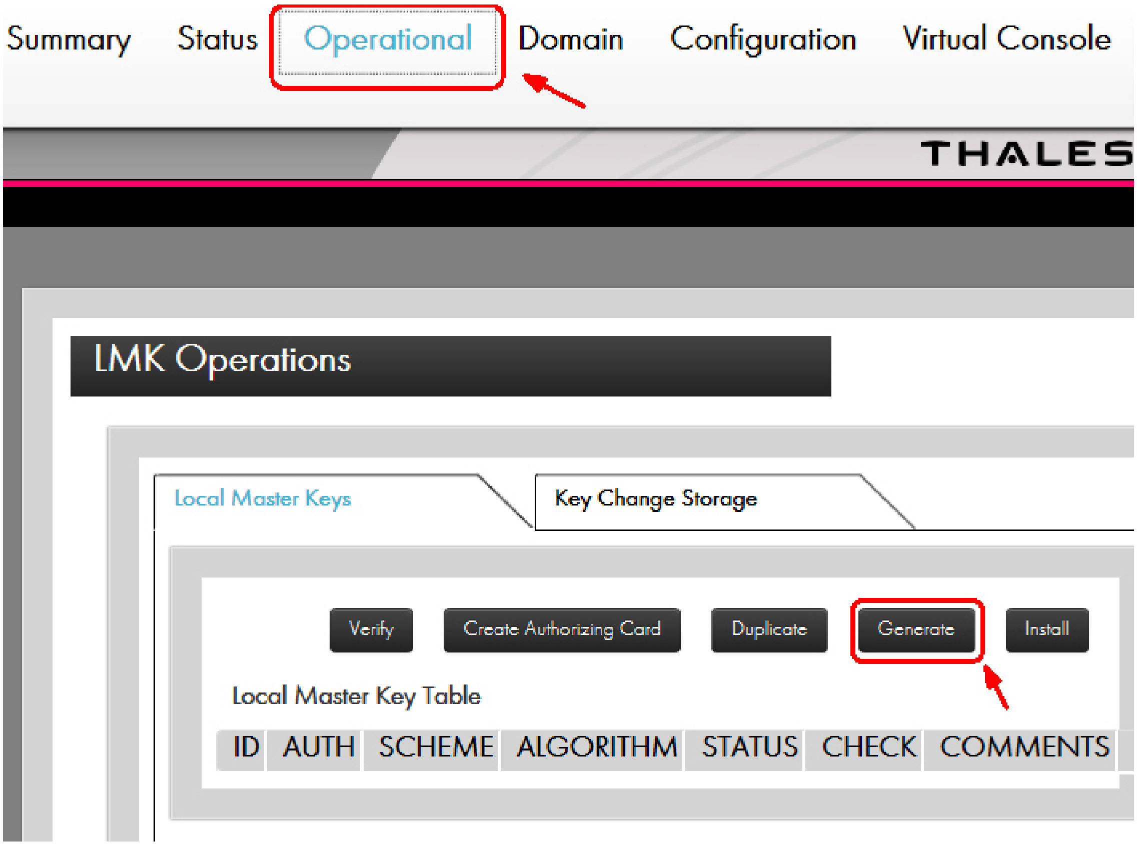
- CTA shares
- LMK shares
- Settings

To add “authorizing officer” functionality to your Left and Right LMK, follow the steps below.

1. Verify that you are in the **Secure** state.

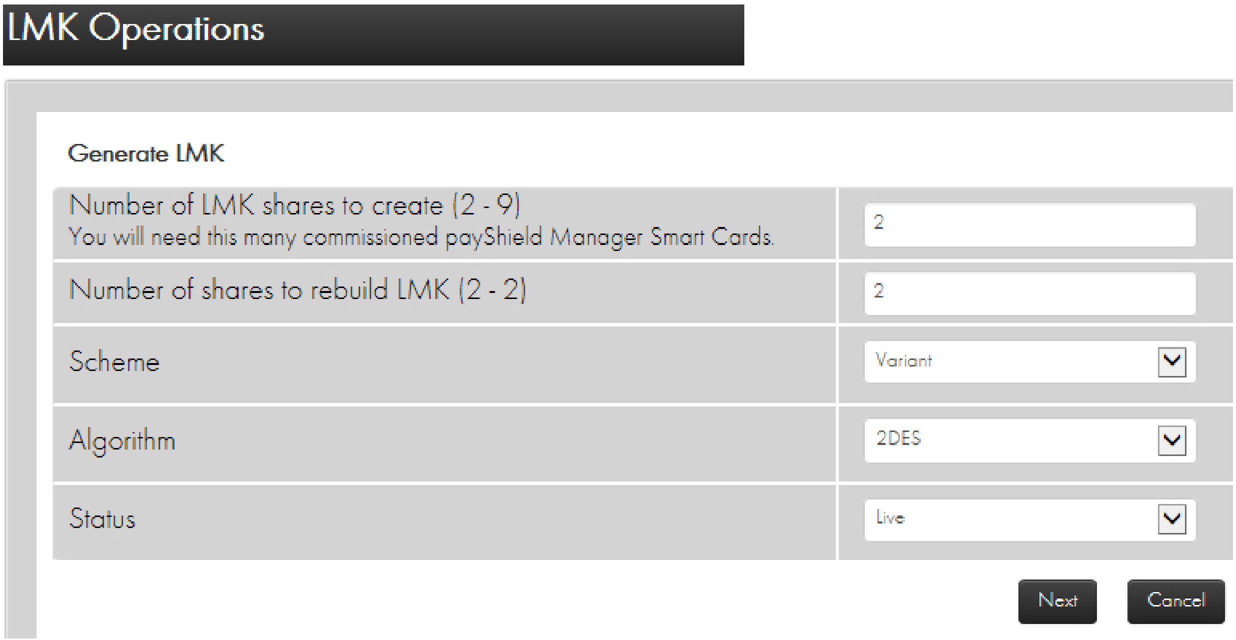


2. Navigate to the **Operational** tab.



3. Click **Generate**.

   The Generate LMK screen displays showing the default settings.

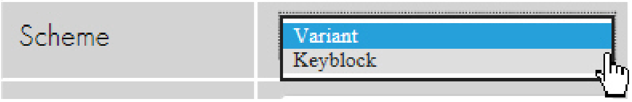


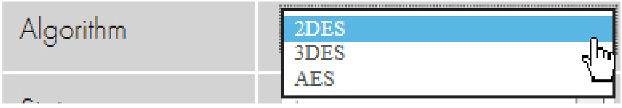
LMK Operations

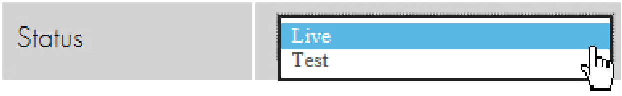
Generate LMK

Number of LMK shares to create (2 - 9) You will need this many commissioned payShield Manager Smart Cards.	2
Number of shares to rebuild LMK (2 - 2)	2
Scheme	Variant
Algorithm	2DES
Status	Live

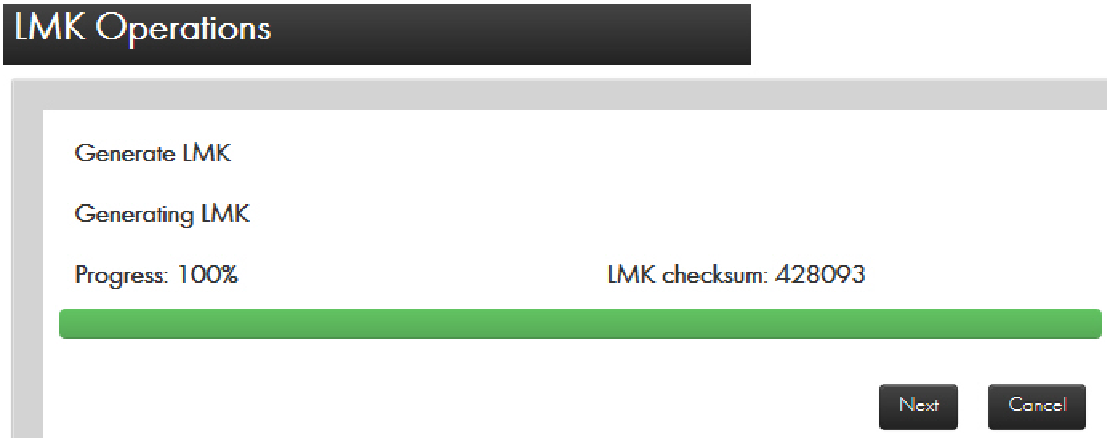
4. Enter your preferred settings from the drop downs:







5. Click **Next.**



LMK Operations

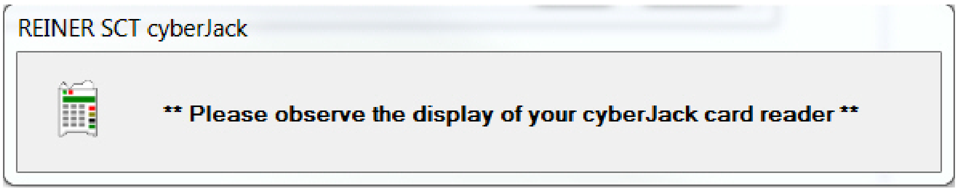
Generate LMK

Generating LMK

Progress: 100%

LMK checksum: 428093

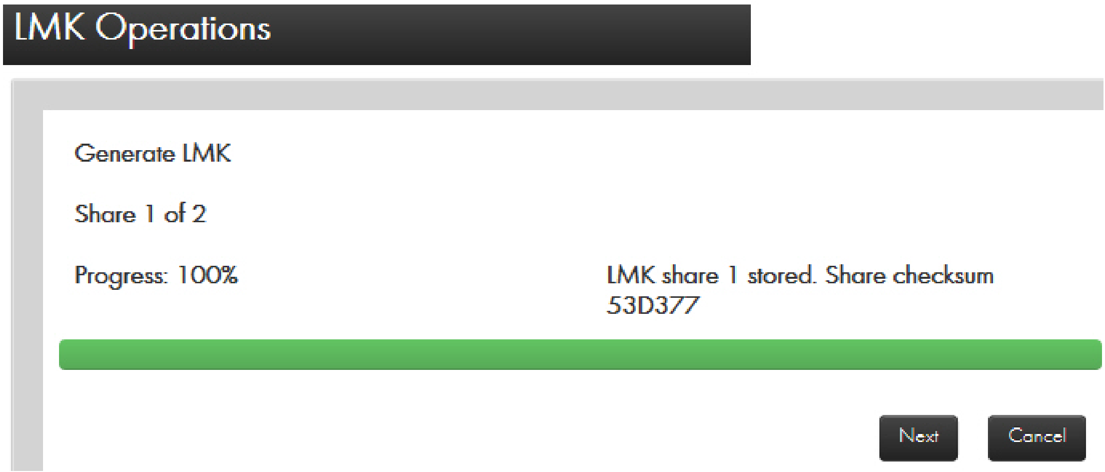
6. Click **Next**.



REINER SCT cyberJack

** Please observe the display of your cyberJack card reader **

7. Insert your Smart Card into the card reader, enter the PIN, and press **OK**.



LMK Operations

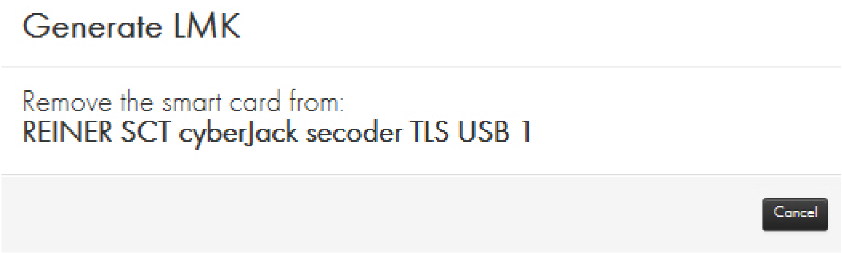
Generate LMK

Share 1 of 2

Progress: 100%

LMK share 1 stored. Share checksum 53D377

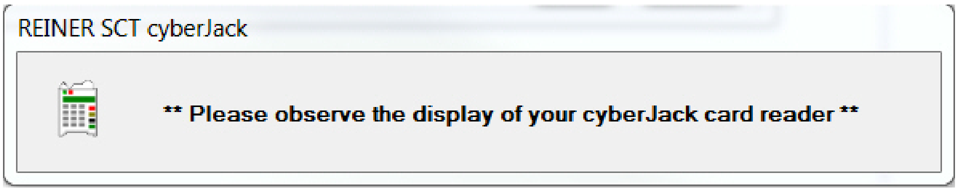
8. Click **Next**.



Generate LMK

Remove the smart card from:
REINER SCT cyberJack secoder TLS USB 1

9. Remove your Smart Card from the card reader.

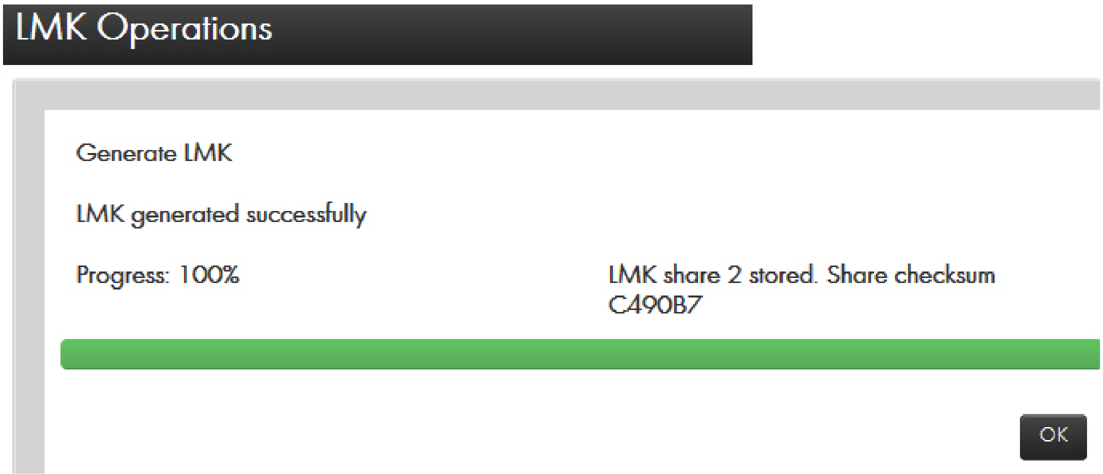


REINER SCT cyberJack

** Please observe the display of your cyberJack card reader **

10. Insert the second Smart Card into the card reader.

11. Enter your PIN and press **OK**.



LMK Operations

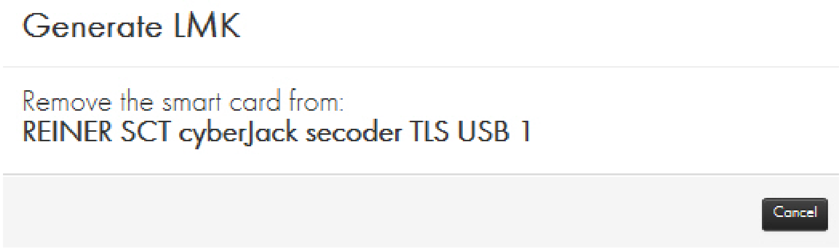
Generate LMK

LMK generated successfully

Progress: 100%

LMK share 2 stored. Share checksum C490B7

12. Click **OK**.

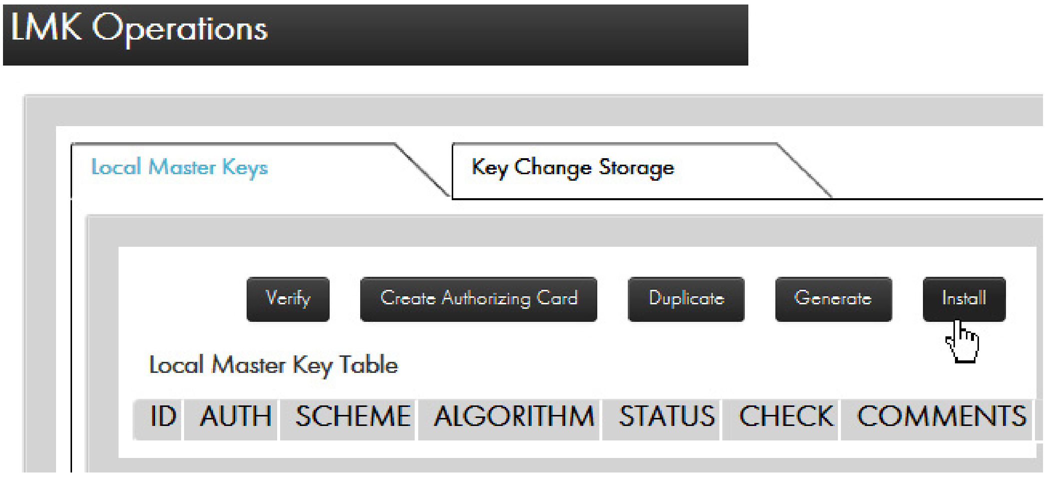


Generate LMK

Remove the smart card from:
REINER SCT cyberJack secoder TLS USB 1

13. Remove the Smart Card from the card reader.

14. Click **Install**.

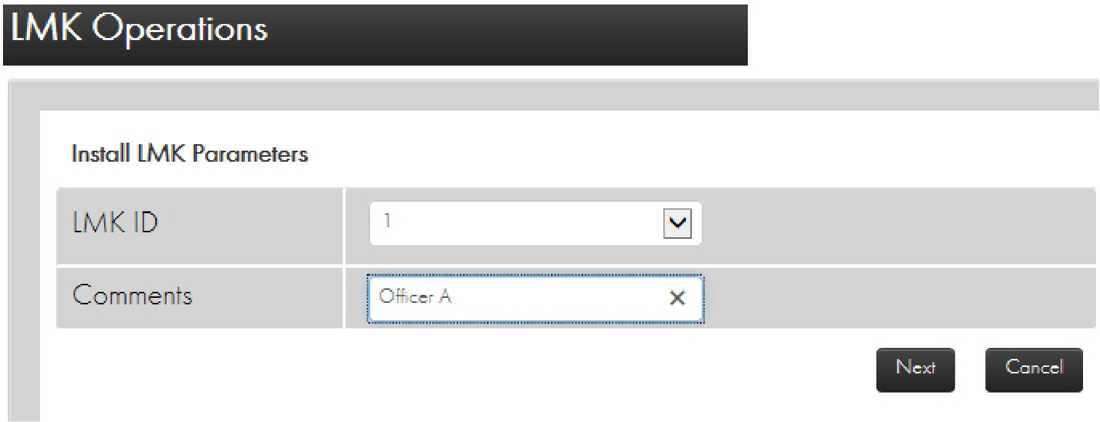


LMK Operations

Local Master Key Table

ID	AUTH	SCHEME	ALGORITHM	STATUS	CHECK	COMMENTS

15. Enter the LMK Parameters.

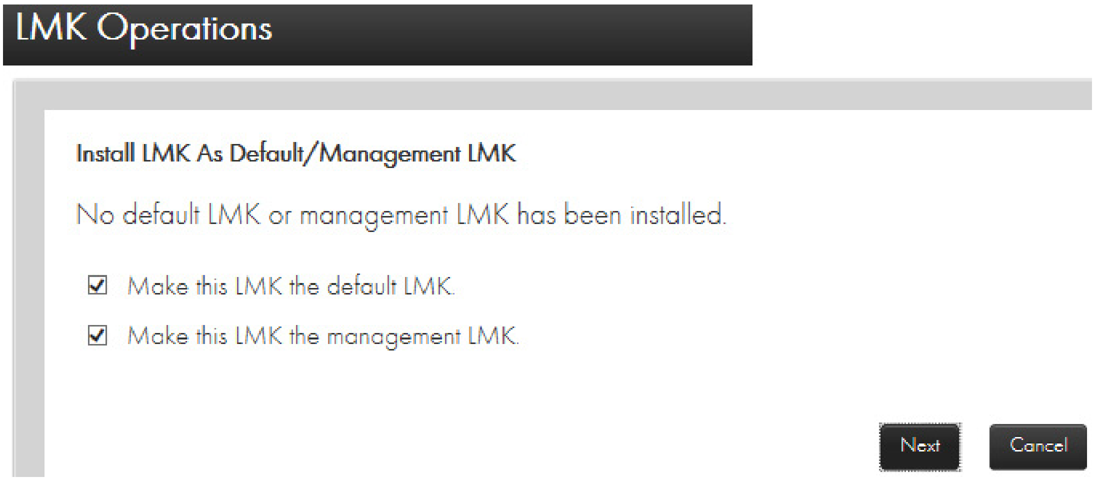


LMK Operations

Install LMK Parameters

LMK ID	1
Comments	Officer A

16. Click **Next**.



LMK Operations

Install LMK As Default/Management LMK

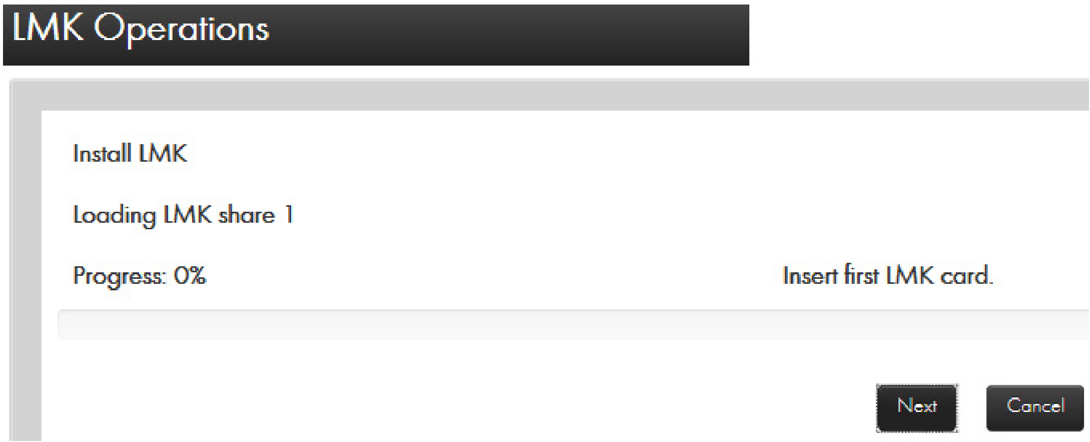
No default LMK or management LMK has been installed.

☑ Make this LMK the default LMK.

☑ Make this LMK the management LMK.

17. Click your preferences or use the default settings.

18. Click **Next**.



LMK Operations

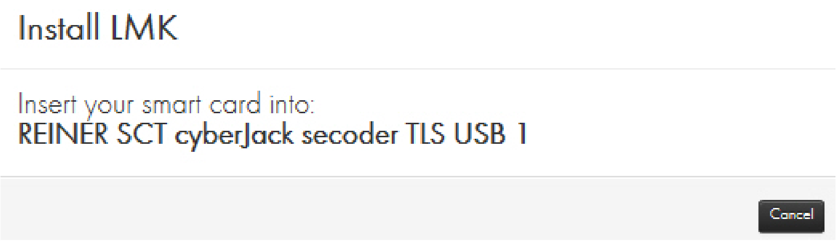
Install LMK

Loading LMK share 1

Progress: 0%

Insert first LMK card.

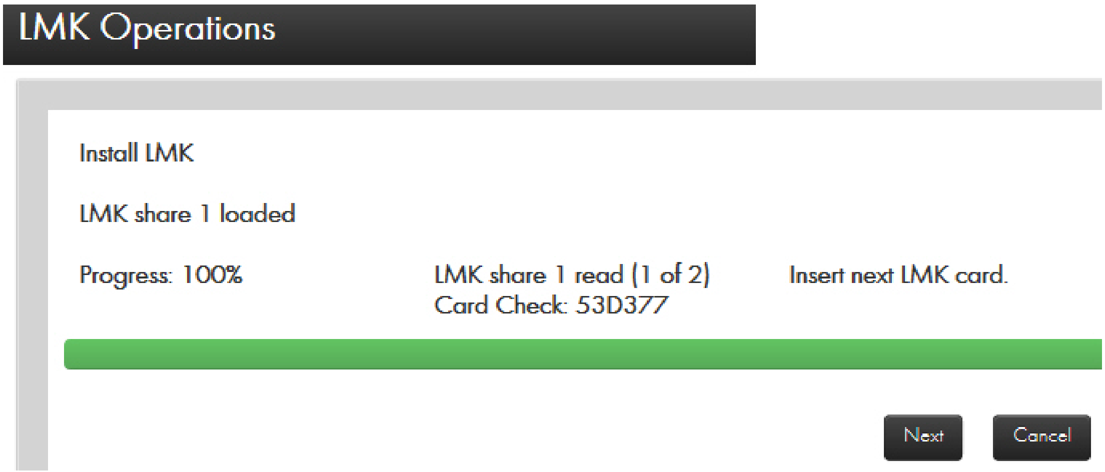
19. Follow the prompt and insert the first LMK card.



Install LMK

Insert your smart card into:
REINER SCT cyberJack secoder TLS USB 1

20. Enter your PIN and press **OK**.



LMK Operations

Install LMK

LMK share 1 loaded

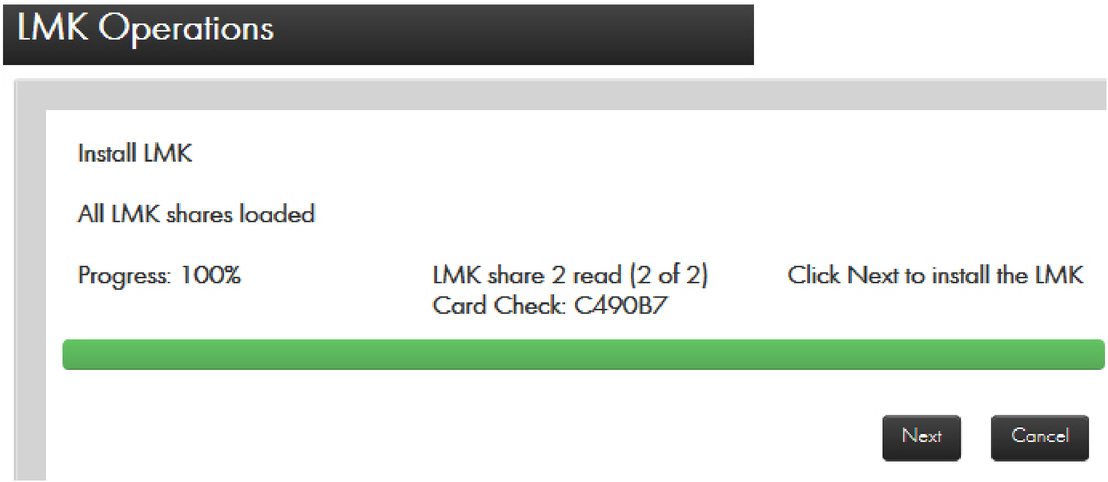
Progress: 100%

LMK share 1 read (1 of 2)
Card Check: 53D377

Insert next LMK card.

21. Insert the next LMK card, enter your PIN and press **OK**.

22. Click **Next** to install the LMK.



LMK Operations

Install LMK

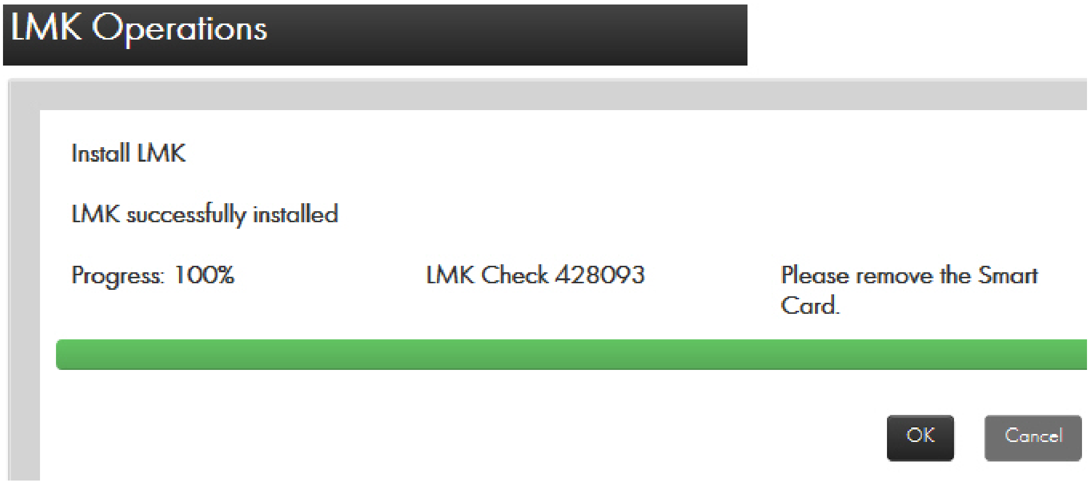
All LMK shares loaded

Progress: 100%

LMK share 2 read (2 of 2)
Card Check: C490B7

Click Next to install the LMK

23. Remove the Smart Card from the reader



LMK Operations

Install LMK

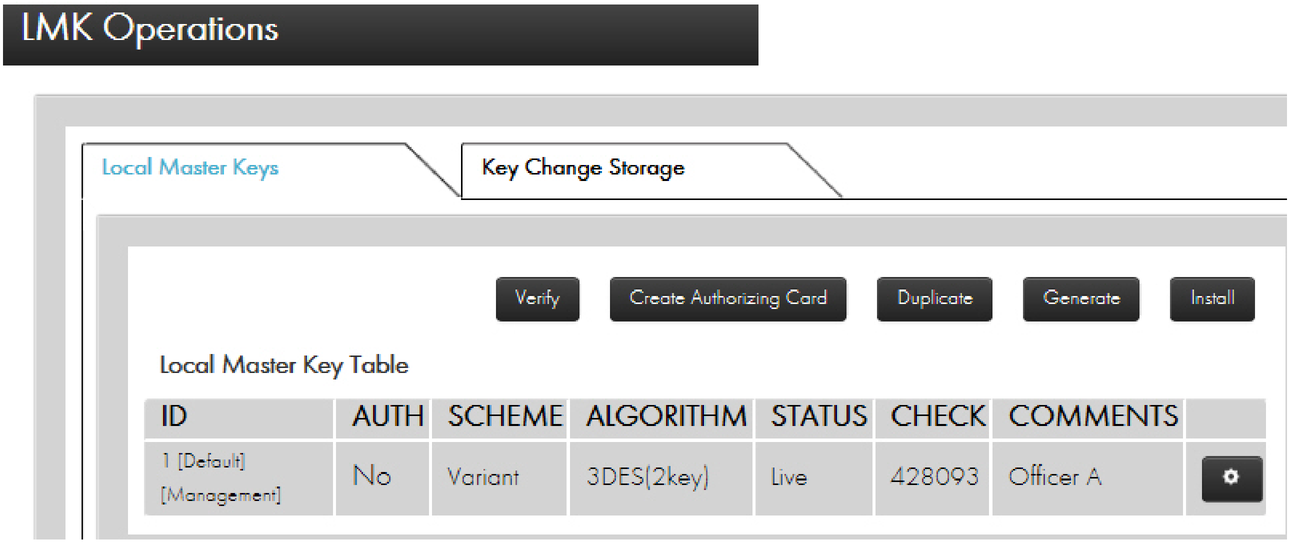
LMK successfully installed

Progress: 100%

LMK Check 428093

Please remove the Smart Card.

24. Click **OK**.



Local Master Key Table

ID	AUTH	SCHEME	ALGORITHM	STATUS	CHECK	COMMENTS	
1 [Default] [Management]	No	Variant	3DES(2key)	Live	428093	Officer A	⚙

The Local Master Key Table populates.

8.8.1.2 Verify an LMK Card

1. Click **Verify**.
2. Insert one of the cards of the card set containing the RLMK you wish to verify.
3. Enter the PIN.
4. Select **OK**.

   The HSM will read the LMK data from the card, and when completed will display a table showing the following:

   - LMK Share
   - Quorum Size
   - Scheme
   - Algorithm
   - Status
   - Checksum

8.8.1.3 Create an Authorizing Card

When in Offline or Secure state, you can create an Authorizing Card (used to enter Authorized state) for a RLMK card.

Prerequisite: The payShield 10K is in the Offline or Secure state.

1. Click **Create Authorizing Card**.

   A system prompt displays.

2. Insert the RLMK card that you wish to create an Authorizing Card for.

3. Enter the card’s PIN.

   The system reads the RLMK card and prompting displays.

4. Insert **a prior commissioned card** to use as an Authorizing Card.

5. Enter the Authorizing card’s PIN.

6. Remove the Authorizing Card upon completion

7. Click **OK**.

8.8.1.4 Duplicate an LMK Card

Prerequisite: The payShield 10K is in the Secure state.

1. Click **Duplicate Card**.

   A system prompt displays.

2. Insert the RLMK card that you wish to duplicate.

3. Enter the card’s PIN.

   The system reads the RLMK card.

4. Click **OK**.

   A system prompt displays.

5. Remove the RLMK card.

6. Insert **a prior commissioned card**.

7. Enter the card’s PIN.

   The system duplicates the card

8. Remove the new card.

9. Click **OK**.

8.8.1.5 Generate an LMK

You can create a new LMK to be stored on RLMK cards.

Prerequisite: The payShield 10K is in the Secure state.

1. Click **Generate**.

   A system prompt displays.

2. Follow the prompts and enter the following information about the new LMK:
   - Number of LMK shares (Default: 2)
   - Number of shares to rebuild (Default: 2)
   - Key scheme (Variant or Key Block)
   - Algorithm
   - Status (Live or Test)
3. Click **Next**.

   A LMK is generated and a checksum displayed.
4. Click **Next**.

   A system prompt displays.
5. Insert **a prior commissioned card** to write the LMK share to.
6. Enter the card's PIN.

   When the HSM is finished writing to the card, it displays a checksum for that LMK share.
7. Click **Next**.
8. Repeat this process until all shares have been written.
9. When complete, click **OK** to return to the main LMK screen.

8.8.1.6 Install an LMK from RLMK Card Set

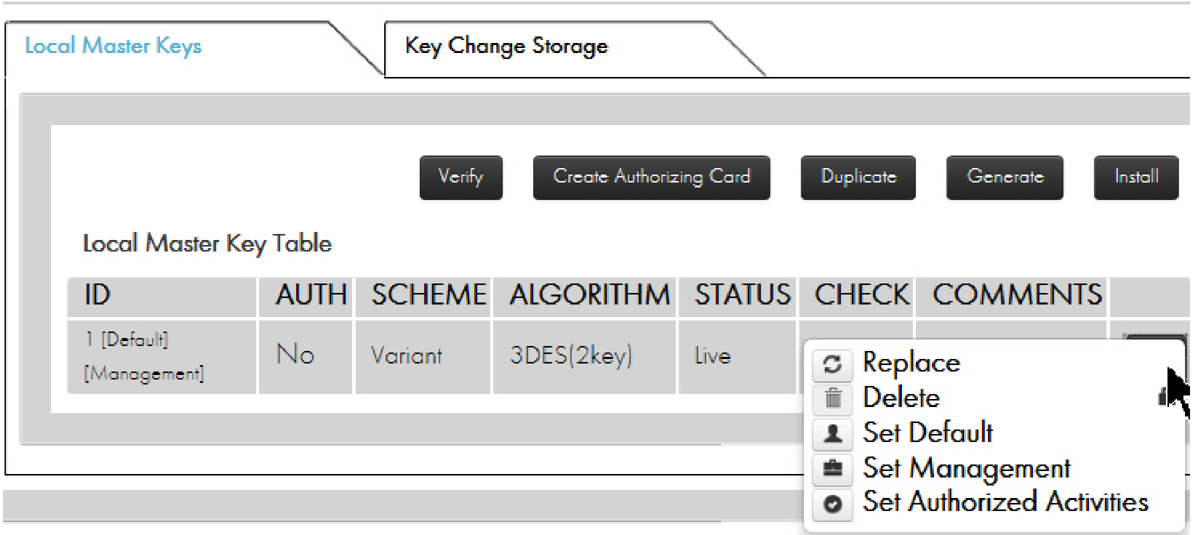
1. Click **Install**.
2. Specify the ID for the new LMK as well as a brief comment describing the LMK.
3. Click **Next**.
4. Insert the RLMK card containing the first LMK share for the new LMK.
5. Enter the card's PIN.
6. Continue inserting LMK share cards when prompted until the entire LMK has been read from the card set.
7. When all cards have been read, click **Next** to install the LMK.
8. Once installed, remove the last card or click **OK** to return to the main LMK screen.

Note: The first 2 RLMK cards will contain the authorizing password used to enter authorized state.

8.8.1.7 Delete an Installed LMK

In Secure state and authorized under the LMK you wish to delete, you may delete an LMK that has already been installed.

1. Click the ⚙ button next to the LMK that you wish to remove.
2. Click **Delete**.



Local Master Key Table

ID	AUTH	SCHEME	ALGORITHM	STATUS	CHECK	COMMENTS
1 [Default] [Management]	No	Variant	3DES(2key)	Live		

3. When prompted, click **OK** to confirm the deletion.

Note: You cannot delete the current Default LMK without first assigning a new Default LMK.

8.8.1.8 Replace an installed LMK

Prerequisite: The payShield 10K is in the Secure state.

1. Click the ⚙ button next to the LMK you wish to replace.
2. Click **Replace**.
3. Specify the LMK ID for the new LMK as well as a brief comment describing the LMK.
4. Click **Next**.
5. Insert the RLMK card containing the first LMK share for the new LMK.
6. Enter the card’s PIN.
7. Continue inserting LMK share cards when prompted until the entire LMK has been read from the card set.
8. When all cards have been read, click **Next** to install the LMK.
9. Once installed, remove the last card or click **OK** to return to the main LMK screen.

8.8.1.9 Set the Default LMK

The Default LMK is a specified LMK (when using Multiple LMKs) to provide a backward compatible mode of use for the HSM.

Prerequisite: The payShield 10K is in the Secure state.

1. Click the ⚙ button next to the LMK that you want to make the Default LMK.
2. Click **Set Default**.
3. When prompted to confirm, click **OK**.

8.8.1.10 Set the Management LMK

The Management LMK is a specified LMK (when using Multiple LMKs) that is used by the HSM for purposes that are not linked to a particular LMK; for example, authenticating audit trail records.

Prerequisite: The payShield 10K is in the Secure state.

1. Click the ⚙ button next to the LMK that you want to make the Management LMK.
2. Click **Set Management**.
3. When prompted to confirm, click **OK**.

8.8.1.11 Enter Authorized State

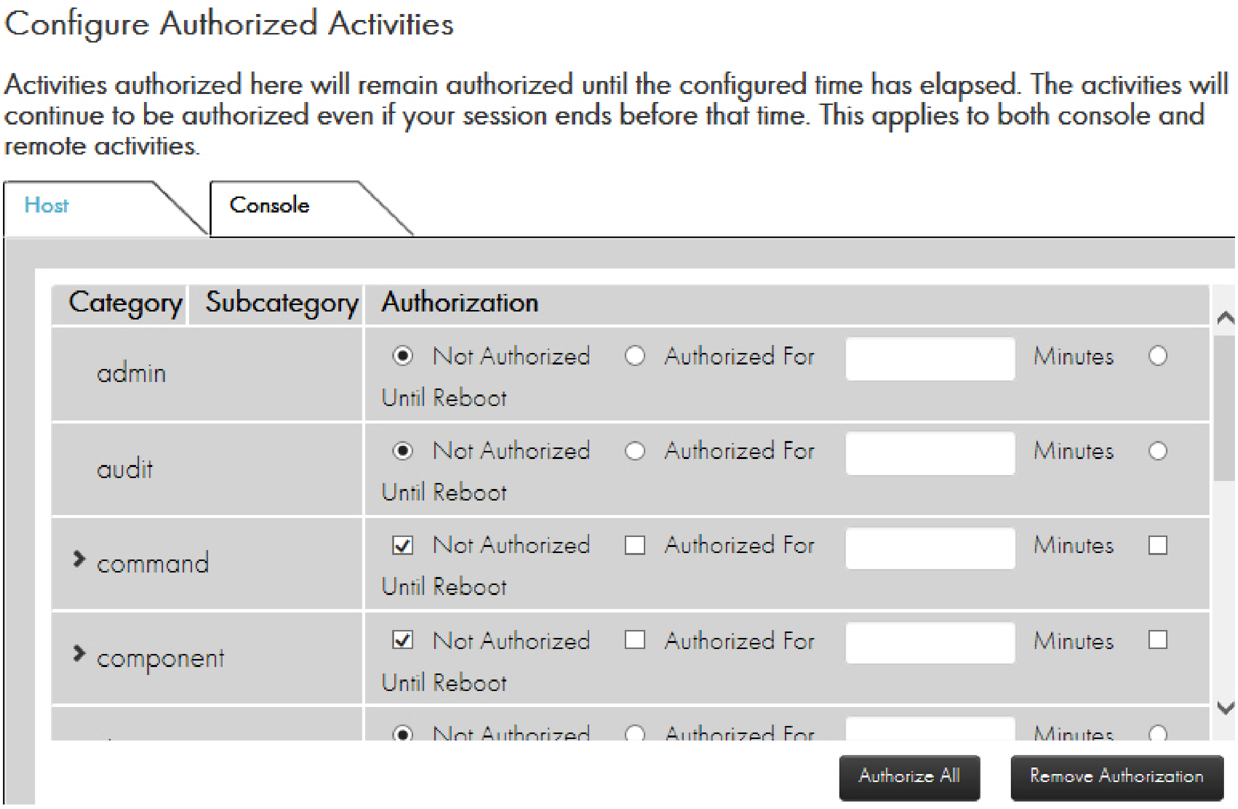
Authorized State is a mode of operation of the HSM that permits one or more specified sensitive functions to be performed. It requires two Authorizing Officers using their Smart Cards and PINs to confirm the activity.

In any state, you may enter Authorized state by clicking the ⚙ button next to the LMK you wish to authorize and select **Set Authorized Activities**.

Depending on the authorization mode selected (single or multi-authorization) from the initial security settings, you will either begin to enter the authorized state (in single authorization mode) or be presented with a menu of authorized activities (in multi-authorization mode).

Note:

- Remote authorization will not work if the Initial Security setting “Use default card issuer password” is checked. The payShield Manager only allows Authorization using Smart Cards.
- Authorized activities may continue, as specified in the authorization, even after the payShield Manager session has terminated. For example, suppose the Console PIN activity has been authorized for 300 minutes using the payShield Manager. The activity will remain authorized for 300 minutes regardless of the state of the payShield Manager.



Configure Authorized Activities

Activities authorized here will remain authorized until the configured time has elapsed. The activities will continue to be authorized even if your session ends before that time. This applies to both console and remote activities.

Category	Subcategory	Authorization
admin		● Not Authorized ○ Authorized For ▭ Minutes ○ Until Reboot
audit		● Not Authorized ○ Authorized For ▭ Minutes ○ Until Reboot
› command		☑ Not Authorized □ Authorized For ▭ Minutes □ Until Reboot
› component		☑ Not Authorized □ Authorized For ▭ Minutes □ Until Reboot
		● Not Authorized ○ Authorized For ▭ Minutes ○

8.8.1.12 Single Authorization Mode

You will be prompted to enter a card containing the first of the LMK's authorizing PIN. Insert the card and enter the PIN. You will then be prompted to enter a card containing the second of the LMK's authorizing PIN. Insert the card and enter the PIN. Upon success, the activities will be authorized following the rules for single authorization mode.

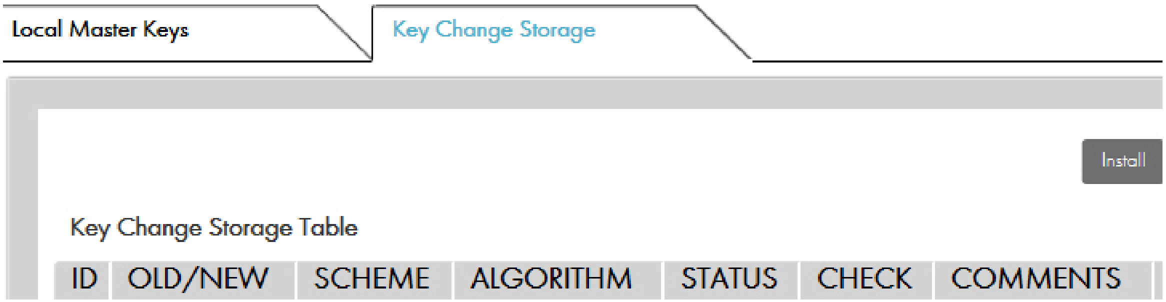
8.8.1.13 Multiple Authorization Mode

You will be presented with two tabs displaying the Host and Console commands, which you can authorize. Place check marks next to the commands that you want to authorize. Additionally, you can specify that the authorization for each command should persist or last for a specified amount of time. For convenience, at the bottom of each tab there are two buttons to allow for adding or removing authorization for all commands. When you are finished Clicking commands, click "Next".

You will be prompted to enter a card containing the first of the LMK's authorizing PIN or passwords. Insert the card and enter the PIN. You will then be prompted to enter a card containing the second of the LMK's authorizing passwords. Insert the card and enter the PIN. Upon success, the activities will be authorized following the rules for single authorization mode.

8.8.1.14 Key Change Storage

This tab provides a table that shows and allows the management of the Key Change Storage table, which is a tamper-proof area of memory in the HSM that stores "old" LMK(s), used to permit translation of keys following an LMK change.



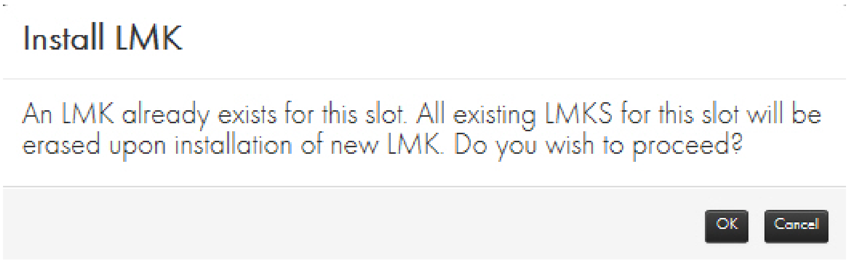
Key Change Storage Table

ID	OLD/NEW	SCHEME	ALGORITHM	STATUS	CHECK	COMMENTS

8.8.1.15 Install LMK from RLMK card set

When authorized under the given LMK and in secure state you can install an "old" LMK into the same ID for that LMK of the Key Change Storage table by clicking the "Install" button.

Note: You can install an "old" LMK in the Key Change Storage table when there is an LMK in the same ID of the LMK table. For example, if there is an LMK in ID 1, you may install an "old" LMK in ID 1 of the Key Change Storage table.



Install LMK

An LMK already exists for this slot. All existing LMKS for this slot will be erased upon installation of new LMK. Do you wish to proceed?

Specify the ID for the old LMK as well as a brief comment describing the LMK and click “Next”. Insert the RLMK card containing the first LMK share for the LMK and enter the card’s PIN. Continue inserting LMK share cards when prompted until the entire LMK has been read from the card set. When all cards have been read, click “Next” to install the LMK. Once installed, remove the last card or click “OK” to return to the main LMK screen.

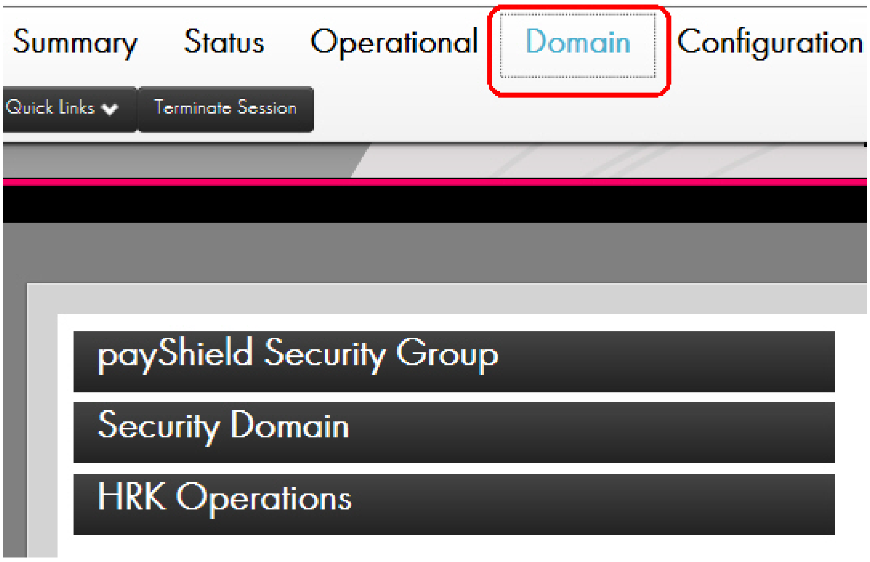
8.8.1.16 Delete an installed LMK

In secure state, you may delete an old LMK that has already been installed by clicking on the ⚙ button next to the old LMK you wish to remove and Click “Delete”. When prompted, click “OK” to confirm that you want to delete.

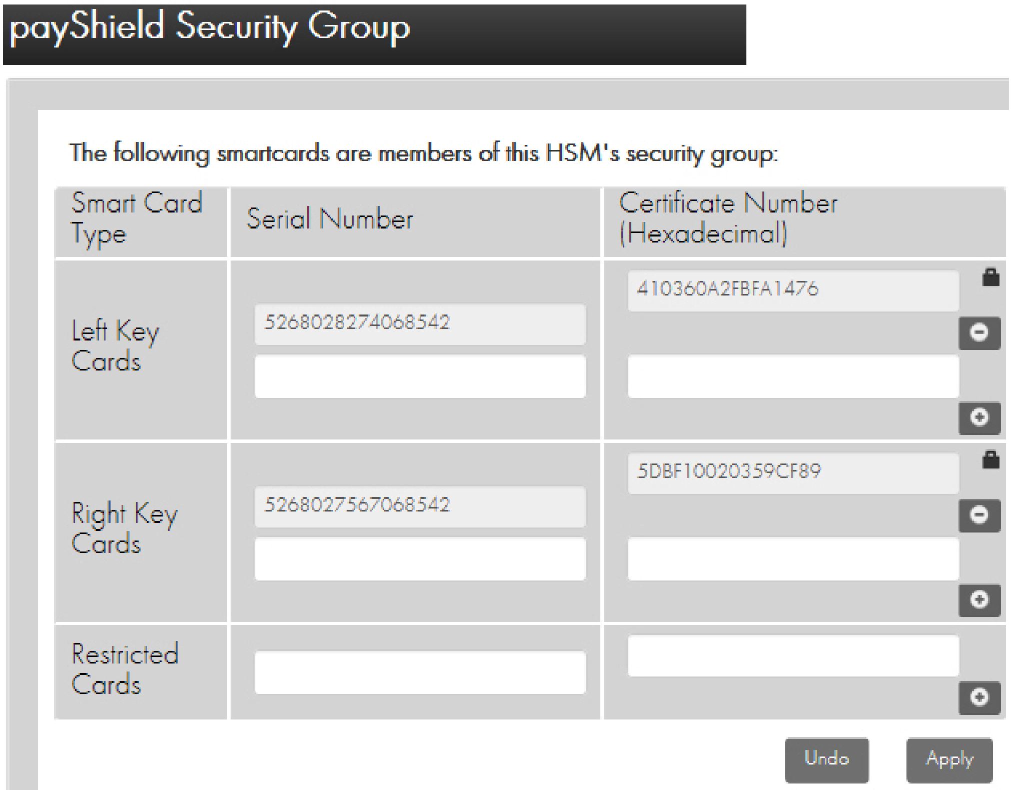
8.8.1.17 Replace an Old LMK

In secure state and authorized under the desired LMK, you may replace an installed old LMK by clicking on the ⚙ button next to the LMK you wish to replace and Click “Replace”. The ID for the old LMK is pre-set (and cannot be changed). Enter a brief comment describing the LMK and click “Next”. Insert the RLMK card containing the first LMK share for the LMK and enter the card’s PIN. Continue inserting LMK share cards when prompted until the entire LMK has been read from the card set. When all cards have been read, click “Next” to install the LMK. Once installed, remove the last card or click “OK” to return to the main LMK screen.

8.9 Domain


Summary
Status
Operational
Domain
Configuration
Quick Links
Terminate Session
payShield Security Group
Security Domain
HRK Operations

8.9.1 payShield Security Group



payShield Security Group

The following smartcards are members of this HSM's security group:

Smart Card Type	Serial Number	Certificate Number (Hexadecimal)
Left Key Cards	5268028274068542	410360A2FBFA1476
Right Key Cards	5268027567068542	5DBF10020359CF89
Restricted Cards		

In this tab, you can control which RACCs are usable as Left, Right and Restricted Key Cards. Each section provides a list of all card serial numbers that are usable as that type of card. To remove a card, click the minus icon next to the card you want to remove. Note that you cannot remove the last of either the Left or Right Key Card.

If both a Left and Right Key Card have logged into the HSM, you may add a new card (independent of the HSM’s state) by entering the Key Card’s serial number and Certificate Number in the text box for the appropriate section and click the plus icon. Select the “Apply” button after adding all the desired card serial numbers.

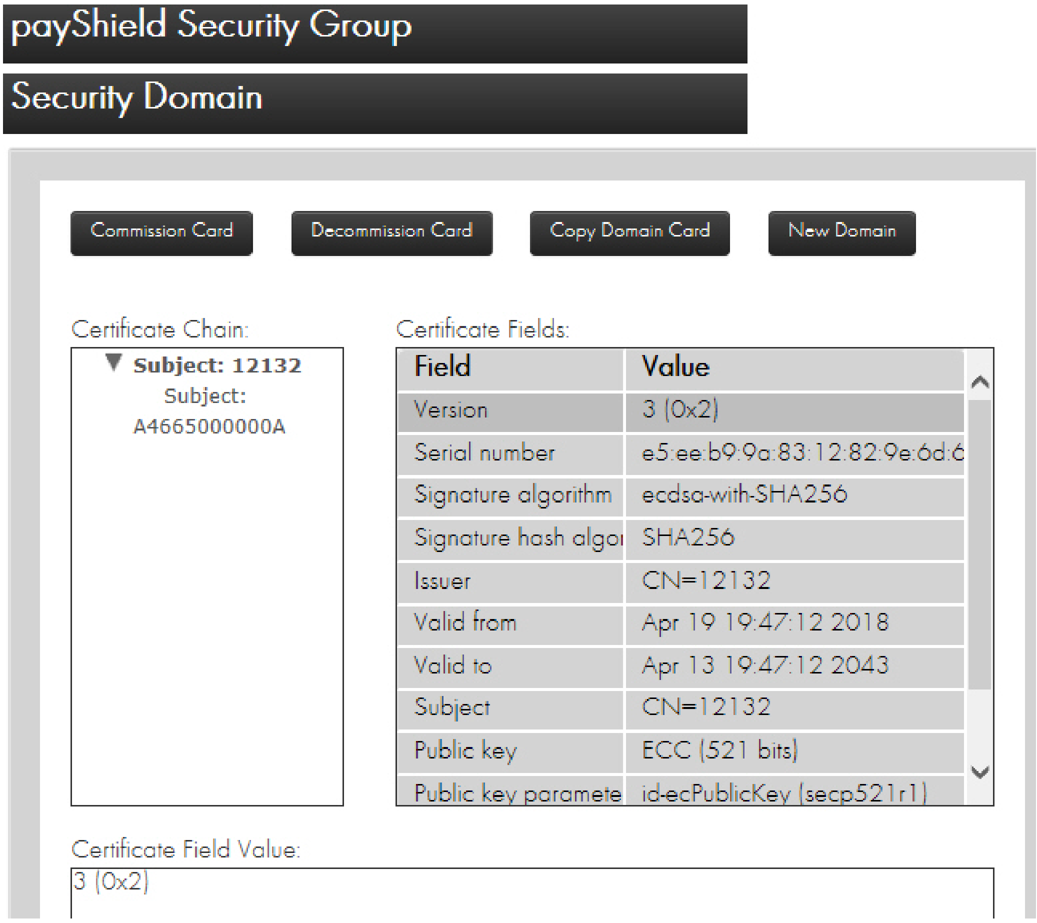
Note:

To get the Smart Card’s Certificate Number:

- Remove any Smart Card currently inserted in the Smart Card reader,
- Select the ▦ button on the bottom right of the main page,
- Click to view the Smart Card Details, and
- Insert the Smart Card you wish to add to the whitelist in the Smart Card reader.

8.9.2 Security Domain

In this tab, you controls the domain and cards. Additionally, a table is displayed showing information on the loaded certificates.



Certificate Chain:

▼ Subject: 12132
Subject:
A4665000000A

Certificate Fields:

Field	Value
Version	3 (0x2)
Serial number	e5:ee:b9:9a:83:12:82:9e:6d:6
Signature algorithm	ecdsa-with-SHA256
Signature hash algoi	SHA256
Issuer	CN=12132
Valid from	Apr 19 19:47:12 2018
Valid to	Apr 13 19:47:12 2043
Subject	CN=12132
Public key	ECC (521 bits)
Public key paramete	id-ecPublicKey (secp521r1)

Certificate Field Value:

3 (0x2)

The following sections describe the available operations.

8.9.2.1 Commission a Smart Card

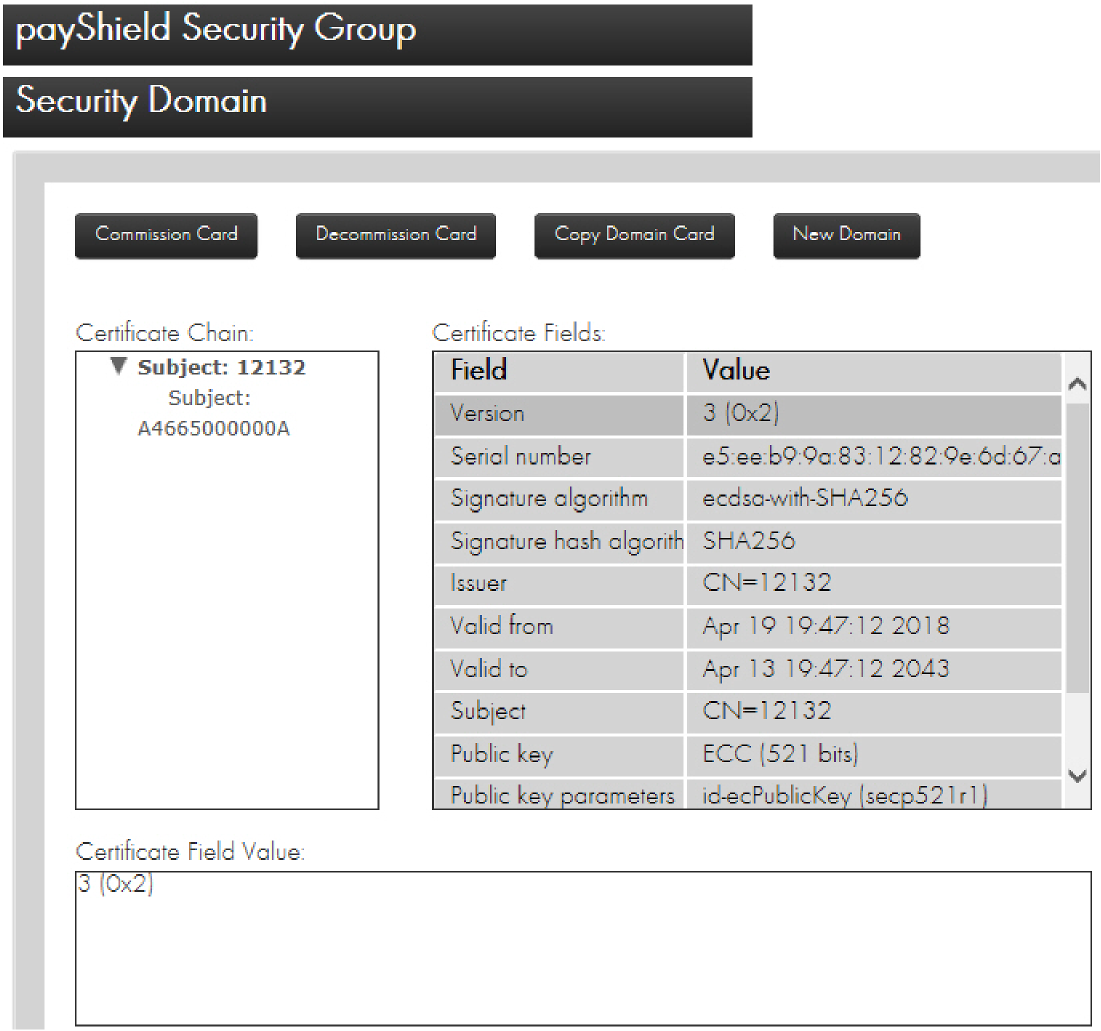
When you commission a Smart Card, you are adding it to a security domain.

Note: As described below, you may commission a card by clicking on the “Commission Card” button. Click Next to begin. When prompted, enter the first CTA card and enter the card’s PIN. Continue entering cards when prompted until the entire CTA card set has been loaded. When the entire CTA has been loaded, you will be shown a table containing information on the security domain. Click “Next” to commission your new cards. When prompted, enter the card (either a new Smart Card or a card that was previously commissioned) to commission, and enter the card’s new PIN. When the card has been commissioned, you may continue to commission additional cards by clicking “Next”.

Prerequisite:

Your logged on in the **Secure** state.

1. Navigate to: **Domain > Security Domain**



Certificate Chain:

▼ Subject: 12132
Subject: A4665000000A

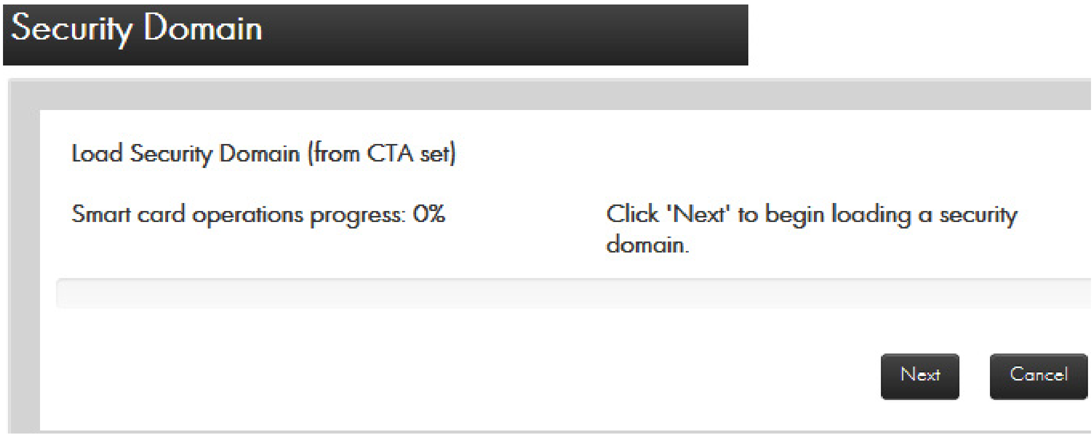
Certificate Fields:

Field	Value
Version	3 (0x2)
Serial number	e5:ee:b9:9a:83:12:82:9e:6d:67:a
Signature algorithm	ecdsa-with-SHA256
Signature hash algorith	SHA256
Issuer	CN=12132
Valid from	Apr 19 19:47:12 2018
Valid to	Apr 13 19:47:12 2043
Subject	CN=12132
Public key	ECC (521 bits)
Public key parameters	id-ecPublicKey (secp521r1)

Certificate Field Value:

3 (0x2)

2. Click **Commission Card**.



Security Domain

Load Security Domain (from CTA set)

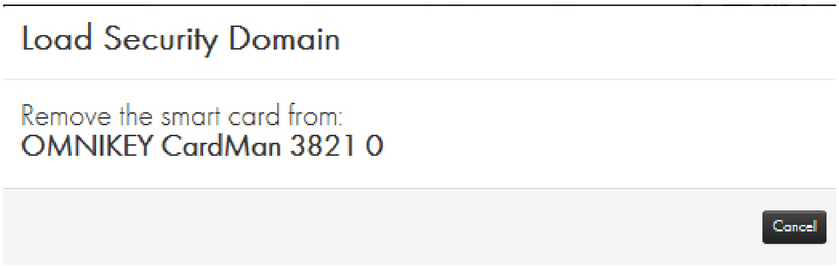
Smart card operations progress: 0%

Click 'Next' to begin loading a security domain.

3. Insert one card from your existing CTA into the card reader.

   Note: You must move efficiently, as this operation will timeout.

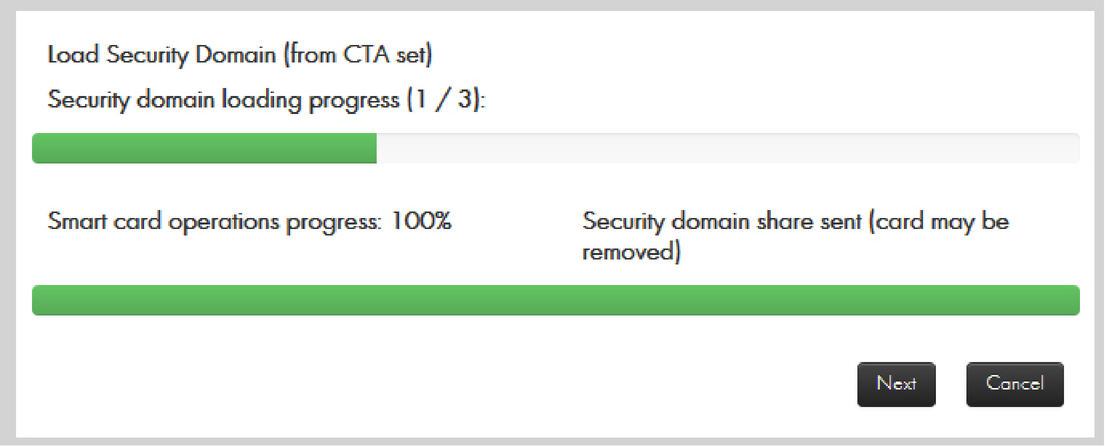
4. Click **Next**.



Load Security Domain

Remove the smart card from:
OMNIKEY CardMan 3821 0

5. Click **Next**.



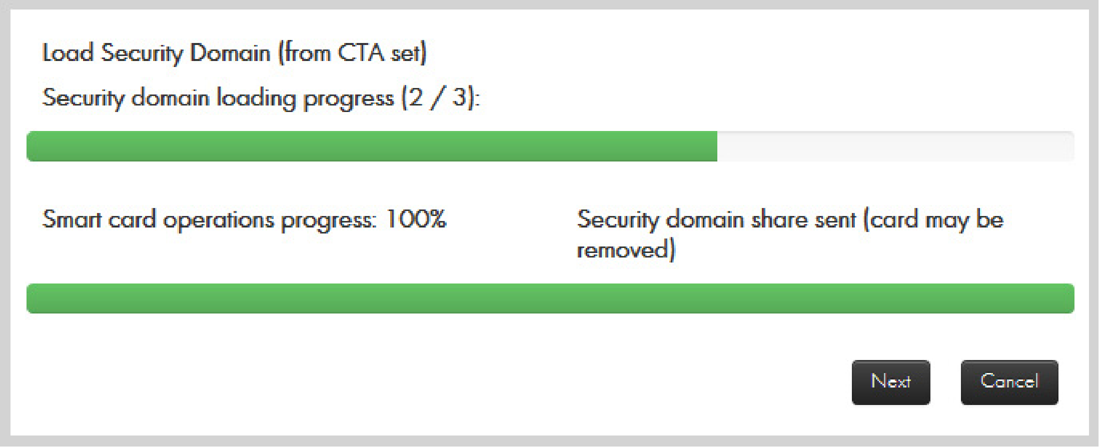
Load Security Domain (from CTA set)

Security domain loading progress (1 / 3):

Smart card operations progress: 100%

Security domain share sent (card may be removed)

6. Click **Next**.

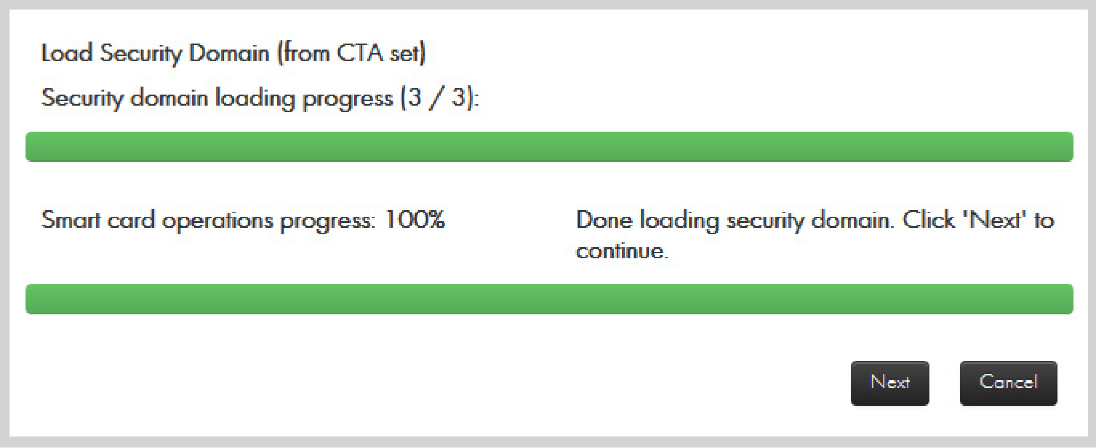


Load Security Domain (from CTA set)

Security domain loading progress (2 / 3):

Smart card operations progress: 100%

Security domain share sent (card may be removed)



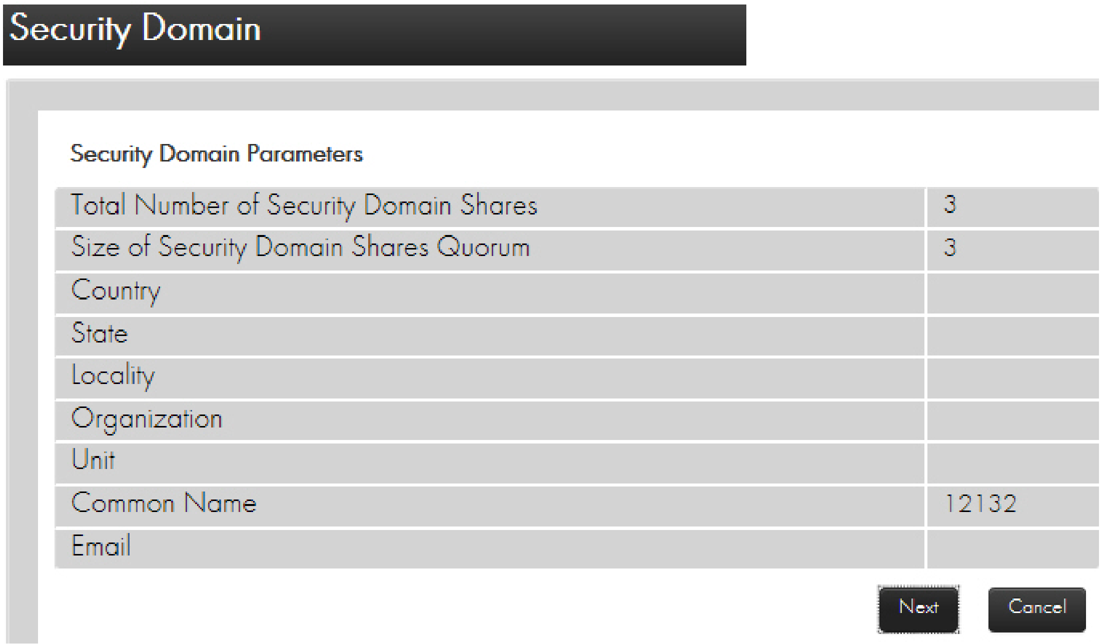
Load Security Domain (from CTA set)

Security domain loading progress (3 / 3):

Smart card operations progress: 100%

Done loading security domain. Click 'Next' to continue.

7. Click **Next**.

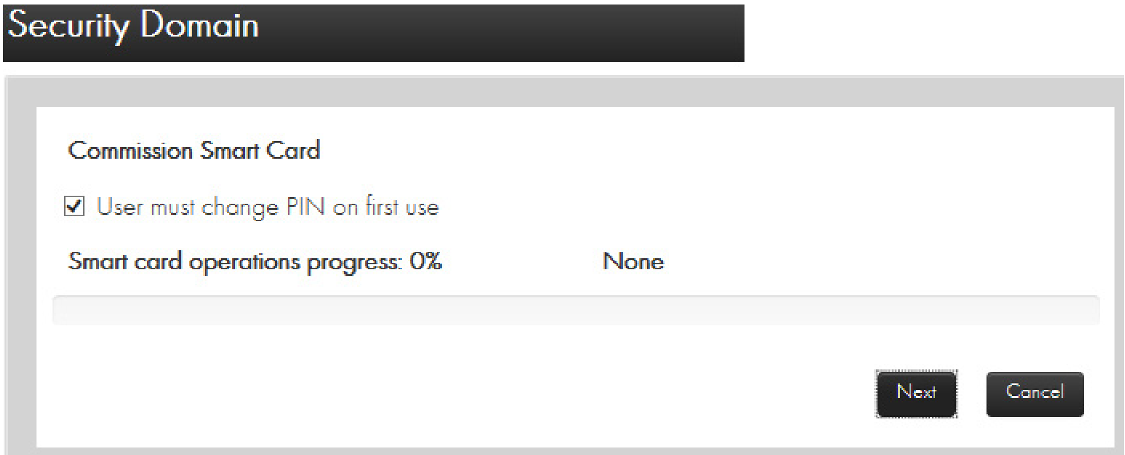


Security Domain

Security Domain Parameters

Total Number of Security Domain Shares	3
Size of Security Domain Shares Quorum	3
Country	
State	
Locality	
Organization	
Unit	
Common Name	12132
Email	

8. Click **Next**.



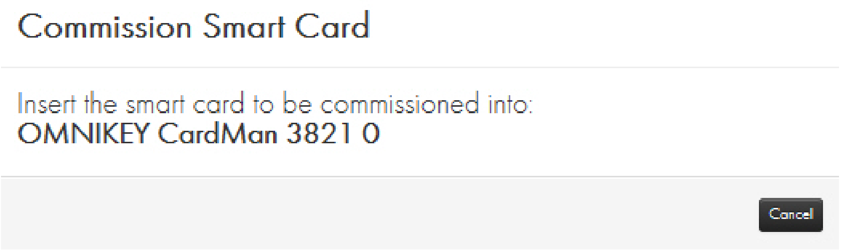
Security Domain

Commission Smart Card

☑ User must change PIN on first use

Smart card operations progress: 0% None

9. Click **Next**.



Commission Smart Card

Insert the smart card to be commissioned into:
OMNIKEY CardMan 3821 0

10. Enter your PIN and press **OK**.

11. Enter the new PIN two times followed by **OK**.

Note: Follow this link, should you need to return to: Section 3.6, “Migrate LMK Cards to become RLMK Cards”, on page 463.

8.9.2.2 Decommission a Card

Decommissioning a card is essentially erasing the certificates from it. Once decommissioned, the card cannot be used in an HSM until it has been commissioned again.

In any state, you may decommission a card by clicking on the “Decommission Card” button. Click **Next** to begin. Click **OK** in the warning dialogue to continue. When prompted, insert the card you want to decommission.

8.9.2.3 Copy a Domain Card

In secure state, you may create a duplicate of a domain (CTA share) card by clicking on the “Copy Domain Card” button. When prompted, enter the CTA card to be copied and enter the card’s PIN.

When prompted, remove the CTA card, insert a prior commissioned card to write the CTA share onto and enter the card’s PIN.

8.9.2.4 Create a New Security Domain

In secure state, you may create a new Security Domain by clicking on the “New Domain” button. You will be prompted to enter the following information:

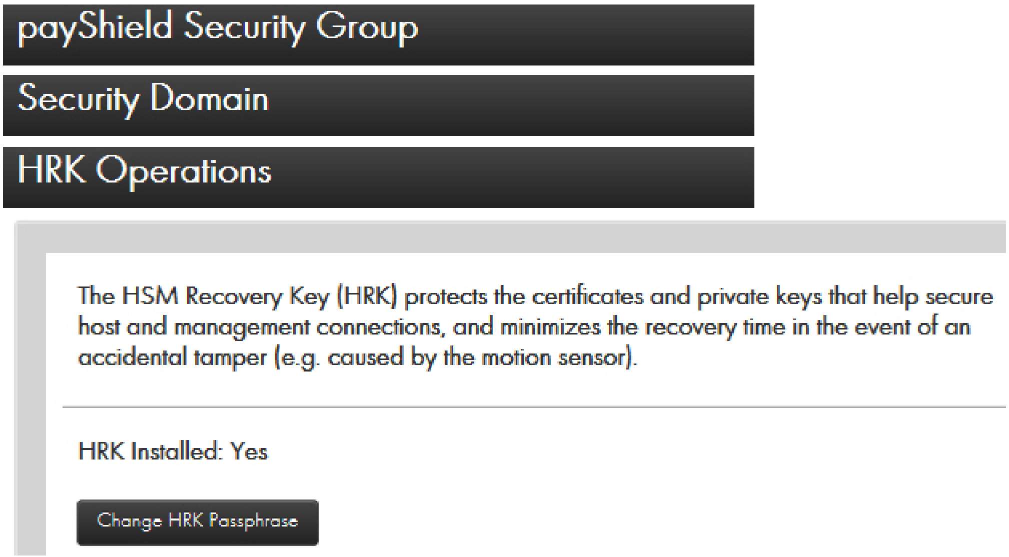
- Number of Security Domain Shares
- Quorum Size
- Country, State, Location
- Organization, Unit
- Common Name
- Email

Once all information has been entered, click “Next” to proceed. When prompted, enter a new or previously commissioned Smart Card (if it is already commissioned, it will confirm that you wish to overwrite the current data) to store the first CTA share and enter a PIN for the card twice. Continue clicking “Next” and inserting additional cards until all CTA shares have been written. When finished, click “Finish” to return to the Security Domain screen.

8.9.2.5 HRK Operations

The HRK is used to encrypt the HSM’s private key used by the HSM in establishing TLS/SSL sessions for the Host and management interfaces.

This tab is used to change the Administrator passphrases for the HRK.



payShield Security Group

Security Domain

HRK Operations

The HSM Recovery Key (HRK) protects the certificates and private keys that help secure host and management connections, and minimizes the recovery time in the event of an accidental tamper (e.g. caused by the motion sensor).

HRK Installed: Yes

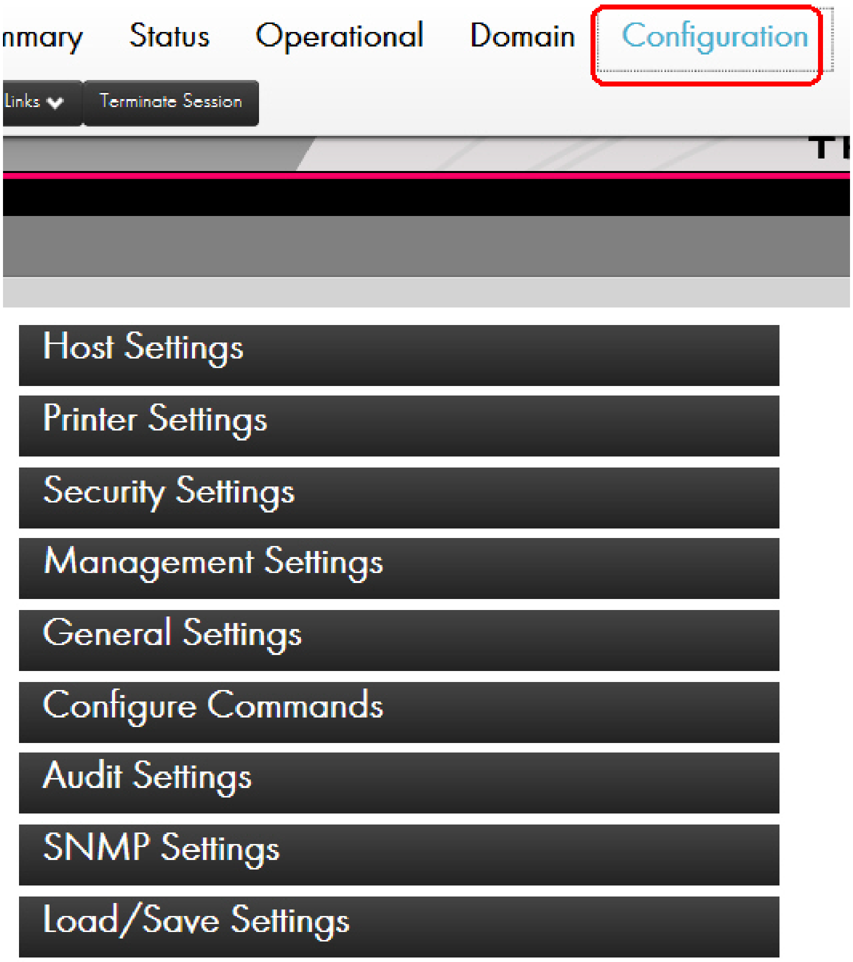
To change a passphrase, click “Change HRK Passphrase”. In the table, specify which Administrator you want to change the passphrase for, use the keyboard enter the current passphrase, use the keyboard to enter the new passphrase twice in the appropriate boxes, and click “Next”.

Passphrases require the following:

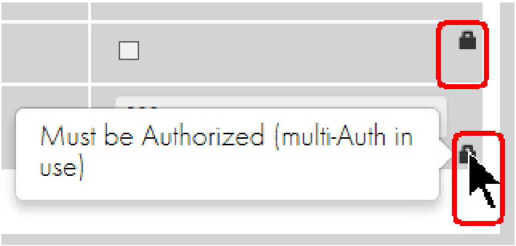
- At least 2 upper case characters
- At least 2 lower case characters
- At least 2 numbers
- At least 2 special characters

Note: In order to send the passphrases securely to the payShield, the browser requires a commissioned Smart Card (e.g,. it can be any one of the security domain’s commissioned Smart Cards). Follow the instructions displayed by the wizard for presenting the commissioned Smart Card. Changing the HRK passphrases takes about a minute.

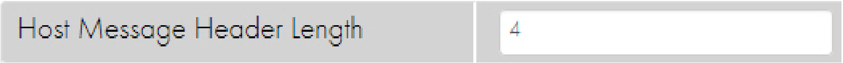
8.10 Configuration



Note: Presence of a lock icon, indicates the setting/action requires proper authorization.



8.10.1 Host Settings

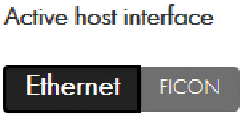


Host Message Header Length: 4

Host Message Header Length: Each transaction to the HSM begins with a string of characters (header), which the Host can use to identify the transaction (or for any other purpose). The HSM returns the string unchanged to the Host in the response message. The length of the header can be set to any value between 1 and 255; the default value is 4.

8.10.2 Active Host Interface

The current active Host interface for the HSM is emphasized as shown below. In this case, the Ethernet interface is the current active Host interface.

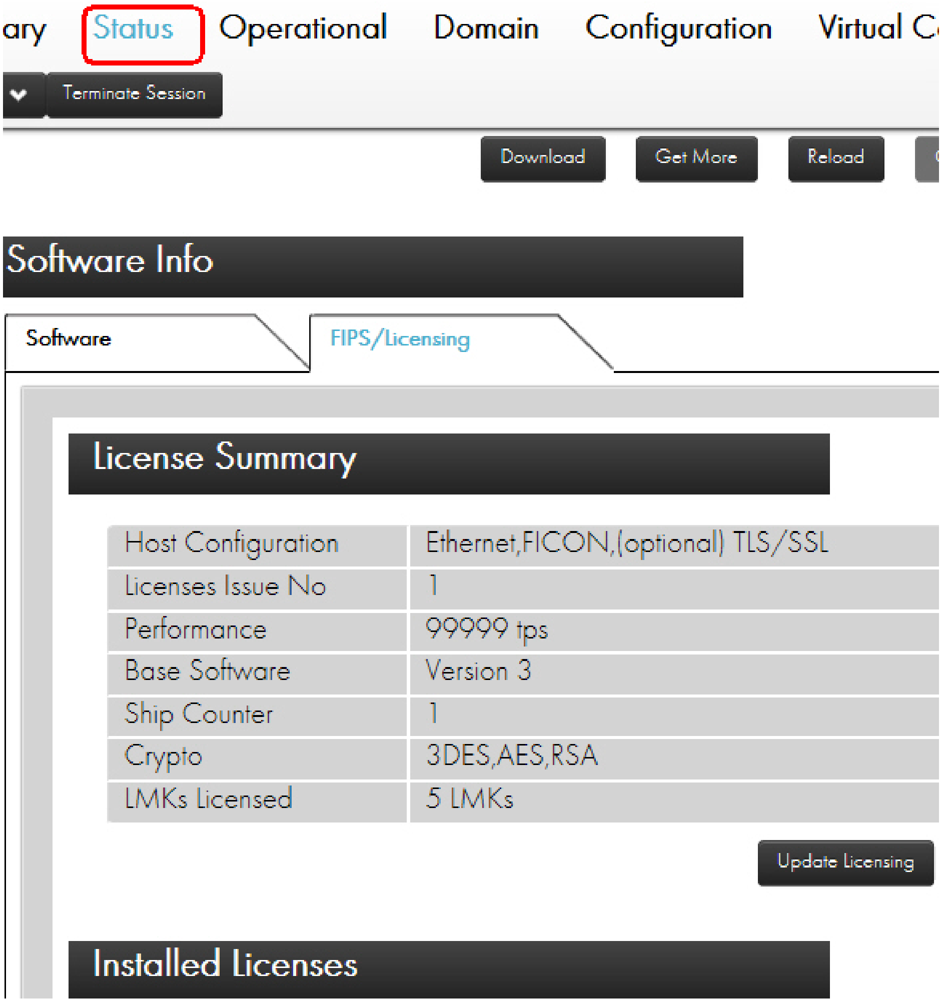


Active host interface

.

In offline or secure state, you may choose the “Ethernet”, or “FICON” as the active Host interface port by selecting the appropriate button, completing the settings for the interface (as explained below), and selecting the “Apply” button.

Note: Interfaces are licensed. If an interface is not available, your HSM may not be licensed for it. Review the interface license. Navigate to Status > Software Info > FIPS/Licensing.



Host Configuration	Ethernet,FICON,(optional) TLS/SSL
Licenses Issue No	1
Performance	99999 tps
Base Software	Version 3
Ship Counter	1
Crypto	3DES,AES,RSA
LMKs Licensed	5 LMKs

8.10.3 Ethernet

The payShield provides 2 Host Ethernet interfaces and allows the port speed and duplexity to be set independently.

The HSM's Host Ethernet interfaces support the delivery of Host commands via TCP/IP or UDP/IP.

The two Host Ethernet interfaces support speeds of 10, 100, and 1,000 Mbits/sec each and require unique IP addresses.

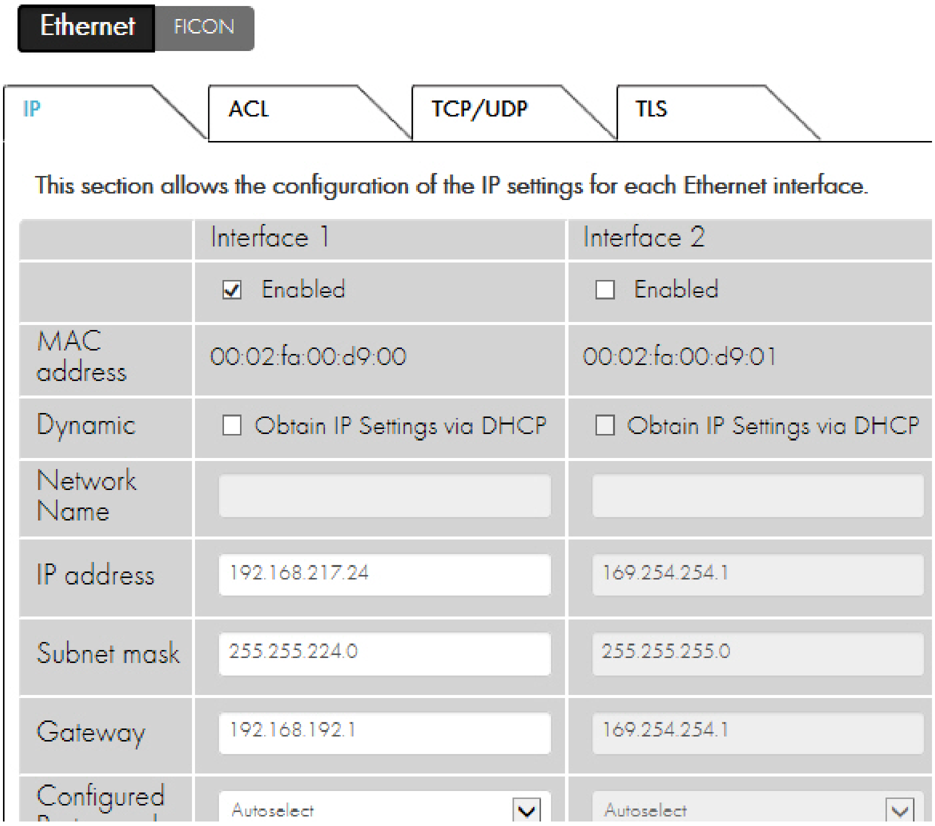
It is recommended that the Management Ethernet Port be on different IP subnet from the Host Ethernet Ports.

After making alterations to the Ethernet settings, press “Apply” to commit the changes to the HSM.

8.10.3.1 IP

In this section, network settings may be set up for each Ethernet interface provided the unit is in offline or secure state.

You may enable each interface independently using the “Enabled” check box. You must have at least one interface enabled when Ethernet is the Clicked Active Host Interface.



This section allows the configuration of the IP settings for each Ethernet interface.

	Interface 1	Interface 2
	☑ Enabled	□ Enabled
MAC address	00:02:fa:00:d9:00	00:02:fa:00:d9:01
Dynamic	□ Obtain IP Settings via DHCP	□ Obtain IP Settings via DHCP
Network Name		
IP address	192.168.217.24	169.254.254.1
Subnet mask	255.255.224.0	255.255.255.0
Gateway	192.168.192.1	169.254.254.1
Configured	Autoselect	Autoselect

The following items are set up for each Host port:

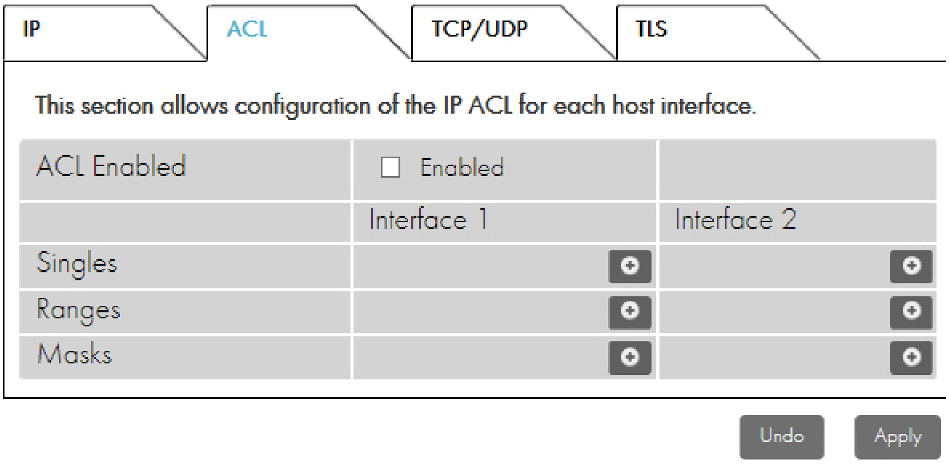
- MAC address
  - A read only field showing the MAC address of the Host Ethernet port.
- Dynamic
  - If checked, this port will be configured using DHCP instead of manually configured and the “Network Name” field becomes editable while the “IP address”, “Subnet mask”, and “Gateway” fields become read-only.
- Network Name
  - The HSM will specify this user-friendly name in the DHCP request as the desired name for this interface. If your DNS is configured properly, the given Network Name can be used to address this HSM interface.
- IP Address

- When DHCP is not employed, a static IP address for the payShield 10K's Host port may be specified. This must be a unique IP address on the Host network.
- Example: 192.168.001.010

- Subnet Mask
  - When DHCP is not employed, a subnet mask for the payShield 10K's Host port may be specified. This is used to define the network class.
  - Example: 255.255.255.000
- Gateway
  - When DHCP is not employed, a default gateway address for the payShield 10K's Host port may be specified. This is the IP address of the default gateway in the network.
  - Example: 192.168.001.001
- Configured Port Speed
  - The speed and duplexity at which the Host port is to run.
- Actual Port Speed
  - A read only field that displays the actual speed as reported by the Ethernet interface.

8.10.3.2 Access Control List (ACL)

In this section, an Access Control List to restrict access to each of the HSM's Ethernet Host Interfaces may be enabled and setup provided the unit is in offline or secure state.



This section allows configuration of the IP ACL for each host interface.

ACL Enabled	☐ Enabled	
	Interface 1	Interface 2
Singles	⊕	⊕
Ranges	⊕	⊕
Masks	⊕	⊕

Each interface may have its own set of ACLs. Control may be restricted using any combination of:

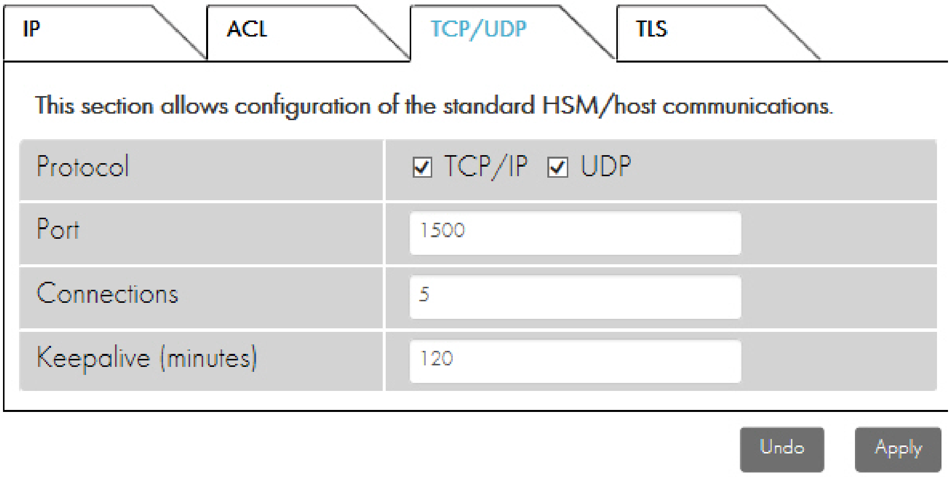
- Singles
  - A single IP address.

  - Example: 192.168.1.5
- Ranges
  - A range of addresses consisting of a starting address and an ending address.
  - Example: 192.168.1.5 / 192.168.1.10
- Masks
  - A range of addresses consisting of a base address and a subnet mask.
  - Example: 192.168.1.90 / 255.255.255.128

Entries may be added or removed using the plus and minus icons in each section.

8.10.3.3 TCP/UDP

In this section, TCP and UDP protocol settings may be altered provided the unit is in offline or secure state.



This section allows configuration of the standard HSM/host communications.

Protocol	☑ TCP/IP ☑ UDP
Port	1500
Connections	5
Keepalive (minutes)	120

The following options are available:

- Protocol
  - Specify which protocols (TCP and/or UDP) the HSM should accept as incoming connections. If unchecked, any incoming traffic conforming to that protocol will be discarded. (Note that it is not valid to un-check both TCP and UDP.)
- Port
  - The base port to be used for communication with connecting Hosts.
- Connections
  - The maximum number of simultaneous connections to allow (up to 64).
- Keepalive

– The amount of time (in seconds) that an idle connection should be kept open.

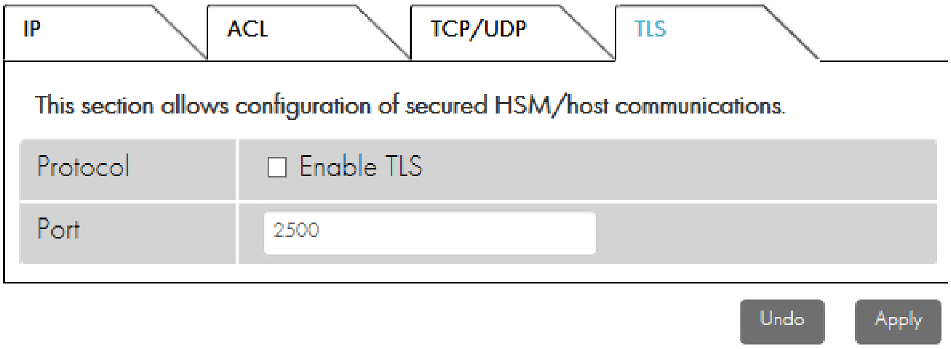
Table 5 *Port Settings*

Port	Protocol	Purpose
xxxx	TCP/UDP	Well-known port for command traffic between host and payShield, as defined in host port parameters. Default is 1500. Use of this port results in the default LMK being used unless the command explicitly identifies another LMK.
xxxx + n	TCP/UDP	Well-known port for command traffic between host and payShield where LMK n-1 is to be used. For example, if the default well-known port has been defined as 1500, then 1501 is used if LMK 0 is required for the command, 1502 is used if LMK 1 is required for the command, and so on. An explicit identification of the LMK in the command overrides the LMK implied by the port number.

–

8.10.3.4 TLS

In this section, the secure Host communications protocols (SSL and/or TLS) and settings may be altered provided the unit is in offline or secure state.



This section allows configuration of secured HSM/host communications.

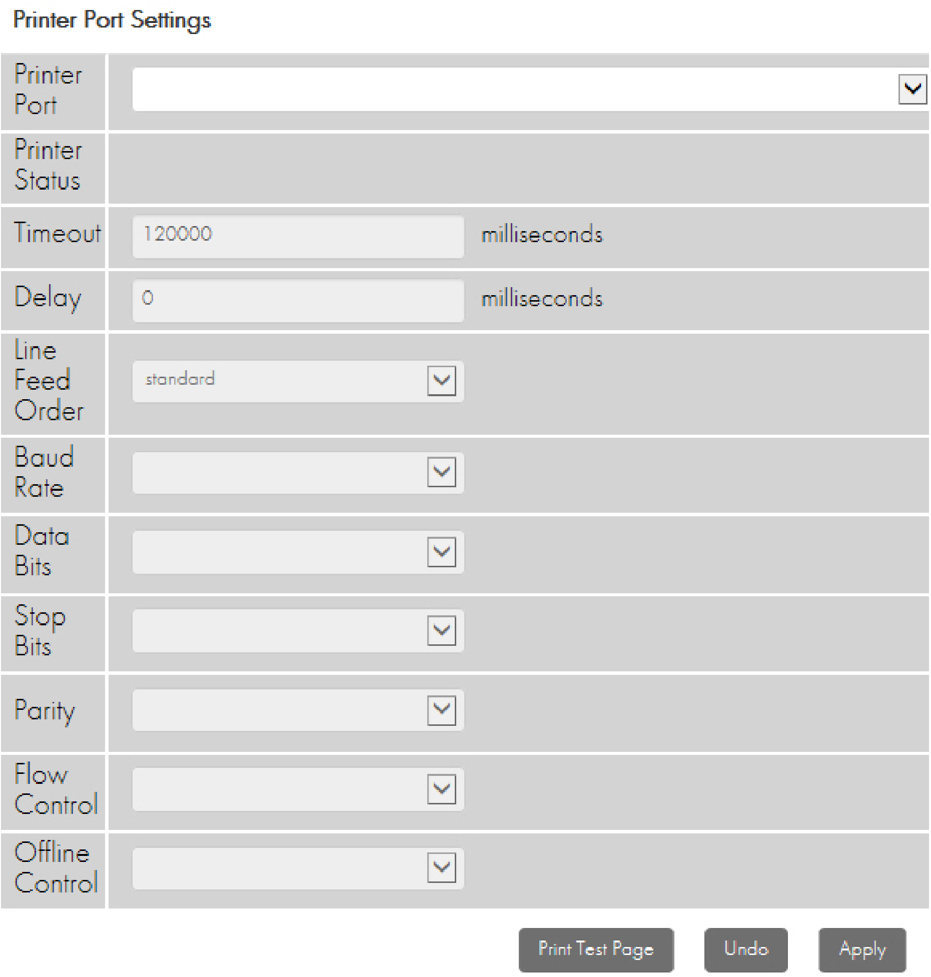
Protocol	☐ Enable TLS
Port	2500

The following options are available:

- Protocol
  - – Specify whether the HSM should use SSL/TLS to require the use of SSL for connections or TLS only to require the use of TLS for securing communications.
- Port
  - – The base port to be used for communication with connecting Hosts.

8.10.3.5 Printer Settings

You may alter the configuration of connected printers when the unit is in offline or secure settings and there is at least one parallel or serial USB adapter attached to the HSM that has not been designated as a Host Interface by adjusting the settings explained below and selecting the “Apply” button to commit the changes to the HSM. Once configured and still offline or in secure state, you may print a test page to the printer using the “Print Test Page” button.



Printer Port Settings

Printer Port		
Printer Status		
Timeout	120000	milliseconds
Delay	0	milliseconds
Line Feed Order	standard	
Baud Rate		
Data Bits		
Stop Bits		
Parity		
Flow Control		
Offline Control		

Options:

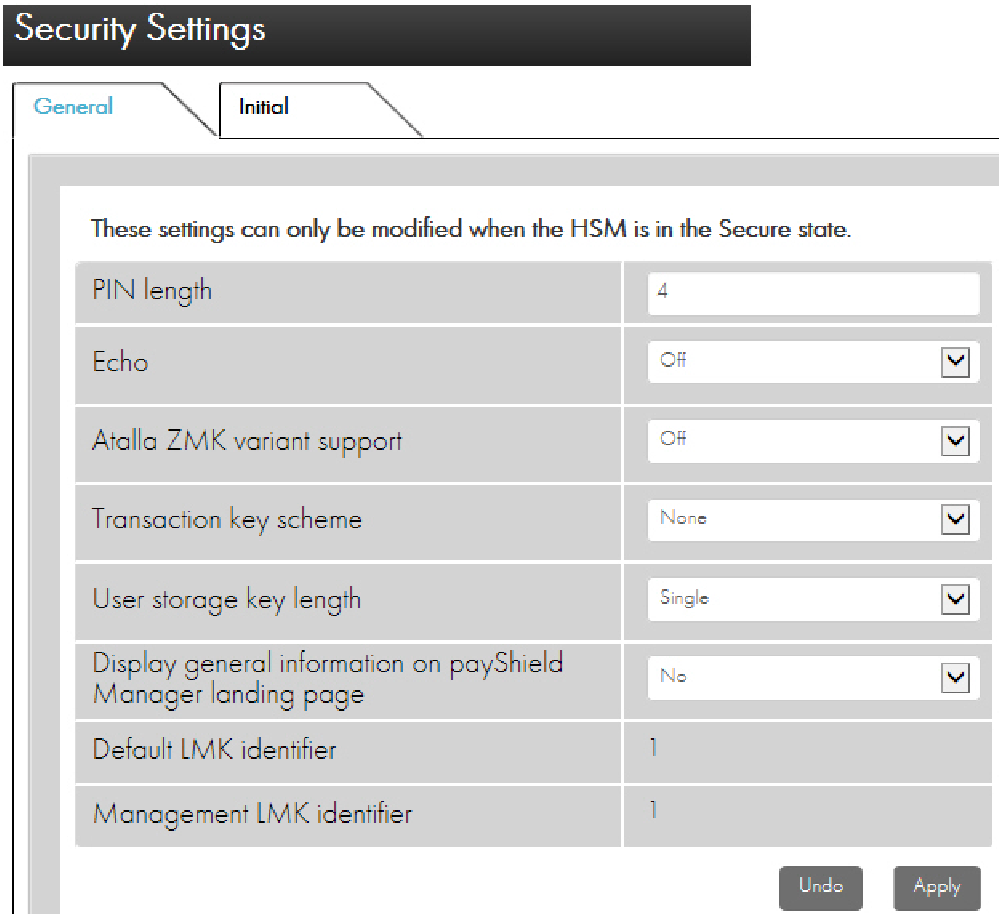
- Printer Port
  - Click the serial or parallel USB adapter that the printer is connected to. Note that once the adapter is designated as a printer interface, it cannot be used as a Console Port.
- Printer Status
  - Read-only field showing the current status of the printer.
- Timeout
  - The time in milliseconds before giving up on an attempt to communicate with the printer.

- Delay
  - The time to wait before attempting to communicate with the printer.
- Line Feed Order
  - May be either standard (<LF><CR>) or reversed (<CR><LF>).
- Baud Rate (serial only)
  - The number of bits per second to transfer. Default: 115200.
- Data Bits (serial only)
  - The number of bits per character. Default: 8.
- Stop Bits (serial only)
  - Number of bits sent at the end of each character. Default: 1
- Parity (serial only)
  - Means of checking for errors in transmission. May be set to None, Odd, or Even. Default: None.
- Flow Control
  - Specifies whether to use any hardware or software mechanisms to control the flow of data. Default: None.
- Offline Control
  - Specifies whether to use DTR or RTS signals to detect if the printer is offline. Click none to disable this feature. Default: None.

8.10.4 Security Settings

You may alter the security configuration of the unit when it is in a secure state by adjusting the settings explained below and selecting the “Apply” button to commit the changes to the HSM. Note that changing any settings in the “Initial” tab result is deleting all the LMKs stored in the unit.

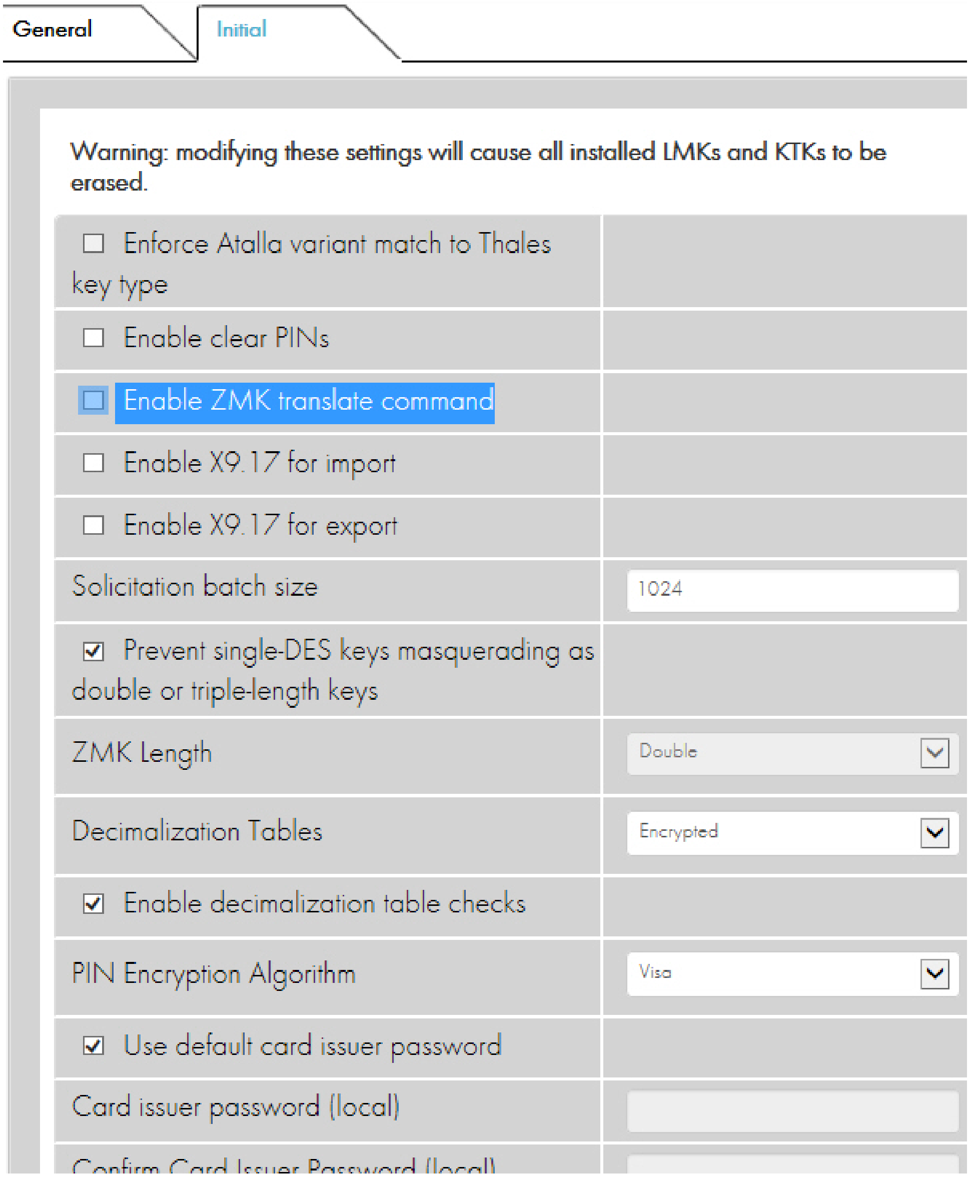
General Tab



These settings can only be modified when the HSM is in the Secure state.

PIN length	4
Echo	Off
Atalla ZMK variant support	Off
Transaction key scheme	None
User storage key length	Single
Display general information on payShield Manager landing page	No
Default LMK identifier	1
Management LMK identifier	1

Initial Tab



General | Initial

Warning: modifying these settings will cause all installed LMKs and KTKs to be erased.

□ Enforce Atalla variant match to Thales key type	
□ Enable clear PINs	
□ Enable ZMK translate command	
□ Enable X9.17 for import	
□ Enable X9.17 for export	
Solicitation batch size	1024
☑ Prevent single-DES keys masquerading as double or triple-length keys	
ZMK Length	Double
Decimalization Tables	Encrypted
☑ Enable decimalization table checks	
PIN Encryption Algorithm	Visa
☑ Use default card issuer password	
Card issuer password (local)	
Confirm Card Issuer Password (local)	

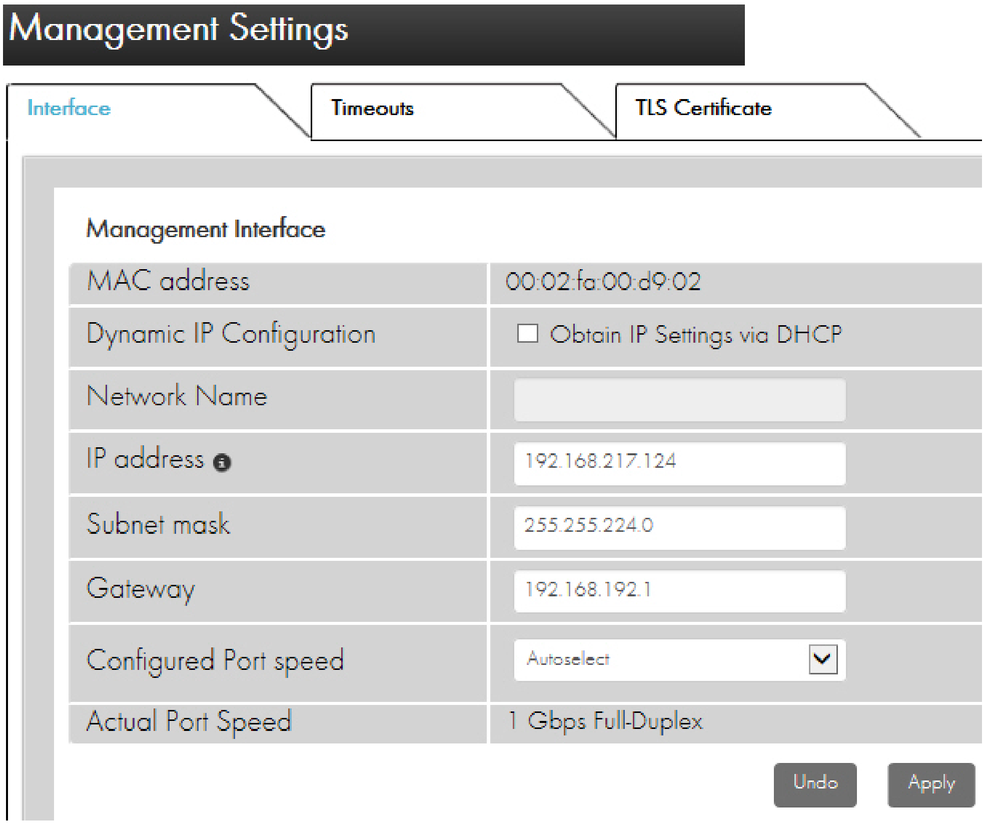
8.10.4.1 Security Parameter Descriptions

Refer to the *payShield 10K Security Manual* for a full description of the security parameters and their settings.

8.10.5 Management Settings

You may alter the management settings when the HSM is in the offline or secure state. Select the “Apply” button to commit the changes to the HSM.

8.10.5.1 Management - Interface



Management Interface

MAC address	00:02:fa:00:d9:02
Dynamic IP Configuration	□ Obtain IP Settings via DHCP
Network Name	
IP address	192.168.217.124
Subnet mask	255.255.224.0
Gateway	192.168.192.1
Configured Port speed	Autoselect
Actual Port Speed	1 Gbps Full-Duplex

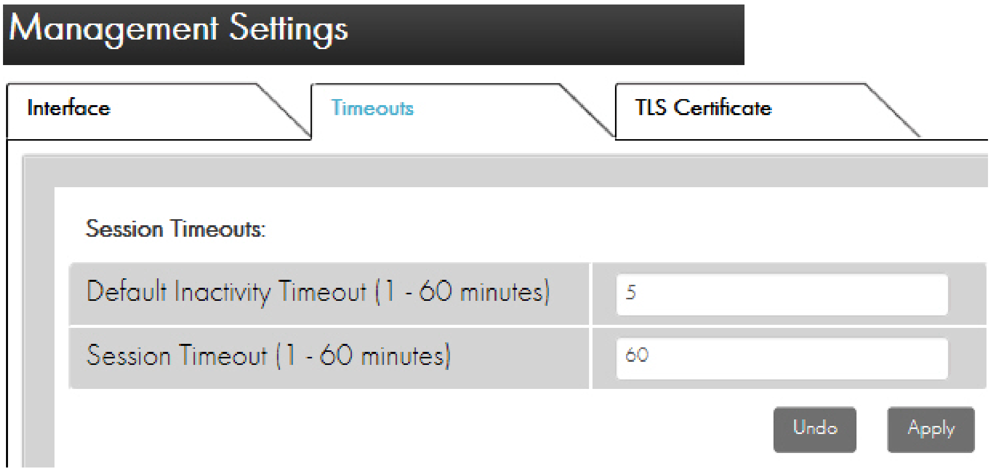
In this section, network settings may be adjusted for the Management Ethernet interface. The following options are available:

- MAC address:
  - A read only field showing the MAC address of the management port.
- Dynamic IP Configuration:
  - If checked, the management port will be configured using DHCP instead of manually configured and the “Network Name” field becomes editable while the “IP address”, “Subnet mask”, and “Gateway” fields become un-editable.

- Network Name:
  - The HSM will specify this user-friendly name (following section 3.14 of RFC1533) in the DHCP request as the desired name for this interface. If your DNS is configured properly, the given Network Name can be used to address this HSM interface.
- IP address:
  - When DHCP is not employed, you may specify a static IP address for the payShield 10K's management port. This must be a unique IP address on the management network.
  - Example: 192.168.002.010
- Subnet mask:
  - When DHCP is not employed, you may specify a subnet mask for the payShield 10K's management port. This is used to define the network class. It is highly recommended that the management network and Host network are not the same.
  - Example: 255.255.255.000
- Gateway:
  - When DHCP is not employed, you may specify a default gateway address for the payShield 10K's management port. This is the IP address of the default gateway in the network.
  - Example: 192.168.002.001
- Configured Port Speed:
  - The speed and duplexity at which the management port is to run.
- Actual Port Speed:
  - A read only field that displays the actual speed as reported by the Ethernet interface.

8.10.5.2 Management - Timeouts

This tab allows for configuration of the different timeout options for management sessions.

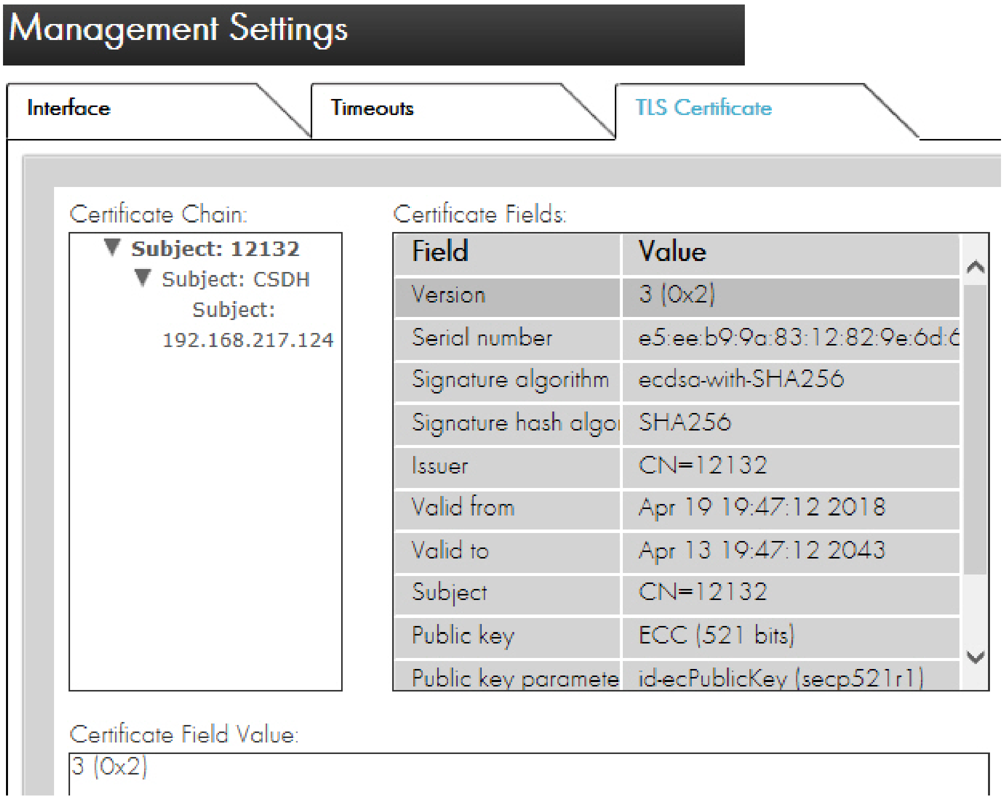


Session Timeouts:

Default Inactivity Timeout (1 - 60 minutes)	5
Session Timeout (1 - 60 minutes)	60

- Default Inactivity Timeout:
  - This timeout is triggered when the payShield Manager detects no user activity. After the configured time has elapsed, the inactive user will be automatically logged out.
- Session Timeout:
  - This timeout begins when you logs in and continuously counts down, irrespective of activity. When the timer reaches 0, you is automatically logged out.
  - The Time Remaining counter, seeded with this value, is located in the bottom right of the management screen. As the time approaches zero, the counter will display in red alerting you that session time is expiring.

8.10.5.3 Management - TLS Certificate



Management Settings

Certificate Chain:

- Subject: 12132
  - Subject: CSDH
    - Subject: 192.168.217.124

Certificate Fields:

Field	Value
Version	3 (0x2)
Serial number	e5:ee:b9:9a:83:12:82:9e:6d:6
Signature algorithm	ecdsa-with-SHA256
Signature hash algo	SHA256
Issuer	CN=12132
Valid from	Apr 19 19:47:12 2018
Valid to	Apr 13 19:47:12 2043
Subject	CN=12132
Public key	ECC (521 bits)
Public key paramete	id-ecPublicKey (secp521r1)

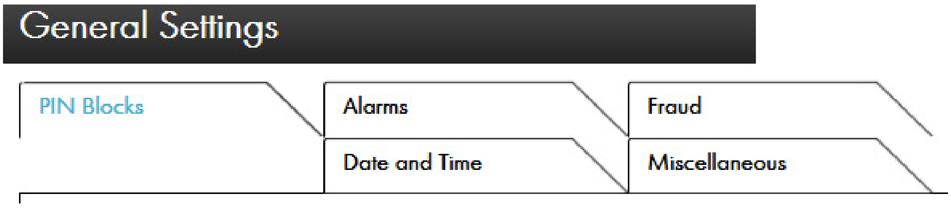
Certificate Field Value: 3 (0x2)

This is the certificate that was created when establishing the security domain (CTA).

8.10.6 General Settings

General Settings include tabs for:

- PIN Blocks
- Alarms
- Fraud
- Date and Time
- Miscellaneous

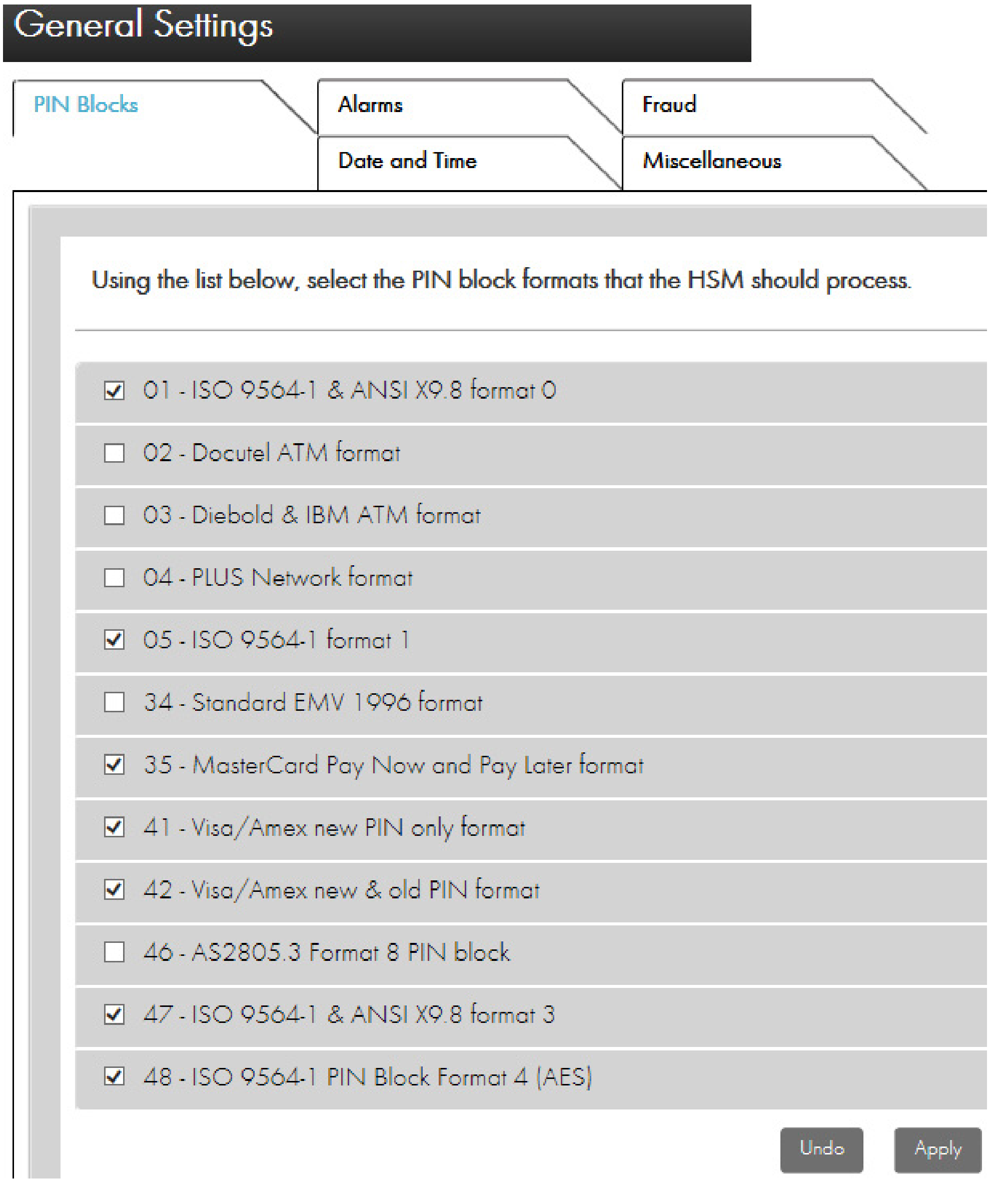


General Settings

8.10.6.1 General - PIN Blocks

– This tab allows you to Click which PIN Block formats should be enabled on the HSM when in offline or secure state.

A Host system would typically not use all the PIN Block formats supported by the HSM. A simple but effective method of locking-down the HSM is to disable (un-check) all unused PIN block formats: the subsequent use of a disabled format would result in an error code (69) being returned. Select the “Apply” button top commit the changes to the HSM.



Using the list below, select the PIN block formats that the HSM should process.

☑ 01 - ISO 9564-1 & ANSI X9.8 format 0

□ 02 - Docutel ATM format

□ 03 - Diebold & IBM ATM format

□ 04 - PLUS Network format

☑ 05 - ISO 9564-1 format 1

□ 34 - Standard EMV 1996 format

☑ 35 - MasterCard Pay Now and Pay Later format

☑ 41 - Visa/Amex new PIN only format

☑ 42 - Visa/Amex new & old PIN format

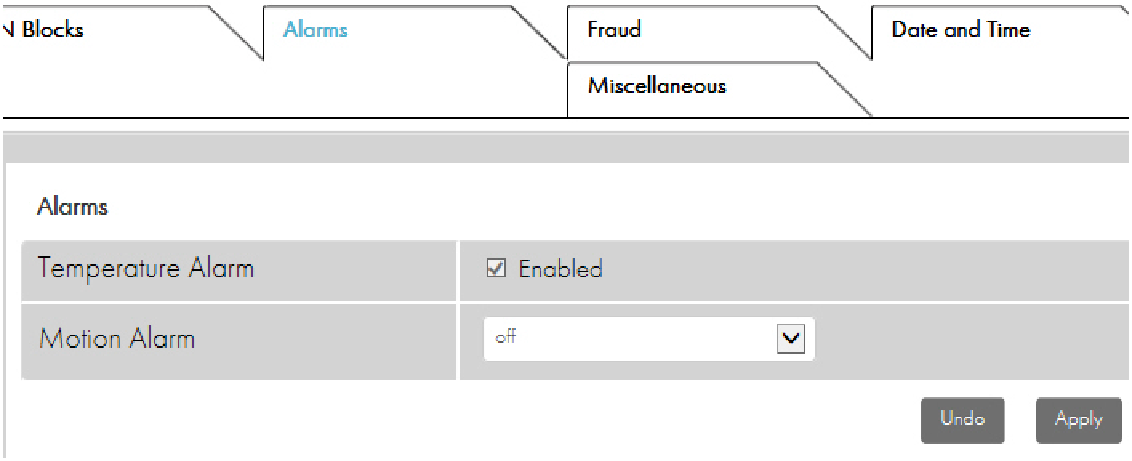
□ 46 - AS2805.3 Format 8 PIN block

☑ 47 - ISO 9564-1 & ANSI X9.8 format 3

☑ 48 - ISO 9564-1 PIN Block Format 4 (AES)

8.10.6.2 General - Alarms

This tab allows you to enable or disable alarms relating to hardware sensors when the unit is in secure state. Select the “Apply” button to commit the changes to the HSM.



Alarms

Temperature Alarm	☑ Enabled
Motion Alarm	off

The following alarms can be monitored/configured:

- Temperature Alarm:
  - Triggers an alert if the temperature inside the HSM exceeds a safe value
  - The Alarm is permanently enabled, and can not be disabled by users
  - 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.
- Motion Alarm:
- The ADXL362 accelerometer in the PayShield 10K acts as a “Motion Sensor” detecting tilt movements. An alarm triggers an alert if the HSM is moved (for example, slid out of the rack).
  - Users can configure the motion sensor’s threshold sensitivity to one of three levels: low, medium, high, corresponding to different movement thresholds
  - When powered by battery, the alarm maintains the same capabilities as when powered by battery or from main power.

– The anti-theft feature relies on tilt angle for determining when to trigger a tamper.

Motion Sensor hardware filter settings:

- Low Sensitivity - 171 milli-g
- Medium Sensitivity - 65 milli-g
- High Sensitivity - 25 milli-g

The Motion sensor activity time is 6 ticks @50Hz (.12 seconds)

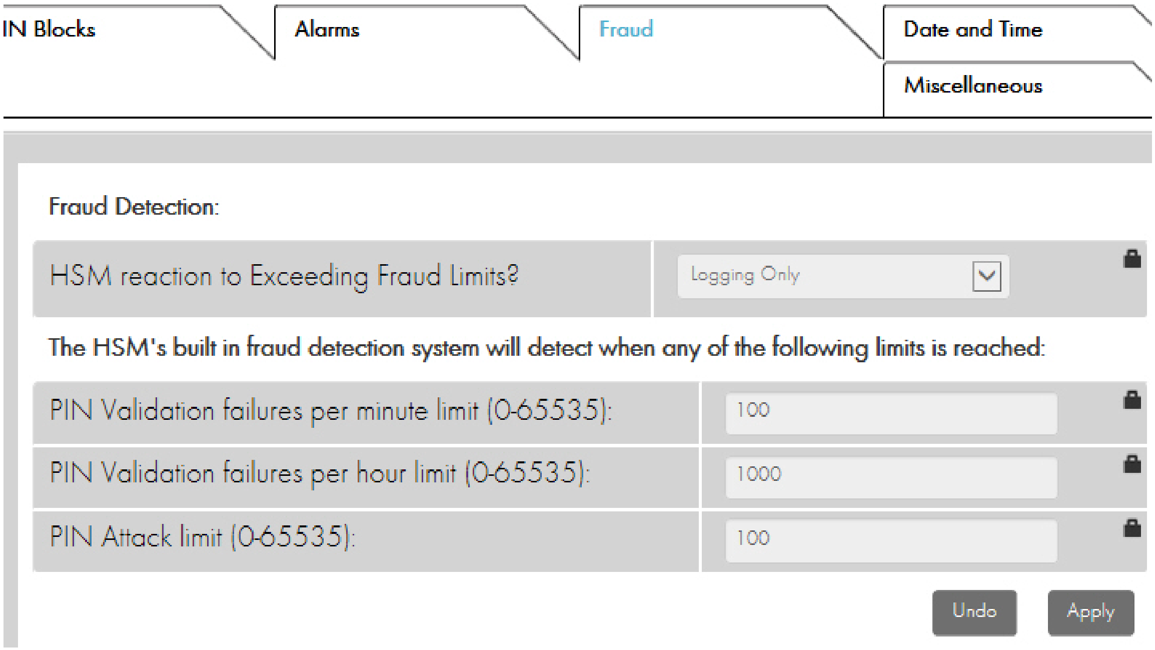
The Hardware filter is a reference setting which tracks the absolute change in acceleration in all three axes ignoring acceleration due to gravity (g). The filter is dynamically updated as the device is tilted.

Motion Sensor tilt threshold values:

- Low Sensitivity - 171 milli-g (Tilt angle 10.0 degrees +-1 degree)
- Medium Sensitivity - 65 milli-g (Tilt angle 6.0 degrees +-1 degree)
- High Sensitivity – 25 milli-g (Tilt angle 1.5 degrees +-1 degree)

8.10.6.3 General - Fraud

This tab allows you to configure fraud detection settings when the unit is offline or in secure state and properly authorized. Select the “Apply” button to commit the changes to the HSM.



Fraud Detection:

HSM reaction to Exceeding Fraud Limits? Logging Only

The HSM's built in fraud detection system will detect when any of the following limits is reached:

PIN Validation failures per minute limit (0-65535): 100

PIN Validation failures per hour limit (0-65535): 1000

PIN Attack limit (0-65535): 100

Options:

- HSM Reaction to Exceeding Fraud Limits:

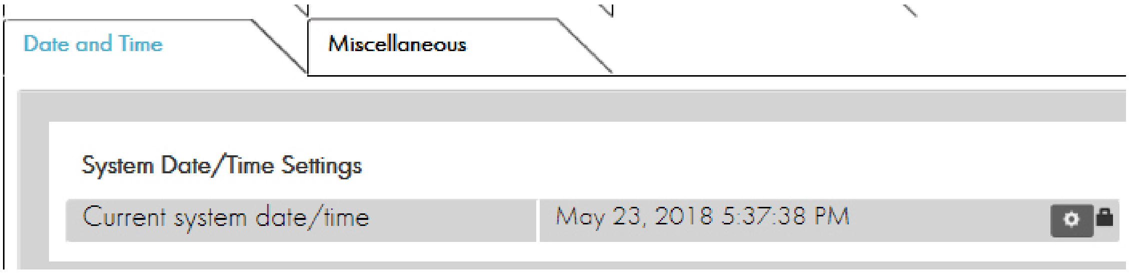
  Click from one of the following options:

- Logging Only: The Health Check data will show how often the limits have been exceeded (if gathering of Health Check statistics is enabled). An entry is also made in the Audit Log when any of the limits is exceeded.
- On: The Health Check data will log the limits being exceeded, but in addition the HSM will start returning error code 39 or delete its LMKs. An entry is also made in the Audit Log when any of the limits is exceeded.

- PIN Validation failures per minute limit:
  - The number of PIN validation failures permitted in a one-minute period before a fraud alert is triggered.
- PIN Validation failures per hour limit:
  - The number of PIN validation failures permitted in a one-hour period before a fraud alert is triggered.
- PIN Attack limit:
  - The number of PIN attacks permitted before a fraud alert is triggered.

8.10.6.4 General - Date and Time

This tab allows you to set the system date and time used by the HSM for audit log entries when the unit is in secure state and properly authorized.



System Date/Time Settings

Current system date/time: May 23, 2018 5:37:38 PM

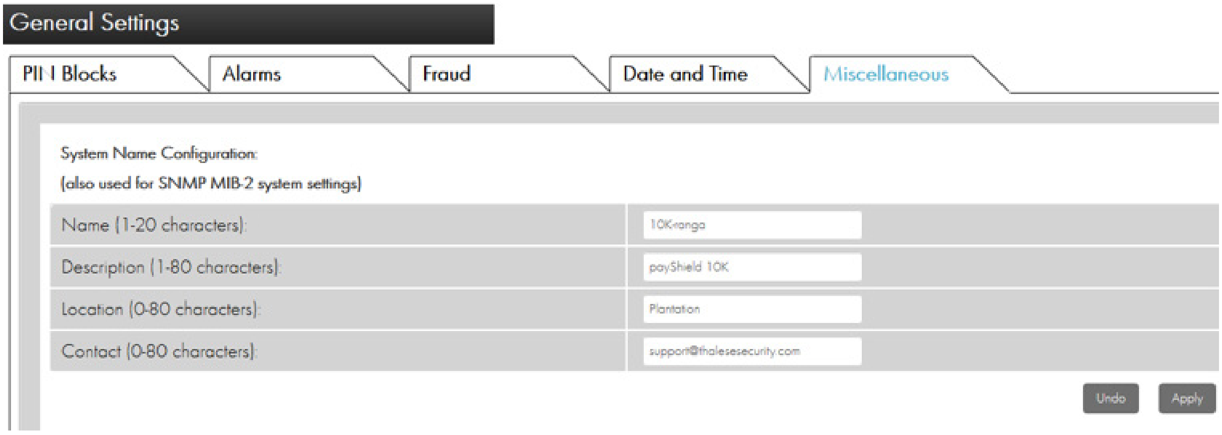
To set the date and time, click the gear icon. In the dialogue box that appears, Click the new date and time values and click “Apply”.

Note: Setting the date or time back may prevent the payShield Manager from allowing a user to login. Care must be taken when changing the date back such that it is not earlier than the creation date/time of any of the Smart Cards that will be used to access the HSM.

8.10.6.5 General - Miscellaneous

This tab allows the user to set the HSM System Name, Description, Location and Contact fields, which are displayed as a more user-friendly way of identifying a particular HSM. These may be altered in any state. Press the “Apply” button to commit the changes to the HSM. Location and Contact fields are optional. These fields are also used for SNMP MIB-2 system objects (sysName, sysDescr, sysLocation, sysContact).

The HSM System Name is displayed in the Landing Page under the Summary section when enabled in the security settings. Configuration for information on enabling the display of the name on the Landing Page.



System Name Configuration:
(also used for SNMP MIB-2 system settings)

Name (1-20 characters):	10K-ranga
Description (1-80 characters):	payShield 10K
Location (0-80 characters):	Plantation
Contact (0-80 characters):	support@thalesesecurity.com

8.10.7 Configure Commands

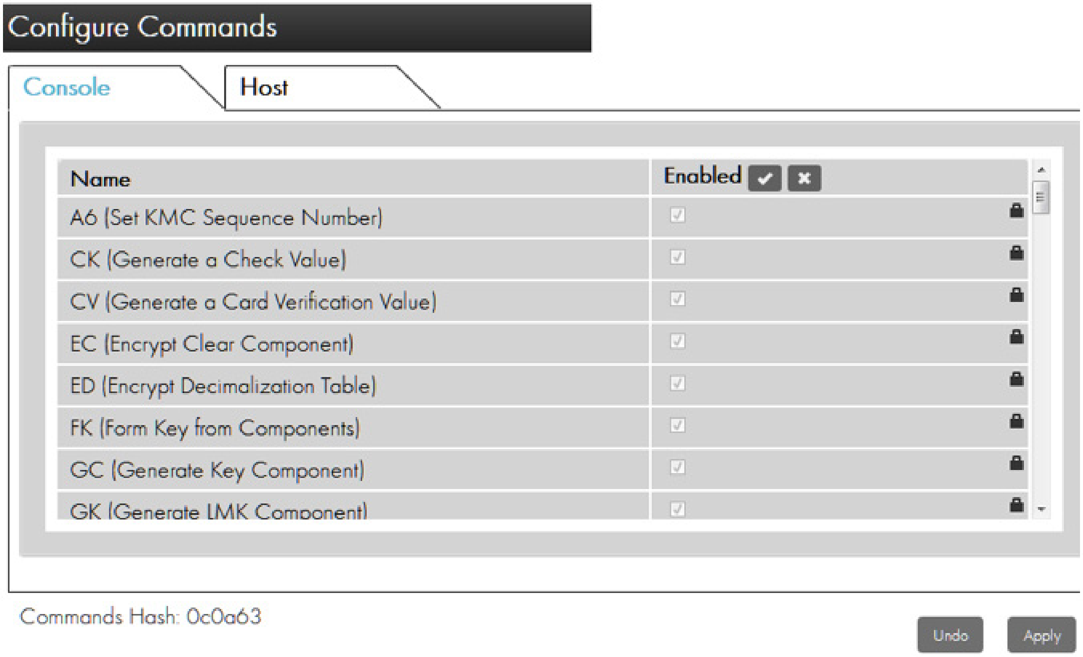
New commands are added to the HSM software on a regular basis. Old commands are rarely removed. As far as is possible, the HSM maintains backward compatibility with existing systems. A side effect is that Host systems tend to use a subset of the commands actually provided by the HSM, leaving many commands unused.

The Configure Commands option allows users to Click which console and Host commands are to be enabled and which disabled when the unit is in secure state.

Commands can be enabled or disabled by checking or un-checking the appropriate box(es) in the tables. Checked items are enabled; unchecked items are disabled.

A simple but effective method of “locking-down” the HSM is to disable all unused commands: the subsequent use of disabled commands would result in an error code (68) being returned.

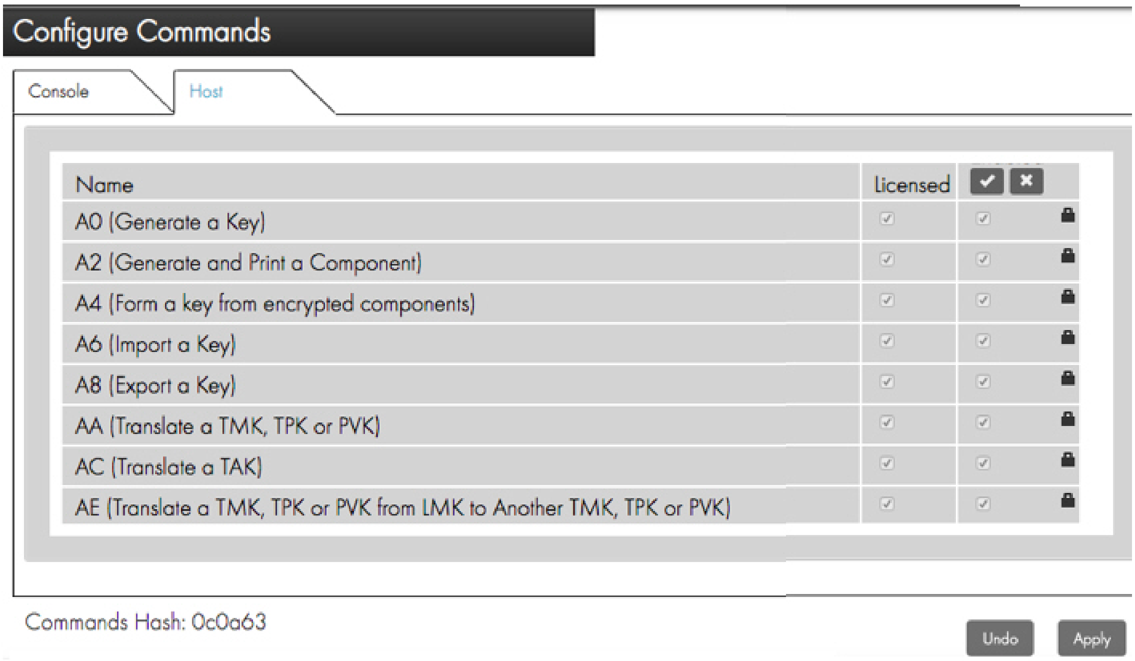
This section is split into two tabs: one for Console Commands, and one for Host Commands. While Console Commands may be enabled or disabled as desired, enabling a Host Command also requires that the corresponding license file to be installed.



Configure Commands

Name	Enabled ✓ ✕	
A6 (Set KMC Sequence Number)	☑	🔒
CK (Generate a Check Value)	☑	🔒
CV (Generate a Card Verification Value)	☑	🔒
EC (Encrypt Clear Component)	☑	🔒
ED (Encrypt Decimalization Table)	☑	🔒
FK (Form Key from Components)	☑	🔒
GC (Generate Key Component)	☑	🔒
GK (Generate LMK Component)	☑	🔒

Commands Hash: 0c0a63

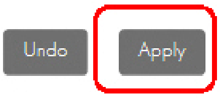


Configure Commands

Name	Licensed	✓ ✕	
A0 (Generate a Key)	☑	☑	🔒
A2 (Generate and Print a Component)	☑	☑	🔒
A4 (Form a key from encrypted components)	☑	☑	🔒
A6 (Import a Key)	☑	☑	🔒
A8 (Export a Key)	☑	☑	🔒
AA (Translate a TMK, TPK or PVK)	☑	☑	🔒
AC (Translate a TAK)	☑	☑	🔒
AE (Translate a TMK, TPK or PVK from LMK to Another TMK, TPK or PVK)	☑	☑	🔒

Commands Hash: 0c0a63

After making changes press the “Apply” button to commit the changes to the HSM.



The UI will generate a SHA-256 Hash over as set of available commands. You can use an offline tools to compute the hash and compare it with the value displayed to ensure that two or more HSMs have the same set of commands available.

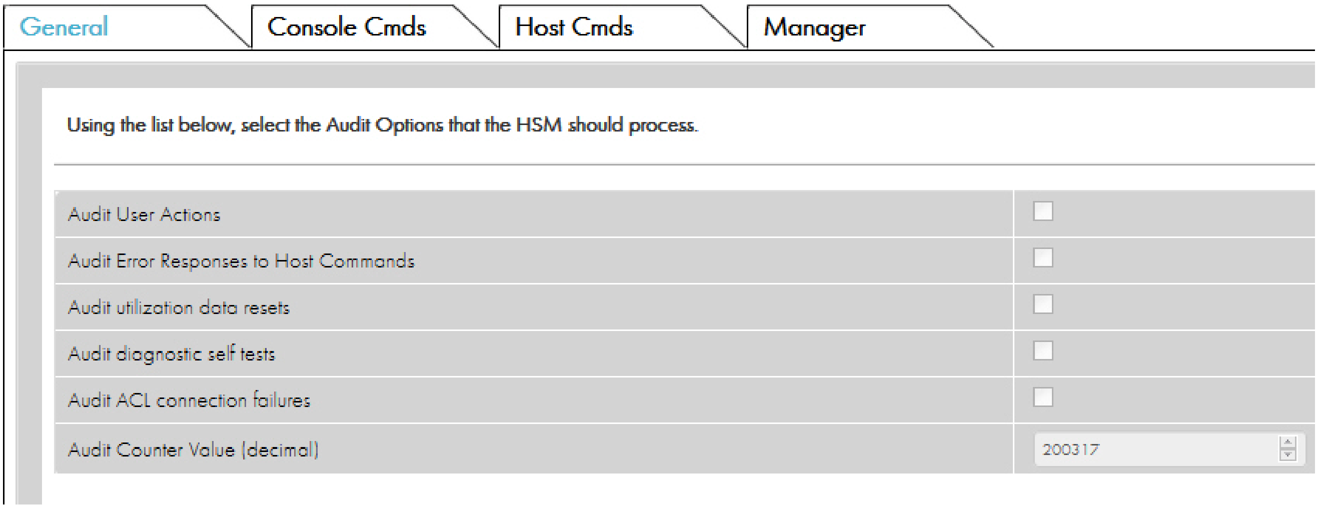
8.10.8 Audit Settings

The HSM’s standard auditing capabilities include auditing (i.e., logging) of various events in the HSM’s Audit Log. The Auditing accordion allows users to Click which items are to be audited and which are not when the unit is offline or in secure state and properly authorized.

After making changes press the “Apply” button to commit the changes to the HSM.

8.10.8.1 Audit - General

Certain sensitive functions, such as key management, authorizations, configurations and diagnostic tests are always recorded in the audit log and their auditing cannot be disabled.



Using the list below, select the Audit Options that the HSM should process.

Audit User Actions	□
Audit Error Responses to Host Commands	□
Audit utilization data resets	□
Audit diagnostic self tests	□
Audit ACL connection failures	□
Audit Counter Value (decimal)	200317

In the General tab, user may enable auditing of the following events:

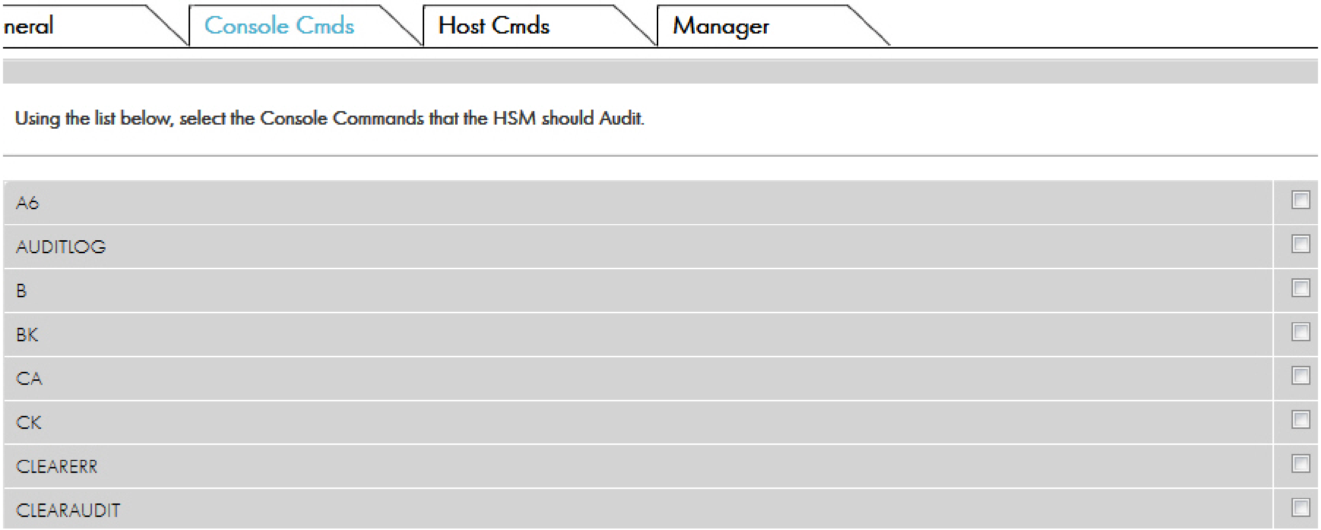
- User Actions
- Error Responses to Host Commands
- Utilization Data Resets
- Diagnostic Self Tests
- ACL Connection Failures

You may also set the audit counter value.

Note: Notification is provided when the audit log is 80%, 95% and 100% full.

Note: Typically, you do not audit commands that run all the time.

8.10.8.2 Audit - Console Commands

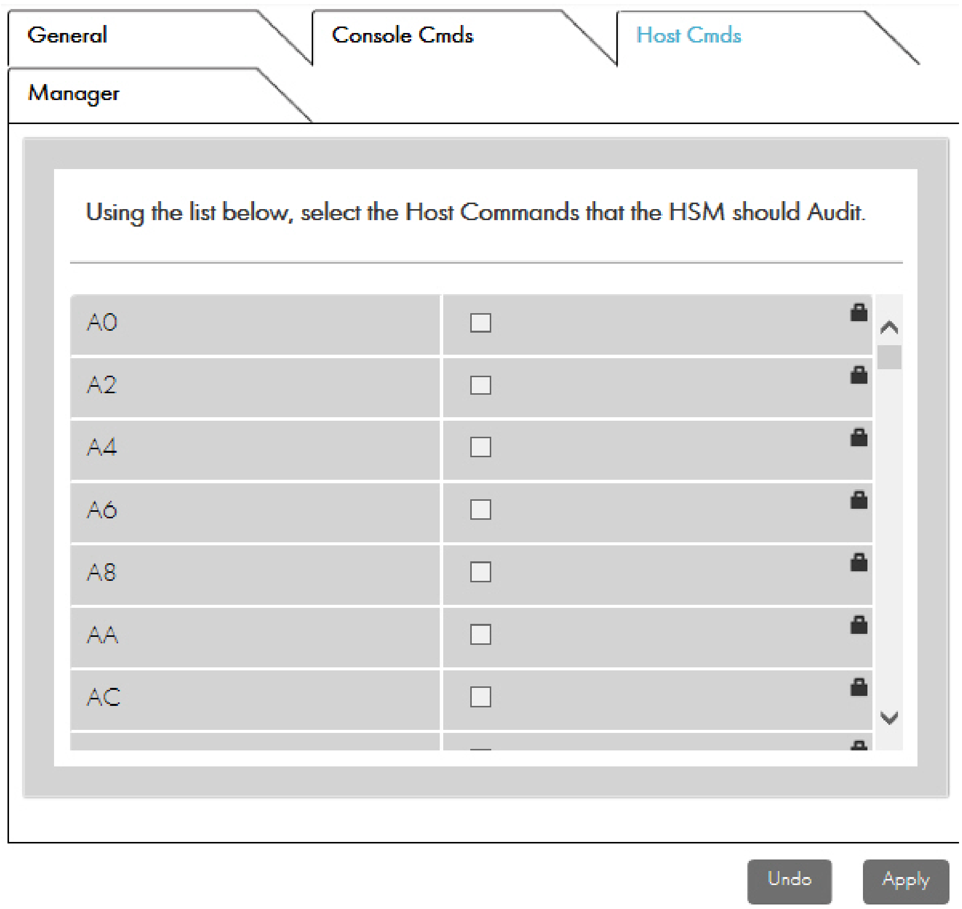


Using the list below, select the Console Commands that the HSM should Audit.

A6	□
AUDITLOG	□
B	□
BK	□
CA	□
CK	□
CLEARERR	□
CLEARAUDIT	□

It is possible to audit any of the console commands. Activities can be enabled or disabled by checking or unchecking the appropriate box(es). Checked items are enabled; unchecked items are disabled.

8.10.8.3 Audit - Host Commands

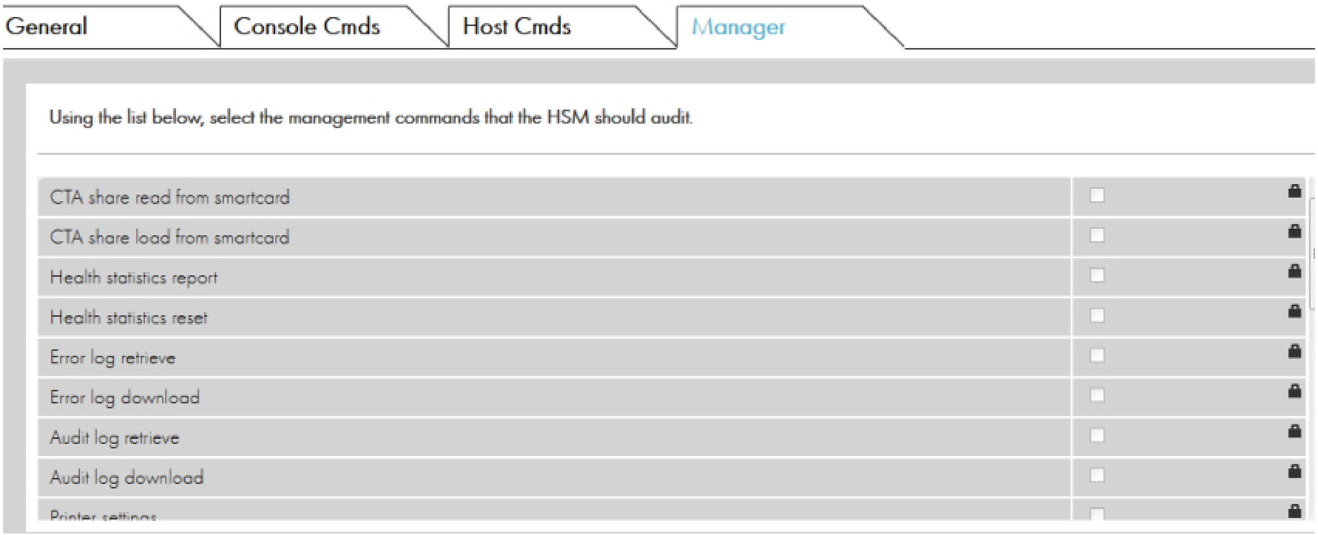


Using the list below, select the Host Commands that the HSM should Audit.

A0	□	🔒
A2	□	🔒
A4	□	🔒
A6	□	🔒
A8	□	🔒
AA	□	🔒
AC	□	🔒

It is possible to audit any of the Host commands available in the HSM's license. Activities can be enabled or disabled by checking or un-checking the appropriate box(es). Checked items are enabled; unchecked items are disabled.

8.10.8.4 Audit - Management Commands



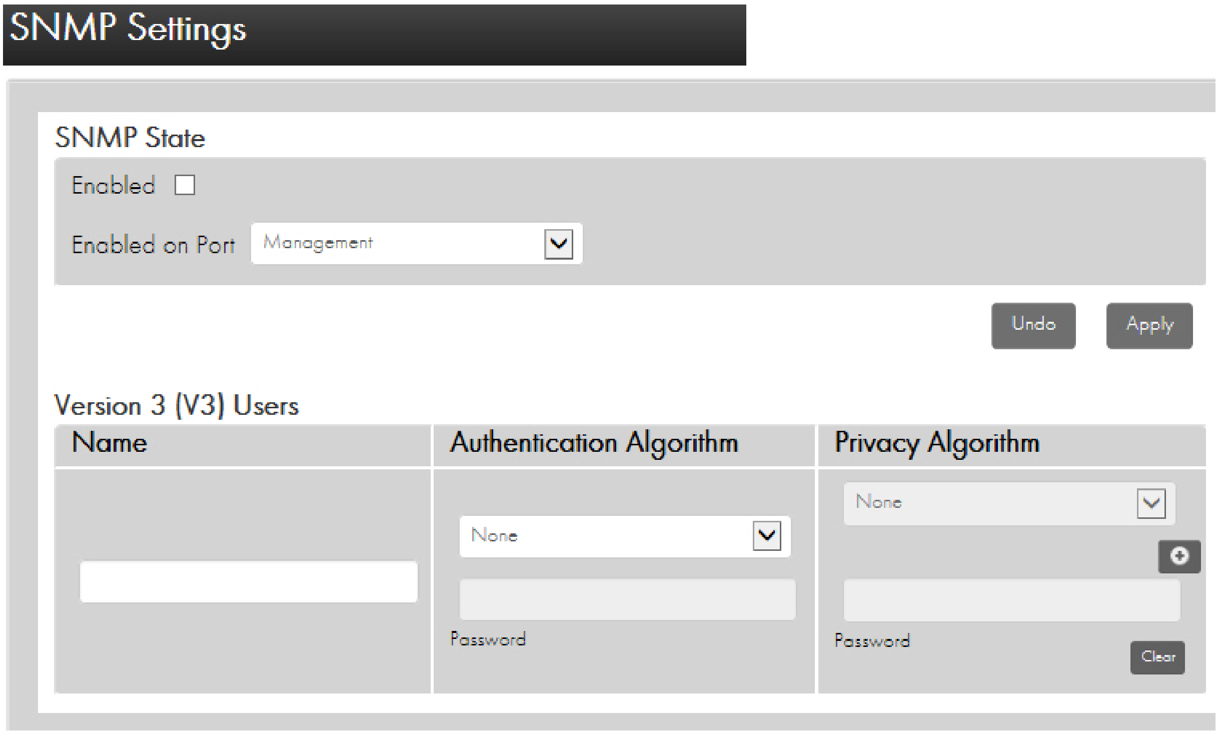
Using the list below, select the management commands that the HSM should audit.

CTA share read from smartcard	☐	🔒
CTA share load from smartcard	☐	🔒
Health statistics report	☐	🔒
Health statistics reset	☐	🔒
Error log retrieve	☐	🔒
Error log download	☐	🔒
Audit log retrieve	☐	🔒
Audit log download	☐	🔒
Printer settings	☐	🔒

In the Manager tab, you may enable auditing of all HSM Manager events, such as logins, state changes and configuration changes.

8.10.9 SNMP Settings

This section allows you to SNMP settings of the HSM when the unit is in any state.



SNMP Settings

SNMP State

Enabled □

Enabled on Port: Management

Version 3 (V3) Users

Name	Authentication Algorithm	Privacy Algorithm
	None Password	None Password

SNMP can be used to retrieve the following information on demand from the HSM:

– “Instantaneous” utilization data relating to HSM loading and Host command volumes.

– Current status of HSM health check factors.

Note: Only SNMP V3 is supported.

- SNMP State

  This section controls the state of the SNMP service using the following fields:

  – Enabled: Check this box to enable SNMP reporting, uncheck it to disable

  – Enabled on Port: Which Ethernet port to use for SNMP traffic

  – You must specify the authentication and privacy algorithms to be used.

  – To add a V3 user, enter the following fields and then click the plus icon:
    Name
    Authentication Algorithm (and password)
    Privacy Algorithm (and password)

– To delete a User, simply click the minus icon next to that user.

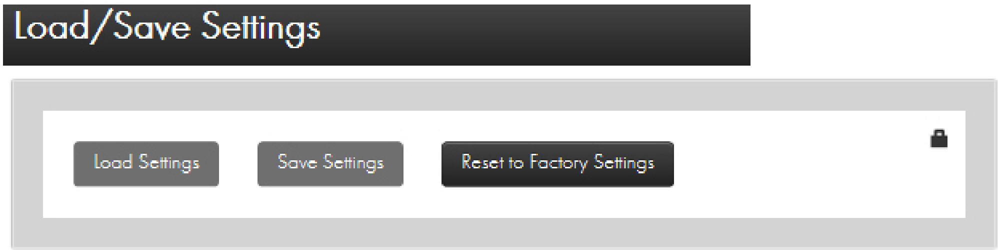
Note: SNMP MIB-2 system values corresponding to MIB2system values in console SNMP command (sysName, sysDescr, sysLocation, sysContact) can be set under **General Settings -> Miscellaneous** tab. Refer to "Section 8.10.6.5, “General - Miscellaneous”, on page 172".---

Table 6 *Port Settings*

Port	Protocol	Purpose
161	UDP	SNMP Requests - Utilization and Health Check data
162	UDP	SNMP Traps.

8.10.10 Load/Save Settings

In this section you can save the active configuration to a Smart Card, reload configuration data from a settings Smart Card, or reset the HSM to its Factory Default settings.

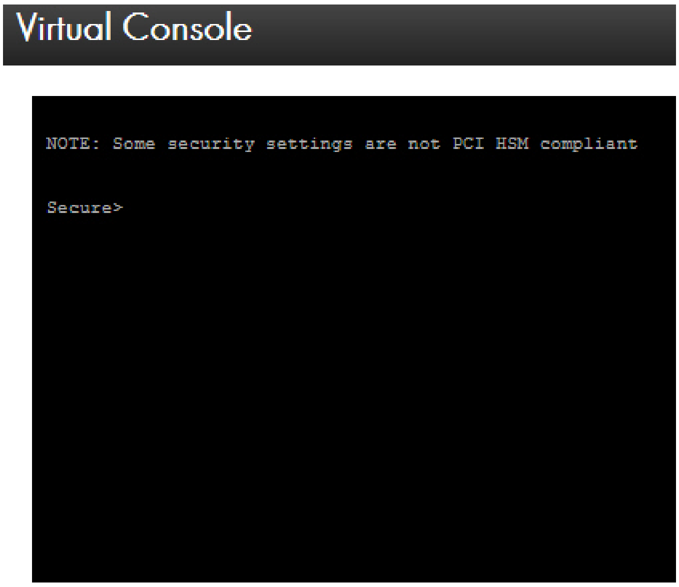


Saving your parameter settings allows you to make changes and then, if necessary, revert to your previous configuration.

Saving or restoring settings must be done in secure state with proper authorization. You may “Reset to Factory Settings” when in secure state.

8.11 Virtual Console

The virtual console provides a reduced set of command instructions. It works the same as the local console and all console operations are support with the exception of commands that may invoke the use of the HSM’s local facilities (e.g., the internal Smart Card reader).



```
NOTE: Some security settings are not PCI HSM compliant

Secure>
```

The following commands may not be used in the virtual console: A, CO, DC, EJECT, FC, GK, GS, LK, LO, NP, RC, RS, SS, VC, XA, XD, XE, XH, XI, XK, XR, XT, XX, and XZ.

Note: In the current implementation of the virtual console, a cursor may not be present. However, the virtual console is still active and functional.

9 Migrating LMKs

9.1 Introduction

Thales payment HSMs have always provided a facility to migrate between LMKs, for example, to re-encrypt operational keys and other data from encryption under one (old) LMK to encryption under another (new) LMK. The need to do this is more important than in the past because:

- Card schemes are requesting that customers change their master keys every 2 years
- Adoption of Key Block LMKs, with their added security, requires a migration from Variant LMKs

This chapter outlines the migration process.

9.2 Multiple LMKs

By default, the payShield 10K is delivered with the ability to install one or two LMKs. If two LMKs are installed, one must be a Variant type and one must be a Key Block type.

Each LMK can be managed by its own team of security officers.

The multiple LMK facility can be used to provide separation between multiple clients, applications, or purposes serviced on the same HSM, and they also make the process of migrating LMKs easier.

9.3 Overview of the process

The LMK Migration process takes keys which are encrypted under an old LMK and re-encrypts them under a new LMK. Both the old and the new LMKs must be installed in the payShield 10K.

There are two types of LMK storage:

- LMK Live storage.

  Transaction processing and other LMK functions can make use only of LMKs in Live storage.
- Key Change storage.

  LMKs in Key Change storage cannot be used for any purpose other than as part of the LMK migration process. Where multiple LMKs are deployed, there is one Key Change storage “slot” for each LMK in the Main storage.

There are 2 ways of allocating old/new keys to Main/Key Change storage:

- The new LMK (which has not yet been deployed for live operation) is loaded into Live storage, and the old LMK (which is still being used for live processing) is loaded into Key Change storage using the LO console command.

It means that the payShield 10K being used for migration cannot be used to process transactions until the LMK migration process is completed and the new LMK comes into operational use, but it is then immediately ready to process transactions because the new LMK is already loaded in Live storage.

- The old LMK (still being used for live operation but about to be obsoleted) is left in Main Live, and the new LMK (which has not yet been deployed for live operation) is loaded into Key Change storage using the LN console command.

  This option means that the payShield 10K can continue processing transactions using the current LMK at the same time as it is used for migrating keys to the new LMK. On the other hand, when the new LMK is ready to go live, the new LMK must be loaded into Live storage before any transactions can be processed.

At a high level, the steps to migrate an old LMK to a new LMK are as follows:

1. Create Smart Cards with components for the new LMK.
2. Load the new LMK (**from components cards**) into either LMK Live storage or LMK Key Change storage.

   Either:

   – leave the old LMK in LMK Live storage and load the new LMK (from component cards) into LMK Key Change storage

   or

   – load the new LMK (**from component cards**) into LMK Live storage and load the old LMK (from components cards) into LMK Key Change storage in the same HSM.
3. Re-encrypt the operational keys from the old LMK to the new LMK and hold these in a pending new key database.
4. Re-encrypt PINs from the old LMK to the new LMK and hold these in a pending new PIN database.
5. Re-encrypt decimalization tables from the old LMK to the new LMK and hold these in a pending new decimalization table database.
6. If the new LMKs have been loaded into Key Change storage, re-load them into Live storage.
7. Make the pending key/PIN/decimalization table databases the live databases.

9.4 Generating new LMK component Smart Cards

LMKs are set up in the payShield 10K by loading a number (typically 3) of components which are then combined within the HSM to form the LMK. (The formed LMK is never available outside of the HSM.) The LMK components are loaded from LMK Smart Cards.

The first stage, therefore, is to create Smart Cards which have the components for the new LMK. These components have completely random values, and are created on any payShield 10K.

Each component must be held by a different security officer, and access to the component cards must be securely controlled (e.g., by storing the card securely and requiring security officers to check the cards out and in).

All component cards are required to load (or form) an LMK, and so loss of any card or absence of a card holder prevents the LMK from being loaded (or re-loaded at a later date, if necessary). Therefore at least one backup should be made of each component card.

Note that the terms "LMK card" and "LMK component card" are interchangeable. Only LMK components are ever written to cards - the whole LMK is never written to a card.

9.4.1 Types of LMK component cards

There are two types of LMK component cards:

- HSM LMK cards - using the card reader built into the HSM. This type of card is created and used by operators using a console and the HSM card reader.
- payShield Manager RLMK cards - created by operators using payShield Manager and the card reader attached to the remote management PC.

The principles are the same for both types of card, although the detail of the processes is different. The two types of card are incompatible, although either type of card can be created from the other.

9.5 Formatting LMK Smart Cards

9.5.1 HSM LMK Cards

Before they can be written to, Smart Cards must be formatted.

Cards which have been used previously and are no longer required can be re-formatted to enable the new components to be written to them.

Do not re-format the component cards for the old LMK that you are about to migrate from.

Each component holder should format their own card plus at least one backup per component.

HSM LMK Smart Cards are formatted using the FC console command.

Follow this link for additional instruction: Appendix , “Console Commands”

9.5.2 payShield Manager LMK Cards

With payShield Manager, the LMK components are written to RLMK cards which are provided by Thales. RLMK cards do not require formatting.

9.6 Generating LMK Component Cards

9.6.1 HSM LMK Cards

Each component holder should now generate a component and write it to their Smart Card and backup card(s). This is done using the GK console command.

Follow this link for additional instruction: Appendix , “Console Commands”

Various warnings and errors may be reported during this process. These are easy to understand, and appropriate responses should be made.

9.6.2 payShield Manager RLMK Cards

LMK components for use with payShield Manager are written to RLMK cards using the Generate button in payShield Manager's **Operational > LMK Operations > Local Master Keys** tab.

These cards use a quorum (i.e., “m of n”) approach to define how many of the cards must be used when loading an LMK. The operator provides the following information when generating the LMK:

- Number of LMK shares, i.e. “n” (Default: 2)
- Number of shares to rebuild, i.e. “m” (Default: 2)
- Key scheme (Variant or Key Block)
- Algorithm
- Status (Live or Test)

9.7 Creating Copies of LMK Component Cards

Because all component cards are needed when the LMK is loaded, copies of each LMK card should be made to allow for misplacement or for issuing to deputies.

9.7.1 Duplicating HSM LMK cards

- During LMK card generation

  Multiple copies may be made at the time of generating the LMK card.

- Using a console command

  It is possible at any time to copy an existing HSM LMK card using the DC console command.

  Follow this link for additional instruction: Appendix , “Console Commands”

9.7.2 Duplicating a payShield Manager RLMK card

A copy of an existing RLMK component card can be made using the Duplicate button in payShield Manager's **Operational > LMK Operations > Local Master Keys** tab.

9.8 Loading the new LMK

In the previous sections, we explained how to create a set of cards containing the components for the new LMK. Each component is "owned" by a different security officer, with no one security officer having access to more than one component. One holder of each of the required number of components must be present to allow the LMK to be loaded onto the payShield 10K using the component Smart Cards.

The new LMK now needs to be installed into either LMK Live storage or LMK Key Change storage depending on the approach being taken.

The new LMK can be loaded using a Console or payShield Manager.

9.8.1 Using the Console

9.8.1.1 Loading (or forming) the LMK

The LMK is loaded using either:

- the LK console command if the new LMK is to be loaded into LMK Live storage, or
- the LN console command if the new LMK is to be loaded into LMK Key Change storage.

The payShield 10K must be in the Secure state. In addition, if the LN console command is being used, then the HSM must be in the Authorized state. If multiple authorized states is enabled, the activity category is admin (with no sub-category), and the console interface should be selected.

The Smart Cards used must be HSM cards - not cards created for payShield Manager.

9.8.1.2 Checking the LMK

It is recommended that a check is made that the new LMK has been properly loaded.

This can be done using the A console command, to put the HSM into authorized state (followed by the C command to cancel the authorized state). The A command can be run in any HSM state. The operation of this command depends on whether multiple authorized activities has been enabled in the security settings (e.g., by using the CS console command).

Follow this link for additional instruction: Appendix , "Console Commands"

9.8.2 Using payShield Manager

9.8.2.1 Installing the LMK

The new LMK is loaded using the Install button in the appropriate payShield Manager tab:

- **Operational > LMK Operations > Local Master Keys** where the new LMK is to be loaded into LMK Live storage, or
- **Operational > LMK Operations > Key Change Storage** where the new LMK is to be loaded into LMK Key Change storage.

The LMK ID will need to be specified.

9.8.2.2 Checking the LMK

The installed LMK can be checked by viewing the LMK list.

Navigate to either of the following:

- **Operational > LMK Operations > Local Master Keys**
- **Operational > LMK Operations > Key Change Storage**

9.9 Loading the old LMK

So far, you have created a set of cards containing the components for the new LMK, and used them to load into the HSM the “new” LMK that keys and data to be re-encrypted to.

To migrate keys from encryption under an old (current) LMK to encryption under the new LMK, we also need to have the old LMK loaded in the HSM. The old LMK can be left in LMK Lives storage or loaded into LMK Key Change Storage, depending on the approach being taken.

If the old LMK is to be loaded into Key Change Storage, this can be done using a Console or payShield Manager.

9.9.1 Using the Console

The old LMK is loaded into Key Change Storage using the LO console command.

Follow this link for additional instruction: Appendix , “Console Commands”

The payShield 10K must be in Secure state. In addition, the HSM must be in Authorized state. If multiple authorized states are enabled, the activity category is *admin* (with no sub-category), and the console interface should be selected.

The use of the LO console command is the same as for the LK console command mentioned previously, except that no existing LMK needs to be erased and so you will not be prompted to confirm an erasure.

After loading the old LMK, the HSM should be returned to Online state by turning the physical keys.

9.9.2 Using payShield Manager

The old LMK is loaded using the Install button in payShield Manager's **Operational > LMK Operations > Key Change Storage** tab. This can only be done if there is an LMK with the same ID in the LMK table.

9.10 Migrating keys between Variant LMKs

We now have installed in the HSM both the old LMK that the operational keys are currently encrypted under and the new LMK that they need to be encrypted under for the future. We now need to take each existing operational key in the old key database (encrypted under the old LMK), re-encrypt it using the new LMK, and put it in a new key database.

In order to do this, an application needs to be set up at the host that:

- Takes each operational key (encrypted under the old LMK) from the old key database
- Sends the encrypted key to the HSM using the BW host command.
- Receives the BX response from the HSM containing the operational key encrypted under the new LMK.
- Puts the operational key encrypted under the new LMK into the new key database.

9.10.1 BW Host command

This section examines the BW host command as it is used to convert an operational key encrypted under an old LMK of the Variant type to encryption under a new LMK of the Variant type.

The BW host command automatically adapts its processing depending on where the old and new LMKs are stored:

- If the old LMK was loaded into Key Change storage (e.g., the LO console command was used), then keys and data are re-encrypted from encryption under the (old) LMK in Key Change storage to encryption under the (new) LMK in Live storage.
- If the new LMK was loaded into Key Change storage (e.g., the LN console command was used), then keys and data are re-encrypted from encryption under the (old) LMK in Live storage to encryption under the (new) LMK in Key Change storage.

The table below indicates the structure of the BW host command when it is used in this way.

Field	Length & Type	Notes
Message Header	m A	This field contains whatever the user wants. The length of the field is defined using the *CH* console command or *Configuration / Host Settings* in payShield Manager. It is subsequently returned unchanged in the response to the host.
Command Code	2 A	Must have the value 'BW'.
Key Type code	2 H	Indicates the LMK under which the key is encrypted: '00' : LMK pair 04-05 (Key Type 000) '01' : LMK pair 06-07 (Key Type 001) '02' : LMK pair 14-15 (Key Type 002) '03' : LMK pair 16-17 (Key Type 003) '04' : LMK pair 18-19 (Key Type 004) '05' : LMK pair 20-21 (Key Type 005) '06' : LMK pair 22-23 (Key Type 006) '07' : LMK pair 24-25 (Key Type 007) '08' : LMK pair 26-27 (Key Type 008) '09' : LMK pair 28-29 (Key Type 009) '0A' : LMK pair 30-31 (Key Type 00A) '0B' : LMK pair 32-33 (Key Type 00B) '10' : Variant 1 of LMK pair 04-05 (Key Type 100) '42' : Variant 4 of LMK pair 14-15 (Key Type 402) 'FF' : Use this value where the key type is specified after the first ';' delimiter below. This allows key types other than those listed above to be specified.
Key length flag	1 N	'0' : for single-length key '1' : for double-length key '2' : for triple-length key.
Key	16/32 H or 1 A + 32/48 H	The operational key to be translated, encrypted under the old LMK.
Delimiter	1 A	Optional. Only present if 'FF' was supplied above for the Key Type code and the following field is present. Value ';'.
Key Type	3 H	Where 'FF' was entered for Key Type Code, this is the 3-digit key type code of the key being translated.
Delimiter	1 A	Optional. If present the following three fields must be present. Value ';'.
Reserved	1 A	Optional. If present must be '0' (zero).

Field	Length & Type	Notes
Key Scheme (LMK)	1 A	Optional. Key scheme for encrypting key under LMK (or '0' (zero).
Reserved	1 A	Optional. If present must be '0' (zero).
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	Where the user is using multiple LMKs on the same HSM, this allows the ID of the LMK being migrated to be selected. Minimum value = '00'; maximum value is defined by license. This field must be present if the above Delimiter is present. If the field is not present, then the default LMK will be used.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19'.
Message Trailer	n A	Optional. The contents of the trailer is as required by the user, and is returned unchanged in the response. Maximum length 32 characters.

9.10.2 BX Response to the Host

In response to the BW host command, the payShield 10K returns the following BX response to the host:

Field	Length & Type	Notes
Message Header	m A	This is a play-back of the header provided in the *BW* command.
Response Code	2 A	Has the value 'BX'.
Error code	2 N	Indicating the general outcome of the *BW* command: '00' : No error '04' : Invalid key type code '05' : Invalid key length flag '10' : Key parity error '44' : migration not allowed: key migration requested when the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y". '45' : Invalid key migration destination key type. '68' : Command disabled or any standard error code.
Key	16/32 H or 1 A + 32/48 H	The resulting key, re-encrypted under the new LMK.
End Message Delimiter	1 C	Present only if a message trailer is present. Value X'19'.
Message Trailer	n A	This is simply a play-back of any trailer included in the *BW* command.

9.11 Migrating keys from Variant to Key Block LMKs

Key Block LMKs provide additional security compared to Variant LMKs.

The BW host command already described for Variant LMK > Variant LMK migration can also be used for Variant LMK > Key Block LMK migration. When used for this purpose, the BW command and BX response are modified as indicated below.

Note that it is not possible to migrate from:

- Key Block LMKs to Variant LMKs.
- AES Key Block LMKs to TDES Key Block LMKs.

9.11.1 BW Host command

The table below indicates the structure of the BW host command when it is used to migrate from Variant-type LMKs to Key Block-type LMKs. Only the differences compared to Variant LMK > Variant LMK migration are described.

Field	Length & Type	Notes
Message Header	m A	*(As for Variant LMK ⇨ Variant LMK)*
Command Code	2 A	Must have the value 'BW'.
Key Type code	2 H	*(As for Variant LMK ⇨ Variant LMK)*
Key length flag	1 N	*(As for Variant LMK ⇨ Variant LMK)*
Key	16/32 H or 1 A + 32/48 H	*(As for Variant LMK ⇨ Variant LMK)*
Delimiter	1 A	*(As for Variant LMK ⇨ Variant LMK)*
Key Type	3 H	*(As for Variant LMK ⇨ Variant LMK)*
Delimiter	1 A	*(As for Variant LMK ⇨ Variant LMK)*
Reserved	1 A	*(As for Variant LMK ⇨ Variant LMK)*
Key Scheme (LMK)	1 A	*(As for Variant LMK ⇨ Variant LMK)*
Reserved	1 A	*(As for Variant LMK ⇨ Variant LMK)*
Delimiter	1 A	*(As for Variant LMK ⇨ Variant LMK)*
LMK Identifier	2 N	*(As for Variant LMK ⇨ Variant LMK)*
Delimiter	1 A	Must have value '#'

Field	Length & Type	Notes
Key Usage	2 A	The required key usage for the key encrypted under the Key Bock LMK. This information is included in the Key Block header and should be determined using the Key Usage Table. This field determines type of the operational key (e.g. RSA private key, BDK, ZEK), and enforces key separation.
Mode of Use	1 A	The required mode of use for the key encrypted under the Key Bock LMK. This information is included in the Key Block header, and should be determined using the Mode of Use Table. This field determines how the operational key can be used (e.g. encryption, decryption, MACing).
Key Version Number	2 N	A value from '00' to '99', for inclusion in the Key Block header. Determined by the user. '00' denotes that key versioning is not in use for this key.
Exportability	1A	The required exportability for the key encrypted under the Key Bock LMK. This information is included in the Key Block header, and should be determined using the Exportability Table. This field determines how the operational key can be exported (e.g. no export allowed, may only be exported as a Key Block).
Number of Optional Blocks	2 N	A value from '00' to '08', identifying how many optional data blocks the user wants to add into the Key Block Header. Optional data blocks are used to identify parameters (such as key validity dates, key status, algorithm). For a value greater than 0, the following three fields must be repeated for each optional block.
Optional Block Identifier	2 A	Note that the value 'PB' may not be used.
Optional Block Length	2H	The length in bytes of the optional block (including the Identifier and Length). A value of X'04' indicates that the block contains only the identifier and length, and so the next field would not be present.
Optional Data Block	N A	The payload of the optional data block.
End Message Delimiter	1 C	*(As for Variant LMK ⇨ Variant LMK)*
Message Trailer	n A	*(As for Variant LMK ⇨ Variant LMK)*

9.11.2 BX Response to the Host

In response to the BW host command, the payShield 10K returns the following BX response to the host:

	Length &	
Field	**Type**	**Notes**
Message Header	m A	*(As for Variant LMK ⇨ Variant LMK)*
Response Code	2 A	Has the value 'BX'. *(As for Variant LMK Variant LMK)*
Error code	2 N	*(As for Variant LMK ⇨ Variant LMK)*
Key	1 A + n A	The operational key, encrypted under the new Key Block LMK.
End Message Delimiter	1 C	*(As for Variant LMK ⇨ Variant LMK)*
Message Trailer	n A	*(As for Variant LMK ⇨ Variant LMK)*

9.12 Migrating keys between Key Block LMKs

Migration of operational keys between Key Block LMKs is supported in addition to the Variant LMK > Variant LMK and Variant LMK > Key Block LMK migrations already described. This section describes the BW host command when used for this purpose.

Note that it is not possible to migrate from:

- Key Block LMKs to Variant LMKs.
- AES Key Block LMKs to TDES Key Block LMKs.

9.12.1 BW Host command

The table below indicates the structure of the BW host command when it is used to migrate between Key Block-type LMKs.

Field	Length & Type	Notes
Message Header	m A	*(As for Variant LMK ⇨ Key Block LMK)*
Command Code	2 A	Must have the value 'BW'.
Key Type code	2 H	Must be set to 'FF'.
Key length flag	1 H	Must be set to 'F'.
Key	1 A + n A	The operational key to be translated, encrypted under the old Key Block LMK.
Delimiter	1 A	Must have value ';'.
Key Type	3 H	Must be set to 'FFF'.
Delimiter	1 A	*(As for Variant LMK ⇨ Key Block LMK)*
Reserved	1 A	*(As for Variant LMK ⇨ Key Block LMK)*
Key Scheme (LMK)	1 A	*(As for Variant LMK ⇨ Key Block LMK)*
Reserved	1 A	*(As for Variant LMK ⇨ Key Block LMK)*
Delimiter	1 A	*(As for Variant LMK ⇨ Key Block LMK)*
LMK Identifier	2 N	*(As for Variant LMK ⇨ Key Block LMK)*
Delimiter	1 A	*(As for Variant LMK ⇨ Key Block LMK)*
Key Usage	2 A	*(As for Variant LMK ⇨ Key Block LMK)*
Mode of Use	1 A	*(As for Variant LMK ⇨ Key Block LMK)*
Key Version Number	2 N	*(As for Variant LMK ⇨ Key Block LMK)*
Exportability	1A	*(As for Variant LMK ⇨ Key Block LMK)*

Field	Length & Type	Notes
Number of Optional Blocks	2 N	*(As for Variant LMK ⇨ Key Block LMK)*
Optional Block Identifier	2 A	*(As for Variant LMK ⇨ Key Block LMK)*
Optional Block Length	2H	*(As for Variant LMK ⇨ Key Block LMK)*
Optional Data Block	N A	*(As for Variant LMK ⇨ Key Block LMK)*
End Message Delimiter	1 C	*(As for Variant LMK ⇨ Key Block LMK)*
Message Trailer	n A	*(As for Variant LMK ⇨ Key Block LMK)*

9.12.2 BX Response to the Host

In response to the BW host command, the payShield 10K returns the following BX response to the host:

Field	Length & Type	Notes
Message Header	m A	*(As for Variant LMK ⇨ Key Block LMK)*
Response Code	2 A	Has the value 'BX'. *(As for Variant LMK Key Block LMK)*
Error code	2 N	*(As for Variant LMK ⇨ Key Block LMK)*
Key	1 A + n A	*(As for Variant LMK ⇨ Key Block LMK)*
End Message Delimiter	1 C	*(As for Variant LMK ⇨ Key Block LMK)*
Message Trailer	n A	*(As for Variant LMK ⇨ Key Block LMK)*

9.13 Migrating keys from Key Block to Variant LMKs

This migration is not permitted because Variant LMKs are not as strong as key block LMKs.

9.14 Migrating keys for PCI HSM compliance

When it is required to make a payShield 10K compliant with the requirements of the PCI PTS HSM security standard, it may be necessary to move some keys from Variant key type 002 (LMK pair 14-15, Variant 0) to other key types.

Although this can be done as a separate operation, it can be achieved at the same time as migrating between LMKs using the BW host command by entering 'F2' as the Key Type Code, and the desired destination key type in the Key Type field.

9.15 Re-encrypting PINs

Where PINs have been stored encrypted under the old LMK (in LMK Live storage or LMK Key Change storage) these will need to be re-encrypted using the new LMK (in LMK Key Change storage or LMK Live storage). This can be done by using the BG host command.

A host application will take each PIN from the old PIN database, re-encrypt it using the BG host command, and store the re-encrypted PIN into the new PIN database.

9.15.1 BG Host Command

The structure of the BG host command is as follows:

Field	Length & Type	Notes
Message Header	m A	This field contains whatever the user wants. The length of the field is defined using the *CH* console command or *Configuration / Host Settings* in payShield Manager. It is subsequently returned unchanged in the response to the host.
Command Code	2 A	Has the value 'BG'.
Account Number	12 N	The 12 right-most digits of the account number, excluding the check digit.
PIN	L_1 N Or L_1 H	The PIN encrypted under the old LMK, where L_1 is the old encrypted PIN length. L_1 N applies where PIN encryption algorithm A (Visa method) is specified in the security settings, and L_1 H applies where PIN encryption algorithm B (Racal method) is specified.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.

Field	Length & Type	Notes
LMK Identifier	2 N	Where the user is using multiple LMKs on the same HSM, this allows the required LMK to be selected. Minimum value = '00'; maximum value is defined by license. This field must be present if the above Delimiter (%) is present. If the field is not present, then the default LMK will be used.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19'.
Message Trailer	n A	Optional. The contents of the trailer is as required by the user, and is returned unchanged in the response. Maximum length 32 characters.

9.15.2 BH Response

The HSM returns the following BH response to the host's BG command:

Field	Length & Type	Notes
Message Header	m A	This is a play-back of the header provided in the *BG* command.
Response Code	2 A	Has the value 'BH'.
Error code	2 N	Indicating the general outcome of the *BG* command: '00' : No error '68' : Command disabled or any standard error code.
PIN	L_2 N Or L_2 H	The PIN encrypted under the new LMK, where L_2 is the new encrypted PIN length. L_2 N applies where PIN encryption algorithm A (Visa method) is specified in the security settings, and L_2 H applies where PIN encryption algorithm B (Racal method) is specified.
End Message Delimiter	1 C	Present only if a message trailer is present. Value X'19'.
Message Trailer	n A	This is simply a play-back of any trailer included in the BW command.

9.16 Re-encrypting decimalization tables

For security, it is recommended that decimalization tables be encrypted. They are encrypted under the LMK, and so will need to be re-encrypted when migrating to a new LMK.

This is achieved by having a host application which takes each decimalization table from the old decimalization table database and re-encrypting it under the new LMK using the LO host command (not to be confused with the LO console command discussed earlier!) and then storing it in a new decimalization table database. The new LMK can be in either Key Change storage or Live storage.

The structure of the LO host command is as follows:

Field	Length & Type	Notes
Message Header	m A	This field contains whatever the user wants. The length of the field is defined using the *CH* console command or *Configuration / Host Settings* in payShield Manager. It is subsequently returned unchanged in the response to the host.
Command Code	2 A	Most have the value 'LO'.
Decimalization Table (old LMK)	16 H	A decimalization table encrypted under the old LMK.
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	Where the user is using multiple LMKs on the same HSM, this allows the required LMK to be selected. Minimum value = '00'; maximum value is defined by license. This field must be present if the above Delimiter (%) is present. If the field is not present, then the default LMK will be used.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19'.
Message Trailer	n A	Optional. The contents of the trailer is as required by the user, and is returned unchanged in the response. Maximum length 32 characters.

The payShield 10K returns the following LP response to the host:

Field	Length & Type	Notes
Message Header	m A	This is a play-back of the header provided in the *LO* command.
Response Code	2 A	Has the value 'LP'.

Field	Length & Type	Notes
Error code	2 N	Indicating the general outcome of the *LO* command: '00' : No error '68' : Command disabled or any standard error code
Decimalisation Table (new LMK)	16 H	The decimalisation table encrypted under the new LMK.
End Message Delimiter	1 C	Present only if a message trailer is present. Value X'19'.
Message Trailer	n A	This is simply a play-back of any trailer included in the BW command.

9.17 Switching to the new LMK

Following the activities described above, the system is now in the following state:

- Old databases of operational keys, PINs, and decimalization tables, encrypted under the old LMK, are still being used for production.
- New databases of operational keys, PINs, and decimalization tables, encrypted under the new LMK are pending but not yet being used for production.
  - One or more HSMs may have been taken out of service in order to re-encrypt the operational keys, PINs, and decimalization tables.
  - These would be HSMs that have the old (current) LMK (which is still being used on other HSMs for production) loaded in Key Change Storage (e.g. by using the LO console command), and the new LMK (not yet in use for production work) in their Live storage.
  - In this case there are other HSMs with the old LMK in their Live storage, which are doing production work using keys, PINs, and decimalization tables in the old versions of the databases.
- Production host applications are still using the old databases of operational keys, PINs, and decimalization tables.

In order to start using the new LMK, the following changes must be synchronized:

- Host production applications start using the new databases of operational keys, PINs, and decimalization tables.
- If the re-encryption of keys was done on an HSM with the new LMK in Live storage, then this HSM is immediately ready to start processing transactions using the new LMK. However, the new LMK needs to be loaded into LMK Live storage on those HSMs that were processing transactions using the old LMK.
- On the other hand, if the re-encryption of keys was done on an HSM with the new LMK in Key Change storage, then the new LMK needs to be loaded into LMK Live storage on all the HSMs in the system.

A total interruption of service can be avoided by a gradual switchover from the old LMK to the new - but in this case the host applications must know whether an HSM is using the old or new LMK and must retrieve the key or data from the appropriate database.

The use of the Multiple LMK feature of the payShield 10K offers additional options, and is described in the following section.

9.18 Taking advantage of Multiple LMKs

The payShield 10K supports multiple concurrent LMKs. The base product allows the user to implement one Variant-type LMK and one Key Block-type LMK, and optional licenses are available to provide up to 20 LMKs in any combination of types.

The multiple LMK feature offers a number of valuable benefits, and provides additional flexibility to simplify the process.

Here is an example of how the multiple LMK feature can be used where the old (still Live) LMK is in LMK Key Change storage and the new (future) LMK is in LMK Live storage:

- Let us take as a starting point a production system which has the live LMK at LMK 00.
- LMK 00 is set up as the default LMK. This means that it is the LMK that is used by default in host commands where no LMK is identified: this provides backwards compatibility to applications developed before the multiple LMK facility was introduced.
- The future, new LMK is loaded as LMK 01 in LMK Live storage (see Loading the new LMK).
- The existing, "old" LMK, which is LMK 00 and is being used for production, is also loaded into LMK Key Change Storage for LMK 01 (see Loading the old LMK.)
- The BW, BG, and LO host commands can now be used to re-encrypt operational keys, PINs, and decimalization tables from the old LMK (which is in Key Change Storage, and also still in LMK 00 and therefore available for production) to the new LMK, which is loaded as LMK 01. This is achieved by setting the LMK Identifier in the host commands to a value of “01”. This must be preceded by a delimiter of “%”.
- When all of the operational keys, PINs, and decimalization tables have been re-encrypted under the new LMK, the host application can start using the new key database when one of the following actions have been taken:

  – The new LMK is re-loaded on the payShield 10K as LMK 00.

  Or

  – Host commands sent to the payShield 10K are amended to use LMK 01 by either:

  - Specifying the value "01" for the LMK identifier in host commands

  Or

  - Directing commands to the relevant TCP port.

The benefit of this approach is that there is no need to take one or more HSMs out of productive use while the LMK migration is being performed, and therefore the key migration using the BW host command can be spread over as many HSMs as desired.

Multiple LMKs could also be used to avoid a "big bang" switchover from old to new LMKs: with the old LMK in one Live storage slot and the new LMK in a second Live storage slot, individual elements of the system can be moved to the new LMK one at a time.

9.19 Clean-up after migration to a new LMK

9.19.1 Deleting the Old LMK from Key Change Storage

The LMK in Key Change Storage should be deleted once it is no longer needed. There are multiple ways of doing this.

9.19.1.1 Using the console

The LMK can be deleted from Key Change Storage using the DO console command. The payShield 10K must be in Secure state.

9.19.1.2 Using payShield Manager

The LMK is deleted using the ⚙button displayed against the LMK in payShield Manager's **Operational > LMK Operations > Key Change Storage** tab. This can only be done in Secure state.

9.19.1.3 Using a Host Command

The BS host command allows the host to erase the LMK in Key Change Storage. The structure of the command is given in the following table:

Field	Length & Type	Notes
Message Header	m A	This field contains whatever the user wants. The length of the field is defined using the *CH* console command or *Configuration / Host Settings* in payShield Manager. It is subsequently returned unchanged in the response to the host.
Command Code	2 A	Must have the value 'BS'.

Field	Length & Type	Notes
Delimiter	1 A	Value '%'. Optional; if present, the following field must be present.
LMK Identifier	2 N	Where the user is using multiple LMKs on the same HSM, this allows the host to select which Old LMK is to be deleted. Minimum value = '00'; maximum value is defined by license. This field must be present if the above Delimiter (%) is present. If the field is not present, then the default LMK will be used.
End Message Delimiter	1 C	Must be present if a message trailer is present. Value X'19'.
Message Trailer	n A	Optional. The contents of the trailer is as required by the user, and is returned unchanged in the response. Maximum length 32 characters.

The BT response has the following structure:

Field	Length & Type	Notes
Message Header	m A	This is a play-back of the header provided in the *BS* command.
Response Code	2 A	Has the value 'BT'.
Error code	2 N	Indicating the general outcome of the *BS* command: '00' : No error '68' : Command disabled or any standard error code
End Message Delimiter	1 C	Present only if a message trailer is present. Value X'19'.
Message Trailer	n A	This is simply a play-back of any trailer included in the BW command.

9.19.2 Deleting the New LMK

In Section 9.18, “Taking advantage of Multiple LMKs”, on page 202, one suggested approach requires the new LMK to be unloaded from a temporary LMK Identifier or location (where it was loaded to enable the migration of keys and data to take place) and loaded to the location where it is required for production work.

Section 9.8, “Loading the new LMK”, on page 187 explains how to load the LMK to the location it is desired, but in addition the LMK should be deleted from its temporary location. This can be done by from the both the console and via payShield Manager.

9.19.2.1 Console

LMK deletion is achieved using the DM console command. This command requires Secure state and authorization - in a multiple authorize state environment, the activity to be authorized is “**admin.console”**.

Note that the DM console command also deletes the relevant old key in Key Change Storage, avoiding the need to do this separately.

9.19.2.2 Using payShield Manager

The LMK is deleted using the ⚙button displayed against the LMK in payShield Manager's **Operational > LMK Operations > Local Master Keys** tab. This can only be done in Secure state.

Appendix A - Console Commands

The payShield 10K provides over 80 console commands.

All console commands are enabled by default.

Note: In contrast, all Host commands are disabled by default. Refer to the *payShield 10K Host Command Manual*.

- Enabling and disabling console commands:

  Command syntax:

  <+ or -> C <command code>

  Where:

  "+" enables and

  "-" disables

  You can use the wild card character (*) as character 1 or 2 of the <command code>.

  For example:

  * = all console commands

  S* = all console commands that begin with "S"

  Multiple commands can be issued with a cumulative effect.

  For example:

  -C* (disables all console commands)

  +CG* (enables all console commands beginning with "G"

Appendix Contents

Console Commands – Listed Alphabetically ... 212

Configuration Commands ... 216

Reset to Factory Settings (RESET) ... 217

Upload Software and Licenses (UPLOAD) ... 219

Configure Commands (CONFIGCMDS) ... 221

Configure PIN Block Formats (CONFIGPB) ... 223

Configure Security (CS) ... 225

View Security Configuration (QS) ... 234

Configure Host Port (CH) ... 239

View Host Port Configuration (QH) ... 242

Host Port Access Control List (ACL) Configuration (CONFIGACL) ... 245

Configure Printer Port (CP) ... 248

View Printer Port Configuration (QP) ... 251

Configure Management Port (CM) ... 253

View Management Port Configuration (QM) ... 255

Configure Auxiliary Port (CA) ... 256

View Auxiliary Port Configuration (QA) ... 258

Configure Alarms (CL) ... 259

View Alarm Configuration (QL) ... 260

View/Change Instantaneous Utilization Period (UTILCFG) ... 261

Suspend/Resume Collection of Utilization Data (UTILENABLE) ... 262

Suspend/Resume Collection of Health Check Counts (HEALTHENABLE) ... 263

View SNMP Settings (SNMP) ... 264

Add an SNMP User (SNMPADD) ... 265

Delete an SNMP User (SNMPDEL) ... 266

Configure SNMP Traps (TRAP) ... 267

Add a new SNMP Trap (TRAPADD) ... 268

Delete an SNMP Trap (TRAPDEL) ... 269

Fraud Detection Commands ... 270

Configure Fraud Detection (A5) ... 271

Re-enable PIN Verification (A7) ... 273

Diagnostic Commands ... 274

Diagnostic Test (DT) ... 275

View Software Revision Number (VR) ... 279

View Available Commands (GETCMDS) ... 281

Show Network Statistics (NETSTAT) ... 283

Test TCP/IP Network (PING) ... 285

Trace TCP/IP route (TRACERT) 286

View/Reset Utilization Data (UTILSTATS) 288

View/Reset Health Check Counts (HEALTHSTATS) 290

Local Master Keys 291

Types of LMKs 291

Multiple LMKs 291

LMK Commands 293

Generate LMK Component(s) (GK) 294

Load LMK (LK) 297

Load 'Old' LMK into Key Change Storage (LO) 303

Load 'New' LMK into Key Change Storage (LN) 307

Verify LMK Store (V) 311

Duplicate LMK Component Sets (DC) 312

Delete LMK (DM) 313

Delete 'Old' or 'New' LMK from Key Change Storage (DO) 314

View LMK Table (VT) 315

Generate Test LMK (GT) 318

Operational Commands 320

Authorization Commands 320

Enter the Authorized State (A) 321

Cancel the Authorized State (C) 323

Authorize Activity (A) 324

Cancel Authorized Activity (C) 334

View Authorized Activities (VA) 336

Logging Commands 337

Display the Error Log (ERRLOG) 338

Clear the Error Log (CLEARERR) 340

Display the Audit Log (AUDITLOG) 341

Clear the Audit Log (CLEARAUDIT) 343

Audit Options (AUDITOPTIONS) 344

Time and Date Commands 347

Query the Time and Date (GETTIME) 349

Set Time for Automatic Self-Tests (ST) 350

Settings, Storage and Retrieval Commands 351

Save HSM Settings to a Smartcard (SS) 352

Retrieve HSM Settings from a Smartcard (RS) 353

Key Management Commands 356

Generate Key Component (GC) 357

Generate Key and Write Components to Smartcard (GS) 360

Encrypt Clear Component (EC) 364

Form Key from Components (FK) ... 367
Generate Key (KG) ... 374
Import Key (IK) ... 378
Export Key (KE) ... 382
Generate a Check Value (CK) ... 386
Set KMC Sequence Number (A6) ... 388
Payment System Commands ... 389
Generate a Card Verification Value (CV) ... 390
Generate a VISA PIN Verification Value (PV) ... 392
Load the Diebold Table (R) ... 394
Encrypt Decimalization Table (ED) ... 396
Translate Decimalization Table (TD) ... 398
Generate a MAC on an IPB (MI) ... 400
Smartcard Commands ... 401
Format an HSM Smartcard (FC) ... 402
Create an Authorizing Officer Smartcard (CO) ... 404
Verify the Contents of a Smartcard (VC) ... 405
Change a Smartcard PIN (NP) ... 406
Read Unidentifiable Smartcard Details (RC) ... 407
Eject a Smartcard (EJECT) ... 408
DES Calculator Commands ... 409
Single-Length Key Calculator (N) ... 410
Double-Length Key Calculator ($) ... 411
Triple-Length Key Calculator (T) ... 412
payShield Manager Commands ... 413
Add a RACC to the whitelist (XA) ... 414
Decommission the HSM (XD) ... 415
Remove RACC from the whitelist (XE) ... 416
Commission the HSM (XH) ... 417
Generate Customer Trust Authority (XI) ... 418
Make an RACC left or right key (XK) ... 420
Commission a smartcard (XR) ... 421
Transfer existing LMK to RLMK (XT) ... 422
Decommission a smartcard (XX) ... 424
HSM commissioning status (XY) ... 425
Duplicate CTA share (XZ) ... 426
Secure Host Communications ... 427
Generate Certificate Signing Request (SG) ... 428
Import Certificate (SI) ... 431
Export HSM Certificate's Chain of Trust (SE) ... 433

View Installed Certificate(s) (SV) 435
Delete Installed Certificate(s) (SD) 438
Generate HRK (SK) 439
Change HRK Passphrase (SP) 440
Restore HRK (SL) 441
KMD Support Commands 442
Generate KTK Components (KM) 443
Install KTK (KN) 444
View KTK Table (KT) 445
Import Key encrypted under KTK (KK) 446
Delete KTK (KD) 447
Error Responses Excluded from Audit Log 448

Console Commands – Listed Alphabetically

Command	Function	Page
A	**Enter the Authorized State**	321
A	**Authorize Activity**	324
A5	**Configure Fraud Detection**	271
A6	**Set KMC Sequence Number**	388
A7	**Re-enable PIN Verification**	273
AUDITLOG	**Display the Audit Log**	341
AUDITOPTIONS	**Audit Options**	344
C	**Cancel the Authorized State**	323
C	**Cancel Authorized Activity**	334
CA	**Configure Auxiliary Port**	256
CH	**Configure Host Port**	239
CK	**Generate a Check Value**	386
CL	**Configure Alarms**	259
CLEARAUDIT	**Clear the Audit Log**	343
CLEARERR	**Clear the Error Log**	340
CM	**Configure Management Port**	253
CO	**Create an Authorizing Officer Smartcard**	404
CONFIGACL	**Host Port Access Control List (ACL) Configuration**	245
CONFIGCMDS	**Configure Commands**	221
CONFIGPB	**Configure PIN Block Formats**	223
CP	**Configure Printer Port**	248
CS	**Configure Security**	225
CV	**Generate a Card Verification Value**	390
DC	**Duplicate LMK Component Sets**	312
DM	**Delete LMK**	313
DO	**Delete 'Old' or 'New' LMK from Key Change Storage**	314
DT	**Diagnostic Test**	275

EC	**Encrypt Clear Component**	364
ED	**Encrypt Decimalization Table**	364
EJECT	**Eject a Smartcard**	408
ERRLOG	**Display the Error Log**	338
FC	**Format an HSM Smartcard**	402
FK	**Form Key from Components**	367
GC	**Generate Key Component**	357
GETCMDS	**View Available Commands**	281
GETTIME	**Query the Time and Date**	349
GK	**Generate LMK Component**	294
GS	**Generate Key and Write Components to Smartcard**	360
GT	**Generate Test LMK**	318
HEALTHENABLE	**Suspend/Resume Collection of Health Check Counts**	263
HEALTHSTAT	**View/Reset Health Check Counts**	290
IK	**Import Key**	378
KD	**Delete KTK**	447
KE	**Export Key**	382
KG	**Generate Key**	374
KK	**Import Key encrypted under KTK**	446
KM	**Generate KTK Components**	443
KN	**Install KTK**	444
KT	**View KTK Table**	445
LK	**Load LMK**	297
LO	**Load 'Old' LMK into Key Change Storage**	303
LN	**Load 'New' LMK into Key Change Storage**	307
MI	**Generate a MAC on an IPB**	400
N	**Single-Length Key Calculator**	410
NETSTAT	**Show Network Statistics**	283
NP	**Change a Smartcard PIN**	406
PING	**Test TCP/IP Network**	285

PV	**Generate a VISA PIN Verification Value**	392
QA	**View Auxiliary Port Configuration**	258
QH	**View Host Port Configuration**	242
QL	**View Alarm Configuration**	260
QM	**View Management Port Configuration**	255
QP	**View Printer Port Configuration**	251
QS	**View Security Configuration**	234
R	**Load the Diebold Table**	394
RC	**Read Unidentifiable Smartcard Details**	407
RESET	**Reset to Factory Settings**	217
RS	**Retrieve HSM Settings from a Smartcard**	353
SD	**Delete Installed Certificate(s)**	438
SE	**Export HSM Certificate's Chain of Trust**	433
SETTIME	**Set the Time**	348
SG	**Generate Certificate Signing Request**	428
SI	**Import Certificate**	431
SK	**Generate HRK**	439
SL	**Restore HRK**	441
SP	**Change HRK Passphrase**	440
SNMP	**View SNMP Settings**	264
SNMPADD	**Add an SNMP User**	265
SNMPDEL	**Delete an SNMP User**	266
SS	**Save HSM Settings to a Smartcard**	388
ST	**Set Time for Automatic Self-Tests**	350
SV	**View Installed Certificate(s)**	435
T	**Triple-Length Key Calculator**	412
TD	**Translate Decimalization Table**	398
TRACERT	**Trace TCP/IP route**	286
TRAP	**Configure SNMP Traps**	267
TRAPADD	**Add a new SNMP Trap**	268

TRAPDEL	**Delete an SNMP Trap**	269
UTILCFG	**View/Change Instantaneous Utilization Period**	261
UTLENABLE	**Suspend/Resume Collection of Utilization Data**	262
UTILSTATS	**View/Reset Utilization Data**	288
UPLOAD	**Upload Software and Licenses**	219
V	**Verify LMK Store**	311
VA	**View Authorized Activities**	336
VC	**Verify the Contents of a Smartcard**	405
VR	**View Software Revision Number**	279
VT	**View LMK Table**	315
XA	**Add a RACC to the whitelist**	414
XD	**Decommission the HSM**	415
XE	**Remove RACC from the whitelist**	416
XH	**Commission the HSM**	417
XI	**Generate Customer Trust Authority**	418
XK	**Make an RACC left or right key**	311
XR	**Commission a smartcard**	421
XT	**Transfer existing LMK to RLMK**	422
XX	**Decommission a smartcard**	424
XY	**HSM commissioning status**	425
XZ	**Duplicate CTA share**	426
$	**Double-Length Key Calculator**	411

Configuration Commands

The payShield 10K provides the following console commands to support configuration operations:

Command	Page
Reset to Factory Settings (RESET)	**217**
Upload Software and Licenses (UPLOAD)	**219**
Configure Commands (CONFIGCMDS)	**221**
Configure PIN Block Formats (CONFIGPB)	**223**
Configure Security (CS)	**225**
View Security Configuration (QS)	**234**
Configure Host Port (CH)	**239**
View Host Port Configuration (QH)	**242**
Host Port Access Control List (ACL) Configuration (CONFIGACL)	**245**
Configure Printer Port (CP)	**248**
View Printer Port Configuration (QP)	**251**
Configure Management Port (CM)	**253**
View Management Port Configuration (QM)	**255**
Configure Auxiliary Port (CA)	**256**
View Auxiliary Port Configuration (QA)	**258**
Configure Alarms (CL)	**259**
View Alarm Configuration (QL)	**260**
View/Change Instantaneous Utilization Period (UTILCFG)	**261**
Suspend/Resume Collection of Utilization Data (UTILENABLE)	**262**
Suspend/Resume Collection of Health Check Counts (HEALTHENABLE)	**263**
View SNMP Settings (SNMP)	**264**
Add an SNMP User (SNMPADD)	**265**
Delete an SNMP User (SNMPDEL)	**266**
Configure SNMP Traps (TRAP)	**267**
Add a new SNMP Trap (TRAPADD)	**268**
Delete an SNMP Trap (TRAPDEL)	**269**

Reset to Factory Settings (RESET)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **RESET**

Function: Returns the HSM to the state it was in when it was shipped from the factory, so that it can be securely taken out of service – e.g. for return to Thales for repair.
Any configuration changes (including port settings) that the customer has applied will be reversed, and any customer data and logs will be erased.
If the HSM is to be returned (e.g. after it has been repaired), a record of all the settings should be made before using this command such that the settings can be re-applied after the HSM's return.
This command also reports whether the HSM is currently configured as it left the factory.

Authorization:

- Authorization is not required.
- The HSM must be in the secure state.

Inputs:

- Confirmation that Reset is required.

Outputs:

- Whether HSM is currently in its factory default state.
- Confirmation of Reset.

Notes:

- This utility cannot reset firmware or licenses installed on the HSM. Therefore, after use of this facility, the HSM will still have the most recently installed firmware and license – which may be different from the firmware and license when the HSM was shipped from the factory.
- At the end of the reset process, the payShield 10K will automatically perform a restart. If the console does not display correctly after this, the payShield 10K should be restarted manually. Turn the unit off and then back on.

Example 1:

```
Secure> RESET <Return>

Reset HSM to factory settings? [Y/N]: Y <Return>

The unit is currently in its factory default state: NO

Resetting the unit will remove all customer data,
including logs, port settings, keys, etc.  This may cause
the console to stop functioning.

This operation should only be performed if this unit is
being
taken out of normal operation.

Do you want to reset to the factory default settings?
[Y/N]: Y <Return>

You selected Yes; please confirm to Proceed with reset?
[Y/N]: Y <Return>

Return to factory default state complete

The HSM will now reboot automatically. This console is
exiting due to: Terminated
```

Example 2:

```
Secure> RESET <Return>

Reset HSM to factory settings? [Y/N]: Y <Return>
The unit is currently in its factory default state: YES

Resetting the unit will remove all customer data,
including logs, port settings, keys, etc.  This may cause
the console to stop functioning.

This operation should only be performed if this unit is
being
taken out of normal operation.

Do you want to reset to the factory default settings?
[Y/N]: N <Return>

Secure>
```

Upload Software and Licenses (UPLOAD)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **UPLOAD**

Function: With this command, you can upload new software and new licenses from the console.

Authorization:
- Authorization is not required.
- The HSM must be in the secure state.

Inputs:
- New software load is available or new license is available.

Outputs:
- The software/license successfully loads.

Example 1:

```
Secure> UPLOAD <Return>

Please select one of the following options:
1) Software update
2) Install new license
Your selection: 1 <Return>
This operation will terminate your session and reboot the
payShield. Do you want to proceed? [Y/N]: Y <Return>

Attached USB Mass storage devices:
Ultra USB 3.0

The following update files are available:
1)      ps10k_update_1.pti
2)      ps10k_update_2.pti
Your selection (choose 0 to exit): 1 <Return>

The following update will be applied: ps10k_update_1.pti

Continue with update? [Y/N]: Y <Return>
Obtaining update package information , please wait...

***** New HSM software is currently being installed.
*****
***** Please do not remove power from the HSM. *****


***** Validating update package *****

***** Installing update package *****

***** New HSM software has been successfully installed.
*****

***** New HSM Software has been successfully installed.
*****

***** Unit will now reboot automatically. *****

Secure>
```

Example 2:

```
Secure> UPLOAD <Return>

Please select one of the following options:
1) Software update
2) Install new license
Your selection: 2 <Return>

Attached USB Mass storage devices:
Ultra USB 3.0

The following License files are available:
1)      C4665271228Q.licence
Your selection: 1 <Return>

Are you sure you want to install license
C4665271228Q.licence? [Y/N]: Y <Return>

***** New HSM License is currently being installed. *****
***** Please do not remove power from the HSM. *****


***** New HSM License has been successfully installed. *****
```

Configure Commands (CONFIGCMDS)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **CONFIGCMDS**

Function: To view the list of enabled host and console commands, and (if in secure state) to enable or disable host and console commands. All available commands are disabled by default.

Commands are enabled or disabled using the following syntax:

[+ or -] [C or H] [<Command Code>]

+ indicates that the specified command should be enabled.
- indicates that the specified command should be disabled.
C indicates that <Command Code> is a Console command.
H indicates that <Command Code> is a Host command.
<Command Code> is the command code to be enabled or disabled, and may contain the wildcard character '*'. If the first character is '*', then the second character is absent, and this matches all command codes of the specified type. If the second character is '*', then this matches all command codes of the specified type starting with the given first character.

Authorization: The HSM must be in the secure state to enable/disable host and console commands. The current status of enablement of host and console commands can be viewed in any state.

Inputs:

- List of host commands to enable.
- List of console commands to enable.
- List of host commands to disable.
- List of console commands to disable.

Outputs:

- Complete list of enabled host commands.
- Complete list of enabled console commands.

Errors:

- Invalid entry

Notes:

- When a disabled host command is invoked, error code 68 is returned.
- When a disabled console command is invoked, the message "Function undefined or not allowed" is displayed.

Example 1: *This example demonstrates the use of the **CONFIGCMDS** console command to view the list of enabled host and console commands.*

```
Online> CONFIGCMDS <Return>

List of enabled Host commands:
A0 A4 GG GY

List of enabled Console commands:
GC     GS     EC     FK

Online>
```

Example 2: *This example demonstrates the use of the **CONFIGCMDS** console command to enable one console command (DE) and disable one host command (A4).*

```
       Secure> CONFIGCMDS <Return>
```

```
List of enabled Host commands:
A0 A4 GG GY
List of enabled Console commands:
GC     GS     EC     FK
Enter command code (e.g. +CDE) or Q to Quit: +CDE
<Return>

List of enabled Host commands:
A0 A4 GG GY
List of enabled Console commands:
GC     GS     EC     FK     DE
Enter command code (e.g. +CDE) or Q to Quit: -HA4
<Return>

List of enabled Host commands:
A0 GG GY
List of enabled Console commands:
GC     GS     EC     FK     DE
Enter command code (e.g. +CDE) or Q to Quit: Q <Return>
Save COMMAND settings to smart card? [Y/N]: N <Return>

Secure>
```

Example 3:

*This example demonstrates the use of the **CONFIGCMDS** console command using the wildcard character '*' to disable all non-core host commands, and then enable just those host commands beginning with 'A'.*

```
Secure> CONFIGCMDS <Return>

List of enabled Host commands:
A0 A4 GG GY
List of enabled Console commands:
GC     GS     EC     FK
Enter command code (e.g. +CDE) or Q to Quit: -H* <Return>

List of enabled Host commands:
List of enabled Console commands:
GC     GS     EC     FK     DE
Enter command code (e.g. +CDE) or Q to Quit: +HA*
<Return>

List of enabled Host commands:
A0 A2 A4 A6 A8 AA AC AE AG AS AU AW AY
List of enabled Console commands:
GC     GS     EC     FK     DE
Enter command code (e.g. +CDE) or Q to Quit: Q <Return>
Save COMMAND settings to smart card? [Y/N]: Y <Return>

Insert card and press ENTER: <Return>
COMMAND settings saved to the smartcard.

Secure>
```

Configure PIN Block Formats (CONFIGPB)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **CONFIGPB**

Function: To view the list of enabled PIN block formats, and (if in secure state) to enable or disable individual PIN block formats.

Authorization: The HSM must be in the secure state to enable/disable PIN block formats. The current status of PIN Block format enablement can be viewed in any state.

Inputs:
- PIN block format identifier.

Outputs:
- List of enabled PIN block formats.

Errors:
- Invalid entry

Example 1: *This example demonstrates the use of the **CONFIGPB** console command to view the list of enabled PIN block formats.*

```
Online> CONFIGPB <Return>

List of enabled PIN Block formats:
01 – ISO 9564-1 & ANSI X9.8 format 0
05 – ISO 9564-1 format 1
35 – MasterCard Pay Now and Pay Later format
41 – Visa/Amex new PIN only format
42 – Visa/Amex new & old PIN format
47 – ISO 9564-1 & ANSI X9.8 format 3
48 – ISO 9564-1 PIN Block Format 4 (AES)

Online>
```

Example 2**:** *This example demonstrates the use of the **CONFIGPB** console command to enable the use of HSM PIN Block format 03.*

```
Secure> CONFIGPB <Return>

List of enabled PIN Block formats:
01 – ISO 9564-1 & ANSI X9.8 format 0
05 – ISO 9564-1 format 1
35 – MasterCard Pay Now & Pay Later format
41 – Visa/Amex new PIN only format
42 – Visa/Amex new & old PIN format
47 – ISO 9564-1 & ANSI X9.8 format 3
48 – ISO 9564-1 PIN Block Format 4 (AES)

Enter + or – followed by PIN Block format or Q to Quit:
+03 <Return>

List of enabled PIN Block formats:
01 – ISO 9564-1 & ANSI X9.8 format 0
03 – Diebold & IBM ATM format
05 – ISO 9564-1 format 1
35 – MasterCard Pay Now & Pay Later format
41 – Visa/Amex new PIN only format
42 – Visa/Amex new & old PIN format
```

```
47 – ISO 9564-1 & ANSI X9.8 format 3
48 – ISO 9564-1 PIN Block Format 4 (AES)

Enter + or – followed by PIN Block format or Q to Quit: Q
<Return>
Save PIN BLOCK settings to smart card? [Y/N]: Y <Return>

Insert card and press ENTER: <Return>
PIN BLOCK settings saved to the smartcard.

Secure>
```

Configure Security (CS)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **CS**

Function: To set the security configuration of the HSM and some processing parameters. CS converts all lower-case alpha values to upper case for display purposes, except for the Card issuer Password. Operation is menu-driven, as shown in the examples. The security settings can optionally be saved to a smartcard.

Authorization: The HSM must be in the secure state to run this command.

Inputs:

- PIN length [4-12]: a one or two-digit number in the range 4 to 12.
- Echo [oN/ofF]: N or F
- Atalla ZMK variant support [oN/ofF]: N or F
- Transaction key scheme: Racal, Australian or None? [R/A/N]: R or A or N
- User storage key length [S/D/T/V]: S, D, T, or V
- Display general information on payShield Manager Landing page? [Y/N]: Y or N
- Default LMK identifier [0-x]: Integer between 0 and x
- Management LMK identifier [0-x] : Integer between 0 and x
- Whether to erase the installed LMKs to enable the following settings to be changed.
- Select clear PINs? [Y/N]: Y or N
- Enable ZMK translate command? [Y/N]: Y or N
- Enable X9.17 for import? [Y/N]: Y or N
- Enable X9.17 for export? [Y/N]: Y or N
- Solicitation batch size [1-1024]: a one to four-digit number, range 1 to 1024.
- Single/double length ZMKs [S/D]: S or D
- Decimalization table Encrypted/Plaintext [E/P]: E
- Enable Decimalization Table Checks? [Y/N]: Y or N
- PIN encryption algorithm [A/B]: A or B
- Whether to use the default Card Issuer password or to enter a different value (of 8 alphanumeric printable characters).
- Authorized State required when importing DES key under RSA key? [Y/N]: Y or N
- Minimum HMAC verification length in bytes [5-64]: number, range 5-64
- Enable PKCS#11 import and export for HMAC keys? [Y/N]: Y or N
- Enable ANSI X9.17 import and export for HMAC keys? [Y/N]: Y or N
- Enable ZEK/TEK encryption of ASCII data or Binary data or None? [A/B/N]: A or B or N
- Restrict Key Check Values to 6 hex chars? [Y/N]: Y or N
- Enable multiple authorized activities? [Y/N]: Y or N
- Allow persistent authorized activities [Y/N]: Y or N
- Enable support for variable length PIN offset? [Y/N]: Y or N
- Enable weak PIN checking? [Y/N]: Y or N
- Enable PIN Block format 34 as output format for PIN translations to ZPK? [Y/N]: Y or N
- Enable translation of account number for LMK encrypted PINs [Y/N]: Y or N.
- Use HSM clock for date/time validation? [Y/N]: Y or N
- Additional padding to disguise key length? [Y/N] : Y or N
- Key export and import in trusted format only? [Y/N] : Y or N
- Protect MULTOS cipher data checksums? [Y/N] : Y or N
- Enable Key Scheme Tag 'X' (X9.17) for storing keys under LMK? [Y/N] : Y or N
- Enable use of Tokens in PIN Translation? [Y/N]: Y or N

- Enable use of Tokens in PIN Verification? [Y/N]: Y or N
- Allow Error light to be extinguished when viewing Error Log? [Y/N]: Y or N
- Ensure LMK Identifier in command corresponds with host port? [Y/N]: Y or N
- Ignore LMK ID in Key Block Header? [Y/N]: Y or N
- Enable import and export of RSA Private keys? [Y/N]: Y or N
- Prevent Single-DES keys masquerading as double or triple-length key? [Y/N]: Y or N
- Disable Single-DES? [Y/N]: Y or N
- Card/password authorization (local) [C/P]: C or P (Card or Password).
- Restrict PIN block usage for PCI HSM compliance? [Y/N]: Y or N.
- Enforce key type 002 separation for PCI HSM compliance [Y/N]: Y or N.
- Enforce Authorization Time Limit? [Y/N]: Y or N.
- Enforce Multiple Key Components? [Y/N]: Y or N.
- Enforce PCI HSMv3 Key Equivalence for Key Wrapping? [Y/N]: Y or N.
- Enforce minimum key strength of 1024-bits for QH verification? [Y/N]: Y or N.
- Enforce minimum key strength of 2048-bits for RSA? [Y/N]: Y or N.
- Save SECURITY settings to smartcard? [Y/N]: Y or N

Outputs:

- Prompts according to the settings chosen (see examples below).

Errors:

Invalid Entry
Card not formatted to save/retrieve HSM settings.
Attempt with another card? [Y/N]

Notes:

- For software versions which have been PCI HSM certified, in order to be PCI HSM compliant a number of security settings must have specific values as follows:
  - Disable Single-DES? – must be “Y”
  - Card/password authorization (local) – must be "C"
  - Restrict PIN block usage for PCI HSM compliance – must be "Y"
  - Enforce key type 002 separation for PCI HSM compliance –must be "Y"
  - Enforce Authorization Time Limit – must be "Y"
  - Enforce Multiple Key Components – must be "Y"
  - Enforce PCI HSMv3 Key Equivalence for Key Wrapping – must be “Y”
  - Enforce minimum key strength of 1024-bits for RSA signature verification – must be “Y”
  - Enforce minimum key strength of 2048-bits for RSA – must be “Y”
- Once all of these settings are at the PCI HSM compliant value, they cannot be changed unless the RESET command is used.
- If the value of the setting "Enforce key type 002 separation for PCI HSM compliance" is "Y", then:
  - Key Type Table 2 is in effect. If the setting has a value of "N", then the HSM is not being operated in a PCI HSM compliant manner and Key Type Table 1 is in effect.
  - The following Host commands are disabled: AA, AE, FC, FE, FG, HC, KA, OE

Example 1: *Erasing LMKs not selected by the user*

```
Secure> CS <Return>
PIN Length [4-12]: 8 <Return>
Echo [oN/ofF]: N <Return>
Atalla ZMK variant support [oN/ofF]: F <Return>
Transaction Key Scheme: Racal, Australian or None [R/A/N]: N
<Return>
User storage key length [S/D/T/V](SINGLE): <Return>
Display general information on payShield Manager Landing page?
[Y/N]: Y <Return>_
Default LMK identifier [0-4](0): <Return>
Management LMK identifier [0-4](0): <Return>

LMKs must be erased before remaining parameters can be set.

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

Save SECURITY settings to smartcard? [Y/N]: N <Return>
Secure>
```

Example 2: *Settings affecting PCI HSM compliance do not have compliant values. The user wishes to use the default card issuer password.*

```
Secure> CS <Return>

Please make a selection.  The current setting is in parentheses.
Press ENTER to keep the current setting.
PIN length [4-12](4): <Return>
Echo [oN/ofF](ON): <Return>92
Atalla ZMK variant support [oN/ofF](ON): <Return>
Transaction key scheme: Racal, Australian or None? [R/A/N](R):
<Return>
User storage key length [S/D/T/V](SINGLE): <Return>
Display general information on payShield Manager Landing page?
[Y/N]: Y <Return>_
Default LMK identifier [0-4](0): <Return>
Management LMK identifier [0-4](0): <Return>

LMKs must be erased before remaining parameters can be set

Erase LMKs? [Y/N]: Y <Return>
Enforce Atalla variant match to Thales key type? [Y/N](YES):
<Return>
Select clear PINs? [Y/N](YES): <Return>
Enable ZMK translate command? [Y/N](YES): <Return>
Enable X9.17 for import? [Y/N](YES): <Return>
Enable X9.17 for export? [Y/N](YES): <Return>
Solicitation batch size [1-1024](5): <Return>

Single/double length ZMKs [S/D](DOUBLE): <Return>
Decimalization table Encrypted/Plaintext [E/P](P): <Return>
Enable Decimalization Table Checks? [Y/N](YES): <Return>

PIN encryption algorithm [A/B](A): <Return>
Use default card issuer password [Y/N](YES): Y <Return>
Authorized State required when importing DES key under RSA key?
[Y/N](YES): <Return>
Minimum HMAC key length in bytes [5-64](10): <Return>
Enable PKCS#11 import and export for HMAC keys [Y/N](YES):
<Return>
Enable ANSI X9.17 import and export for HMAC keys [Y/N](YES):
<Return>
Enable ZEK/TEK encryption of ASCII data or Binary data or None?
[A/B/N] (N): <Return>
Restrict Key Check Values to 6 hex chars [Y/N](YES): <Return>
Enable multiple authorized activities [Y/N](NO): <Return>
Allow persistent authorized activities [Y/N](NO): <Return>
Enable support for variable length PIN offset [Y/N](NO): <Return>
Enable weak PIN checking [Y/N](YES): <Return>
Check new PINs using global list of weak PINs? [Y/N](YES):
<Return>
Check new PINs using local list of weak PINs? [Y/N](YES):
<Return>
Check new PINs using rules? [Y/N](YES): <Return>
Enable PIN Block Format 34 as output format
for PIN Translations to ZPK [Y/N](NO): <Return>
Enable translation of account number for LMK encrypted PINs
[Y/N](NO): <Return>
Use HSM clock for date/time validation? [Y/N](YES): <Return>
Additional padding to disguise key length? [Y/N](NO): <Return>
```

```
Key export and import in trusted format only? [Y/N](NO): <Return>
Protect MULTOS cipher data checksums? [Y/N](YES): <Return>
Enable Key Scheme Tag 'X' (X9.17) for storing keys under LMK?
[Y/N](NO): <Return>
Enable use of Tokens in PIN Translation? [Y/N](NO): <Return>
Enable use of Tokens in PIN Verification? [Y/N](NO): <Return>
Ensure LMK Identifier in command corresponds with host port?
[Y/N](NO):
Ignore LMK ID in Key Block Header? [Y/N](NO):
Enable import and export of RSA Private keys? [Y/N](NO):

The following settings affect PCI HSM compliance:
Prevent single-DES keys masquerading
as double or triple-length key? [Y/N](YES):
The following setting is not PCI HSM compliant:
Disable Single-DES? [Y/N](NO):
Card/password authorization (local) [C/P](C):
Restrict PIN block usage for PCI HSM compliance? [Y/N](YES):
The following setting is not PCI HSM compliant:
Enforce key type 002 separation for PCI HSM compliance?
[Y/N](NO):
Enforce Authorization Time Limit? [Y/N](YES):
The following setting is not PCI HSM compliant:
Enforce Multiple Key Components? [Y/N](NO):
The following setting is not PCI HSM compliant:
Enforce PCI HSMv3 Key Equivalence for Key Wrapping? [Y/N](NO):
The following setting is not PCI HSM compliant:
Enforce minimum key strength of 1024-bits for RSA signature
verification? [Y/N](NO):
The following setting is not PCI HSM compliant:
Enforce minimum key strength of 2048-bits for RSA? [Y/N](NO):
Save SECURITY settings to smartcard? [Y/N]:
Secure>
```

Example 3: *Final setting affecting PCI HSM compliance is about to be set to compliant value. The user is specifying a different card issuer software.*

```
Secure> CS <Return>

Please make a selection.  The current setting is in parentheses.
Press ENTER to keep the current setting.
PIN length [4-12](4): <Return>
Echo [oN/ofF](ON): <Return>
Atalla ZMK variant support [oN/ofF](ON): <Return>
Transaction key scheme: Racal, Australian or None? [R/A/N](R):
<Return>
User storage key length [S/D/T/V](SINGLE): <Return>
Display general information on payShield Manager Landing page?
[Y/N]: Y <Return>
Default LMK identifier [0-4](0): <Return>
Management LMK identifier [0-4](0): <Return>

LMKs must be erased before remaining parameters can be set

Erase LMKs? [Y/N]: Y <Return>
Select clear PINs? [Y/N](YES): <Return>
Enable ZMK translate command? [Y/N](YES): <Return>
Enable X9.17 for import? [Y/N](YES): <Return>
Enable X9.17 for export? [Y/N](YES): <Return>
Solicitation batch size [1-1024](5): <Return>

Single/double length ZMKs [S/D](DOUBLE): <Return>
Decimalization table Encrypted/Plaintext [E/P](P): <Return>
Enable Decimalization Table Checks? [Y/N](YES): <Return>

PIN encryption algorithm [A/B](A): <Return>
Use default card issuer password [Y/N](YES): N <Return>
Enter card issuer password (local):***** <Return>
Password must be 8 characters.
Enter card issuer password (local):******** <Return>
Confirm card issuer password: ******** <Return>
Authorized State required when importing DES key under RSA key?
[Y/N](YES): <Return>
Minimum HMAC key length in bytes [5-64](10): <Return>
Enable PKCS#11 import and export for HMAC keys [Y/N](YES):
<Return>
Enable ANSI X9.17 import and export for HMAC keys [Y/N](YES):
<Return>
Enable ZEK/TEK encryption of ASCII data or Binary data or None?
[A/B/N] (N): <Return>
Restrict Key Check Values to 6 hex chars [Y/N](YES): <Return>
Enable multiple authorized activities [Y/N](NO): <Return>
Allow persistent authorized activities [Y/N](NO): <Return>
Enable support for variable length PIN offset [Y/N](NO): <Return>
Enable weak PIN checking [Y/N](YES): <Return>
Enable PIN Block Format 34 as output format for PIN Translations
to ZPK [Y/N](NO): <Return>
Enable translation of account number for LMK encrypted PINs
[Y/N](YES): <Return>
Use HSM clock for date/time validation? [Y/N](YES): <Return>
Additional padding to disguise key length? [Y/N](NO): <Return>
Key export and import in trusted format only? [Y/N](NO): <Return>
Protect MULTOS cipher data checksums? [Y/N](YES): <Return>
Enable Key Scheme Tag 'X' (X9.17) for storing keys under LMK?
```

```
[Y/N](NO): <Return>
Enable use of Tokens in PIN Translation? [Y/N](NO): <Return>
Enable use of Tokens in PIN Verification? [Y/N](NO): <Return>
Allow Error light to be extinguished when viewing Error Log?
[Y/N](NO): <Return>
Ensure LMK Identifier in command corresponds with host port?
[Y/N](NO): <Return>
Ignore LMK ID in Key Block Header? [Y/N](NO): <Return>
Enable import and export of RSA Private keys? [Y/N](NO): <Return>

The following settings affect PCI HSM compliance - see Console
Reference Manual:
Prevent single-DES keys masquerading as double or triple-length
key? [Y/N](YES): <Return>

Disable Single-DES? [Y/N](YES): <Return>

Card/password authorization (local) [C/P](C): <Return>

The following setting is not PCI HSM compliant:
Restrict PIN block usage for PCI HSM compliance? [Y/N](NO): Y
<Return>

The following setting is not PCI HSM compliant:
Enforce key type 002 separation for PCI HSM compliance?
[Y/N](NO): Y <Return>

Enforce Authorization Time Limit? [Y/N](YES): <Return>

Enforce Multiple Key Components? [Y/N](YES): <Return>

Enforce PCI HSMv3 Key Equivalence for Key Wrapping? [Y/N](YES):
<Return>

Enforce minimum key strength of 1024-bits for RSA signature
verification? [Y/N](YES): <Return>

Enforce minimum key strength of 2048-bits for RSA? [Y/N](YES):
<Return>

These settings will all become PCI HSM compliant.
No further changes will be allowed to these options:
 Prevent single-DES keys masquerading as double or triple-length
key: YES
 Single-DES: DISABLED
 Card/password authorization (local): C
 Restrict PIN block usage for PCI HSM Compliance: YES
 Enforce key type separation for PCI HSM compliance: YES
 Enforce Authorization Time Limit: YES
 Enforce Multiple Key Components: YES
 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

Confirm? [Y/N]: Y <Return>

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

```
Secure>
```

Example 4: *All settings affecting PCI HSM compliance have compliant values*

```
Secure> CS <Return>

Please make a selection.  The current setting is in parentheses.
Press ENTER to keep the current setting.
PIN length [4-12](4): <Return>
Echo [oN/ofF](ON): <Return>
Atalla ZMK variant support [oN/ofF](ON): <Return>
Transaction key scheme: Racal, Australian or None? [R/A/N](R):
<Return>
User storage key length [S/D/T/V](SINGLE): <Return>
Display general information on payShield Manager Landing page?
[Y/N]: Y <Return>
Default LMK identifier [0-4](0): <Return>
Management LMK identifier [0-4](0): <Return>
LMKs must be erased before remaining parameters can be set

Erase LMKs? [Y/N]: Y <Return>
Select clear PINs? [Y/N](YES): <Return>
Enable ZMK translate command? [Y/N](YES): <Return>
Enable X9.17 for import? [Y/N](YES): <Return>
Enable X9.17 for export? [Y/N](YES): <Return>
Solicitation batch size [1-1024](5): <Return>

Single/double length ZMKs [S/D](DOUBLE): <Return>
Decimalization table Encrypted/Plaintext [E/P](P): <Return>
Enable Decimalization Table Checks? [Y/N](YES): <Return>

PIN encryption algorithm [A/B](A): <Return>
Use default card issuer password [Y/N](YES): Y <Return>
Authorized State required when importing DES key under RSA key?
[Y/N](YES): <Return>
Minimum HMAC key length in bytes [5-64](10): <Return>
Enable PKCS#11 import and export for HMAC keys [Y/N](YES):
<Return>
Enable ANSI X9.17 import and export for HMAC keys [Y/N](YES):
<Return>
Enable ZEK/TEK encryption of ASCII data or Binary data or None?
[A/B/N] (N): <Return>
Restrict Key Check Values to 6 hex chars [Y/N](YES): <Return>
Enable multiple authorized activities [Y/N](NO): <Return>
Allow persistent authorized activities [Y/N](NO): <Return>
Enable support for variable length PIN offset [Y/N](NO): <Return>
Enable weak PIN checking [Y/N](YES): <Return>
Enable PIN Block Format 34 as output format for PIN Translations
to ZPK [Y/N](NO): <Return>
Enable translation of account number for LMK encrypted PINs
[Y/N](YES): <Return>
Use HSM clock for date/time validation? [Y/N](YES): <Return>
Additional padding to disguise key length? [Y/N](NO): <Return>
Key export and import in trusted format only? [Y/N](NO): <Return>
Protect MULTOS cipher data checksums? [Y/N](YES): <Return>
Enable Key Scheme Tag 'X' (X9.17) for storing keys under LMK?
[Y/N](NO): <Return>
Enable use of Tokens in PIN Translation? [Y/N](NO): <Return>
Enable use of Tokens in PIN Verification? [Y/N](NO): <Return>
Allow Error light to be extinguished when viewing Error Log?
[Y/N](NO): <Return>
Ensure LMK Identifier in command corresponds with host port?
[Y/N](NO): <Return>
Ignore LMK ID in Key Block Header? [Y/N](NO): <Return>
Enable import and export of RSA Private keys? [Y/N](NO): <Return>

The following settings are all PCI HSM compliant and cannot be
changed.
 Prevent single-DES keys masquerading as double or triple-length
key: YES
 Single-DES: DISABLED
 Card/password authorization (local): C
 Restrict PIN block usage for PCI HSM Compliance: YES
 Enforce key type separation for PCI HSM compliance: YES
 Enforce Authorization Time Limit: YES
 Enforce Multiple Key Components: YES
 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
Save SECURITY settings to smartcard? [Y/N]: Y <Return>
Insert card and press ENTER: <Return>
SECURITY settings saved to the smartcard.
Secure>
```

View Security Configuration (QS)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **QS**

Function: Reports the security configuration of the HSM and some processing parameters, plus the LMK check value.

Authorization: This command does not require any authorization.

Inputs: None.

Outputs:

- See examples below.

Errors: None.

Notes:

- Where the software has been PCI HSM certified, in order to be PCI HSM compliant a number of security settings must have specific values as follows:
  - Disable Single-DES? – must be “Y”
  - Card/password authorization (local) – must be "C"
  - Restrict PIN block usage for PCI HSM compliance – must be "Y"
  - Enforce key type 002 separation for PCI HSM compliance –must be "Y"
  - Enforce Authorization Time Limit – must be "Y"
  - Enforce Multiple Key Components – must be "Y"
  - Enforce PCI HSMv3 Key Equivalence for Key Wrapping – must be “Y”
  - Enforce minimum key strength of 1024-bits for RSA signature verification – must be “Y”
  - Enforce minimum key strength of 2048-bits for RSA – must be “Y”
- Once all of these settings are at the PCI HSM compliant value, they cannot be changed unless the RESET command is used.

Example 1: *Settings affecting PCI HSM compliance do not all have compliant values*

```
Online> QS <Return>

PIN length: 04
Encrypted PIN length: 05
Echo: OFF
Atalla ZMK variant support: OFF
Transaction key support: NONE
User storage key length: SINGLE
Display general information on payShield Manager Landing Page:
NO
Default LMK identifier: 00
Management LMK identifier: 00

Select clear PINs: NO
Enable ZMK translate command: NO
Enable X9.17 for import: NO
Enable X9.17 for export: NO
Solicitation batch size: 1024
ZMK length: DOUBLE
Decimalization tables: ENCRYPTED
Decimalization table checks: ENABLED
PIN encryption algorithm: A

Press "Enter" to view additional security settings... <Return>

Authorized state required when importing DES key under RSA key:
YES
Minimum HMAC length in bytes: 10
Enable PKCS#11 import and export for HMAC keys: NO
Enable ANSI X9.17 import and export for HMAC keys: NO
Enable ZEK/TEK encryption of ASCII data or Binary data or None:
NONE
Restrict key check values to 6 hex chars: YES
Enable multiple authorized activities: YES
Allow persistent authorized activities: NO
Enable variable length PIN offset: NO
Enable weak PIN checking: NO
Enable PIN block Format 34 as output format for PIN
translations to ZPK: NO
Enable translation of account number for LMK encrypted PINs: NO

Use HSM clock for date/time validation: YES
Additional padding to disguise key length: NO
Key export and import in trusted format only: YES
Protect MULTOS cipher data checksums: YES
Enable Key Scheme Tag 'X' (X9.17) for storing keys under LMK:
NO
Enable use of Tokens in PIN Translation: NO
Enable use of Tokens in PIN Verification: NO
Allow Error light to be extinguished when viewing Error Log: NO
Ensure LMK Identifier in command corresponds with host port: NO
Ignore LMK ID in Key Block Header: NO
Enable import and export of RSA Private keys: NO

NOTE: The following settings are not all PCI HSM compliant.
Prevent single-DES keys masquerading as double or triple-length
keys: YES
Single-DES: DISABLED
```

```
Card/password authorization (local): C
Restrict PIN block usage for PCI HSM Compliance: NO
Enforce key type 002 separation for PCI HSM compliance: NO
Enforce Authorization Time Limit: YES
Enforce Multiple Key Components: YES
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

Online>
```

Example 2: *Settings affecting PCI HSM compliance have compliant values*

```
Online> QS <Return>
PIN length: 04
Encrypted PIN length: 05
Echo: OFF
Atalla ZMK variant support: OFF
Transaction key support: NONE
User storage key length: SINGLE
Display general information on payShield Manager Landing Page:
NO
Default LMK identifier: 00
Management LMK identifier: 00
Select clear PINs: NO
Enable ZMK translate command: NO
Enable X9.17 for import: NO
Enable X9.17 for export: NO
Solicitation batch size: 1024
ZMK length: DOUBLE
Decimalization tables: ENCRYPTED
Decimalization table checks: ENABLED
PIN encryption algorithm: A
Press "Enter" to view additional security settings... <Return>
Authorized state required when importing DES key under RSA key:
YES
Minimum HMAC length in bytes: 10
Enable PKCS#11 import and export for HMAC keys: NO
Enable ANSI X9.17 import and export for HMAC keys: NO
Enable ZEK/TEK encryption of ASCII data or Binary data or None:
NONE
Restrict key check values to 6 hex chars: YES
Enable multiple authorized activities: YES
Allow persistent authorized activities: NO
Enable variable length PIN offset: NO
Enable weak PIN checking: NO
Enable PIN block Format 34 as output format for PIN
translations to ZPK: NO
Enable translation of account number for LMK encrypted PINs: NO
Use HSM clock for date/time validation: YES
Additional padding to disguise key length: NO
Key export and import in trusted format only: YES
Protect MULTOS cipher data checksums: YES
Enable Key Scheme Tag 'X' (X9.17) for storing keys under LMK:
NO
Enable use of Tokens in PIN Translation: NO
Enable use of Tokens in PIN Verification: NO
Allow Error light to be extinguished when viewing Error Log: NO
Ensure LMK Identifier in command corresponds with host port: NO
Ignore LMK ID in Key Block Header: NO
Enable import and export of RSA Private keys: NO
The following settings are all PCI HSM compliant and cannot be
changed:
Prevent single-DES keys masquerading as double or triple-length
keys: YES
Single-DES: DISABLED
Card/password authorization (local): C
Restrict PIN block usage for PCI HSM Compliance: YES
Enforce key type 002 separation for PCI HSM compliance: YES
Enforce Authorization Time Limit: YES
Enforce Multiple Key Components: YES
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
Online>
```

Configure Host Port (CH)

Variant ☑		Key Block ☑
Online ☒	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **CH**

Function: To configure the Host port to emulate a type of data communications equipment and control equipment, i.e., Ethernet.

The Host port setting can optionally be saved to a smartcard.
The new settings come into effect a few seconds after the command has completed.

Authorization:

- The HSM must be in the offline or secure state to run this command.
- If settings relating to Secure Host Communications (TLS) or Access Control Lists are to be changed, the payShield 10K must be in Secure state.

Inputs:

- The options are menu driven and the inputs vary depending on the communication mode selected. See examples below.

Outputs: None.

Notes:

- To achieve maximum throughput on the HSM, the TCP/IP interfaces need to be driven with multiple connections (or threads). Optimum performance is normally achieved with 4 - 8 connections (depending on the HSM performance model and the commands being processed). Running with only a single thread can significantly reduce the throughput of the HSM, and means that you will not be able to reach the rated throughput for the machine.
- It is recommended that the Host Ethernet Ports, the Management Ethernet Port, and the Auxiliary Ethernet Port are all on different IP subnets from each other.
- Where dual Ethernet host ports are in use, 2 different IP addresses at the Host computer must be used to drive the 2 ports on the HSM.
- The use of TLS v1.2 is supported on the payShield 10K:
  - o TLS traffic can be supported at the same time as non-TLS traffic.
  - o The specified number of connections are shared between TLS and non-TLS traffic.
  - o The HSM can be forced to accept only TLS traffic by setting the *UDP* and *TCP* options to "*N*".

  For Ethernet communications (not protected by TLS), a Well-Known Port Address is defined (default value 1500).
- If TLS is enabled, a Well-Known Port Address is also required (default value 2500). This works in the same way as the Well-Known Port Address for non-TLS traffic.

Errors: None.

Example 1: *In this example, Ethernet communications using TCP/IP and TLS are selected – all types of traffic are allowed. The IP addresses are set up as static, manually-entered addresses. Access Control Lists are to be used, and will be set up using the CONFIGACL console command. Secure state is required to change TLS or ACL settings.*

```
       Secure> CH <Return>

Please make a selection.  The current setting is in
parentheses.
Message header length [1-255] (4): <Return>
Disable host connections when no LMKs are installed? [Y/N]
(N): <Return>
Host interface [[E]thernet] (E): <Return>
Enter Well-Known-Port (1500): <Return>
Enter Well-Known-TLS-Port (2500): <Return>
UDP [Y/N] (Y): <Return>
TCP [Y/N] (Y): <Return>
Enable TLS [Y/N] (N): Y <Return>
ACL Enabled [Y/N] (N): Y <Return>
Number of connections [1-64] (64): 5 <Return>
Enter TCP keep alive timeout [1-120 minutes] (120):
<Return>
Number of interfaces [1/2] (2): <Return>

Interface Number 1:

IP Configuration Method? [D]HCP or [S]tatic (DHCP): S
<Return>
Enter IP Address (192.168.200.36):192.168.200.100 <Return>
Enter subnet mask (255.255.255.0): <Return>
Enter Default Gateway Address (192.168.200.3): <Return>

Enter speed setting for this port:

    SPEED OPTIONS:
0   Autoselect
1   10BaseT half-duplex
2   10BaseT full-duplex
3   100BaseTX half-duplex
4   100BaseTX full-duplex
5   1000BaseT half-duplex
6   1000BaseT full-duplex

Speed setting (4): 6 <Return>

Interface Number 2:

IP Configuration Method? [D]HCP or [S]tatic (DHCP): S
<Return>
Enter IP Address (192.168.202.110): <Return>
Enter subnet mask (255.255.255.0): <Return>
Enter Default Gateway Address (192.168.202.3): <Return>

Enter speed setting for this port:

    SPEED OPTIONS:
0   Autoselect
1   10BaseT half-duplex
2   10BaseT full-duplex
```

```
3   100BaseTX half-duplex
4   100BaseTX full-duplex
5   1000BaseT half-duplex
6   1000BaseT full-duplex

Speed setting (4): 6 <Return>

Save HOST settings to smart card? [Y/N]: N <Return>

Secure>
```

Example 2: *In this example, Ethernet communications using TLS is enabled - but UDP, and unprotected TCP are not allowed (i.e. all traffic must be protected using TLS). The IP addresses are set up as dynamic addresses to be obtained from a DHCP server. Access Control Lists are not being used. Only one host port is being configured. Secure state is required to change TLS or ACL settings.*

```
       Secure> CH <Return>

Please make a selection.  The current setting is in
parentheses.
Message header length [1-255] (4): <Return>
Disable host connections when no LMKs are installed? [Y/N]
(N): <Return>
Host interface [[E]thernet] (E): <Return>
Enter Well-Known-Port (1500): <Return>
Enter Well-Known-TLS-Port (2500): <Return>
UDP [Y/N] (Y): N <Return>
TCP [Y/N] (Y): N <Return>
Enable TLS [Y/N] (Y): Y <Return>
ACL Enabled [Y/N] (N): N <Return>
Number of connections [1-64] (64): 5 <Return>
Enter TCP keep alive timeout [1-120 minutes] (120):
<Return>
Number of interfaces [1/2] (2): 1 <Return>

Interface Number 1:

IP Configuration Method? [D]HCP or [S]tatic (static): D
<Return>
Network Name (A4665275320Q-host1): HSM1-Host-1 <Return>

Enter speed setting for this port:

    SPEED OPTIONS:
0   Autoselect
1   10BaseT half-duplex
2   10BaseT full-duplex
3   100BaseTX half-duplex
4   100BaseTX full-duplex
5   1000BaseT half-duplex
6   1000BaseT full-duplex

Speed setting (4): 6 <Return>

Save HOST settings to smart card? [Y/N]: N <Return>

Secure>
```

View Host Port Configuration (QH)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **QH**

Function: To display details of the Host port configuration of the HSM.

Authorization: This command does not require any authorization.

Inputs: None.

Outputs: For all systems:

- The message header length. This is the number of characters at the front of each command from the Host to the HSM (after the STX character). The HSM returns the message header in the response.
- Whether to disable the processing of host commands when no LMKs are installed.
- The protocol used.

For an Ethernet system:

- The Well-Known Port. This is the publicized TCP Port address of the HSM.
- The Well-Known TLS Port. This is the publicized TLS Port address of the HSM.
- Transport method: TCP, UDP, TLS
- Number of TCP connections. Each host interface supports this number of connections.
- The TCP Keep_Alive value: A number in minutes
- Whether ACLs are being used.
- The number of host interfaces configured
- The IP address for each host interface, and how they are derived. This is the IP address of the HSM in the system.
- The Network name of the interface, if configured to DHCP
- Subnet mask for each host interface. This is the subnet mask of the attached TCP/IP network. It is recommended that the Host Ethernet Ports, the Management Ethernet Port, and the Auxiliary Ethernet Port are all on different IP subnets from each other.
- The default gateway IP address
- The MAC Address for the interface
- The port speed for each host interface.

Errors: None.

Example 1: *In this example, Ethernet communications using TCP/IP and TLS are selected – all types of traffic are allowed. The IP addresses are set up as static, manually-entered addresses. Access Control Lists are to be used, and will be set up using the CONFIGACL console command.*

```
Online> QH <Return>

Message header length: 04
Disable host connections when no LMKs are installed: No
Protocol: Ethernet
Well-Known-Port: 01500
Well-Known-TLS-Port: 02500
Transport: UDP TCP TLS, 64 connections
TCP Keep_Alive value (minutes): 120 minutes
ACL: Enabled
Number of interfaces : (2)

Interface Number: 1
IP Configuration Method: static
IP address: 192.168.200.36
Subnet mask: 255.255.255.0
Default Gateway: 192.168.200.3
MAC address: 00:d0:fa:04:27:62
Port speed:  1000baseT full-duplex

Interface Number: 2
IP Configuration Method: static
IP address: 192.168.202.110
Subnet mask: 255.255.255.0
Default Gateway: 192.168.202.3
MAC address: 00:d0:fa:04:27:63
Port speed:  1000baseT full-duplex

Online>
```

Example 2: *In this example, Ethernet communications using TCP/IP and TLS are selected - but UDP, and unprotected TCP traffic is not allowed (i.e. all traffic must be TLS protected). The IP address is set up as a dynamic address to be obtained from a DHCP server. Access Control Lists are not being used. Only one host port has been configured.*

```
       Online> QH <Return>

Message header length: 04
Disable host connections when no LMKs are installed: No
Protocol: Ethernet
Well-Known-Port: 01500
Well-Known-TLS-Port: 02500
Transport: TLS, 64 connections
TCP Keep_Alive value (minutes): 120 minutes
ACL: Disabled
Number of interfaces : (1)

Interface Number: 1
IP Configuration Method: DHCP
Network Name: HSM1-Host-1
IP address: 192.168.200.36
Subnet mask: 255.255.255.0
Default Gateway: 192.168.200.3
MAC address: 00:d0:fa:04:3b:4a
```

```
Port speed:  1000baseT full-duplex

Online>
```

Host Port Access Control List (ACL) Configuration (CONFIGACL)

Variant ☑		Key Block ☑
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **CONFIGACL**

Function: To display and amend the Access Control Lists (ACLs) for the HSM's host ports. When ACL checking is enabled using the CH console command, traffic from hosts is accepted only where the host's IP address is included in one of the ACL entries set up using this command.

Authorization: This command does not require any authorization.
The HSM must be in Secure state.

Inputs:

- The user can view/add/delete entries. Entries cannot be amended.
- Each of the 2 host ports has its own ACL set.
- Entries can be of the following types:
  - A single IP address
  - An IP address range
  - An IP address mask
- Multiple types of entry can co-exist.
- Multiple entries of each type are allowed.
- The IP addresses in an entry can overlap with IP addresses in other entries.

Outputs:

- Confirmations and errors only.

Errors:

- IP address formats are validated.

Notes:

- This command sets up the IP addresses and ranges that will be used when checking traffic against the ACL, but the use of ACLs must be enabled in the CH console command before the ACLs configured in this command are applied.
- If the CH console command enables ACL checking but no ACL entries have been configured using CONFIGACL, then all host traffic will be blocked.
- ACLs apply only to Ethernet (including TLS) host traffic.

Example 1: *In this example, only one host interface has been configured in the CH command. There are no existing ACL entries. The user sets up a single address ACL entry, then adds a mask ACL entry, then adds a range ACL entry, and finally deletes the single address ACL entry.*

```
Secure> CONFIGACL <Return>

Access control list for Interface 1:
Single:
        None
Range:
        None
Mask:
        None

Add/Delete/Quit [A/D/Q]: A <Return>

Type - Single/Range/Mask [S/R/M]: S <Return>

IP Address: 10.10.41.10 <Return>

Access control list for Interface 1:
Single:
        1)  10.10.41.10
Range:
        None
Mask:
        None

Add/Delete/Quit [A/D/Q]: A <Return>

Type - Single/Range/Mask [S/R/M]: M <Return>

Base IP Address: 10.10.40.0 <Return>

Mask: 255.255.255.0 <Return>

Access control list for Interface 1:
Single:
        1)  10.10.41.10
Range:
        None
Mask:
        2)  10.10.40.0 to 10.10.40.255
(Mask:255.255.255.0)

Add/Delete/Quit [A/D/Q]: A <Return>

Type - Single/Range/Mask [S/R/M]: R <Return>

From IP Address: 192.168.0.0 <Return>

To IP Address: 192.168.0.92 <Return>

Access control list for Interface 1:
Single:
        1)  10.10.41.10
Range:
        2)  192.168.0.0 to 192.168.0.92
Mask:
        3)  10.10.40.0 to 10.10.40.255
(Mask:255.255.255.0)

Add/Delete/Quit [A/D/Q]: D <Return>
Entry to delete [1/3]: 1 <Return>

Access control list for Interface 1:
Single:
        None
Range:
        1)  192.168.0.0 to 192.168.0.92
Mask:
        2)  10.10.40.0 to 10.10.40.255
(Mask:255.255.255.0)

Add/Delete/Quit [A/D/Q]: Q <Return>

Secure>
```

Example 2: *In this example, both host interfaces have been configured in the CH command. The user simply views the existing ACL for host interface 2, and then exits.*

```
Secure> CONFIGACL <Return>
Interface 1: 10.10.100.216
Interface 2: 10.10.101.216
Select Interface [1/2]: 2 <Return>
Access control list for Interface 2:
Single:
        1)  10.10.40.22
        2)  10.10.40.23
        3)  10.10.40.23
Range:
        4)  10.10.40.200 to 10.10.40.220
Mask:
        None
WARNING: Duplicate - Single: Entries 2 and 3
Add/Delete/Quit [A/D/Q]: Q <Return>
Secure>
```

Configure Printer Port (CP)

Variant ☑		Key Block ☑
Online ☒	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **CP**

Function: To select and configure a connection to a printer attached to the HSM via a USB port. The HSM is compatible with most printers via its USB interfaces:

- A serial printer may be connected using a USB-to-serial converter cable available from Thales
- A parallel printer may be connected using a USB-to-parallel converter cable available from Thales

The new settings come into effect immediately after the command has completed.

Authorization: This command does not require any authorization.

Inputs:

- CR/LF order (standard or reversed): Y or N
- Selected printer connection.
- Setup Parameters, dependent on printer type.
- Whether to print a test page.

Outputs:

- Test page.

Errors:

- Failed to print test page

Notes: A printer must be connected to the HSM before the CP command is invoked.

Example 1: *This example demonstrates the configuration of a printer attached to the HSM via a USB-to-serial cable.*

```
Offline> CP <Return>

Reverse the <LF><CR> order? [Y/N]: N <Return>

The following possible printer devices were found in the
system:
   0. No printer
   1. USB-Serial Controller by PrintCo located at Rear
USB Port
Your selection (ENTER for no change): 1 <Return>
You must configure the serial parameters for this device:

   BAUD RATES
1.   1200
2.   2400
3.   4800
4.   9600 (current value)
5.  19200
6.  38400
7.  57600
8. 115200
Device baud rate (ENTER for no change):  8 <Return>

   DATA BITS
1. 5
2. 6
3. 7
4. 8 (current value)
Device data bits (ENTER for no change): <Return>

   STOP BITS
1. 1 (current value)
2. 2
Device stop bits (ENTER for no change): <Return>

   PARITY
1. none (current value)
2.  odd
3. even
Device parity (ENTER for no change): <Return>

  Flow Control
1. none
2. software (current value)
3. hardware
Printer flow_ctl (ENTER for no change): <Return>

  Printer Offline Control
1. none (current value)
2. RTS
3. DTR
Printer offline control (ENTER for no change): <Return>
Timeout [in milliseconds, min=1000, max=86400000]
(12000): <Return>
Delay [in milliseconds, min = 0, max=7200000] (0):
<Return>
```

```
Print test page? [Y/N]: Y <Return>

Offline>
```

Example 2: *This example demonstrates the configuration of a printer attached to the HSM via a USB-to-parallel cable.*

```
Offline> CP <Return>

Reverse the <LF><CR> order? [Y/N]: N <Return>

The following possible printer devices were found in the
system:
No printer
IEEE-1284 Controller by PrintCo located at Rear USB Port
Your selection (ENTER for no change): 1 <Return>
Timeout [in milliseconds, min=1000, max=86400000] (1000):
<Return>
Delay [in milliseconds, min = 0, max=7200000] (0):
<Return>
Print test page? [Y/N]: Y <Return>

Offline>
```

Example 3: *This example demonstrates the configuration of a printer attached to the HSM via a native USB cable.*

```
Offline> CP <Return>

Reverse the <LF><CR> order? [Y/N]: N <Return>

The following possible printer devices were found in the
system:
   0. No printer
   1. USB Printer by PrintCo located at Rear USB Port
Your selection (ENTER for no change): 1 <Return>
Timeout [in milliseconds, min=1000, max=86400000] (1000):
<Return>
Delay [in milliseconds, min = 0, max=7200000] (0):
<Return>
Print test page? [Y/N]: N <Return>

Offline>
```

View Printer Port Configuration (QP)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **QP**

Function: To display details of the HSM's printer configuration.

Authorization: This command does not require any authorization.

Inputs:

- Print test page: Y or N

Outputs:

- Reverse the <LF><CR> order: YES or NO.
- Validation of current printer configuration.
- The serial configuration settings (serial printer only).

Errors:

- Failed to print test page

Example 1: *This example demonstrates viewing the configuration of a printer attached to the HSM via a USB-to-serial cable.*

```
Online> QP <Return>

The configured printer, USB-Serial Controller by PrintCo
located at Rear USB Port, has been validated
   BAUD RATE:       38400
   DATA BITS:       8
   STOP BITS:       1
   PARITY:          none
   Flow Control:    XON/XOFF
   Offline Control: none
<LF><CR> order reversed: NO
Timeout:  12000 milliseconds
Delay:    0 milliseconds
Print test page? [Y/N]: N <Return>

Online>
```

Example 2: *This example demonstrates viewing the configuration of a printer attached to the HSM via a USB-to-parallel cable.*

```
Online> QP <Return>

The configured printer, IEEE-1284 Controller by PrintCo
located at Rear USB Port, has been validated.
<LF><CR> order reversed: NO
Timeout:  12000 milliseconds
Delay:    0 milliseconds
Print test page? [Y/N]: N <Return>

Online>
```

Example 3: *This example demonstrates viewing the configuration of a printer attached to the HSM via a native USB cable.*

```
Online> QP <Return>

The configured printer, USB Printer by PrintCo located at
Rear USB Port, has been validated
<LF><CR> order reversed: NO
```

```
Timeout:   1000 milliseconds
Delay:     0 milliseconds
Print test page? [Y/N]: N <Return>

Online>
```

Configure Management Port (CM)

Variant ☑	Key Block ☑	
Online ☒	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **CM**

Function: To configure the Management port, which is an Ethernet port used only for management of the HSM. If connection to the host is via Ethernet then the Ethernet host port is used for that purpose. The Management Ethernet port is used to update the HSM's internal software, updating licensing information, and for enabling management of a HSM via the payShield Manager.

The new settings come into effect a few seconds after the command has completed.

It is recommended that the Host Ethernet Ports, the Management Ethernet Port, and the Auxiliary Ethernet Port are all on different IP subnets from each other.

Authorization: The HSM must be in the offline or secure state to run this command.

Inputs:

- Whether IP address is manually or automatically derived.
  - If manually derived, then the address details must be entered.
  - If using DHCP, then a network name may be entered.
- Ethernet speed setting.
- Enable (local or remote) payShield Manager connection?

Outputs: None.

Errors: None.

Example 1: *In this example, the management port has its IP address set up manually.*

```
Offline> CM <Return>

Management Ethernet Interface:
IP Configuration Method? [D]HCP or [S]tatic (DHCP): S
<Return>
Enter IP address (192.168.100.200): 192.168.200.90
<Return>
Enter subnet mask (255.255.255.0): <Return>
Enter Default Gateway Address (192.168.200.1): <Return>

  Enter speed setting for this port:

      SPEED OPTIONS:
  0   Autoselect
  1   10BaseT half-duplex
  2   10BaseT full-duplex
  3   100BaseTX half-duplex
  4   100BaseTX full-duplex
  5   1000BaseT half-duplex
  6   1000BaseT full-duplex

  Speed setting (4): 6 <Return>


Enable payShield Manager connection:
Enable or Disabled? (E): D <Return>
Changing the IP address, Network name, or method requires
```

```
that the Management TLS certificate is regenerated.
Continuing will cause the
certificate to be regenerated under the Customer Trust
Authority. If you
require an externally signed Management TLS certificate
you will need to regenerate a CSR, have it signed and
imported.
Do you wish to proceed? [Y/N]: Y <Return>

Would you like to apply the changes now? [Y/N]: Y
<Return>

Offline>
```

Example 2: *In this example, the management port has its IP address set up automatically by a DHCP server.*

```
Secure> CM <Return>

Management Ethernet Interface:
IP Configuration Method? [D]HCP or [S]tatic (DHCP):
<Return>
Network Name (B46652712260-mgmt): HSM-Mngmnt <Return>

Enter speed setting for this port:

    SPEED OPTIONS:
0   Autoselect
1   10BaseT half-duplex
2   10BaseT full-duplex
3   100BaseTX half-duplex
4   100BaseTX full-duplex
5   1000BaseT half-duplex
6   1000BaseT full-duplex

Speed setting (0): <Return>

Enable payShield Manager connection:
Enable or Disabled? (E): <Return>

Would you like to apply the changes now? [Y/N]: Y
<Return>

Secure>
```

View Management Port Configuration (QM)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **QM**

Function: To display details of the Management port parameters.

Authorization: This command does not require any authorization.

Inputs: None.

Outputs:

- IP configuration method
- Network name (if configuration method is DHCP)
- IP address.
- Subnet mask.
- Default gateway.
- MAC address.
- Ethernet speed setting.
- Enable (local or remote) payShield Manager connection?

Errors: None.

Example 1:

```
Online> QM <Return>

Management Ethernet Interface:
IP Configuration Method: static
IP address: 192.168.200.90
Subnet mask: 255.255.255.0
Default Gateway: 192.168.200.1
MAC address: 00:d0:fa:04:27:64
Port speed:  1000baseT full-duplex
payShield Manager connection: Disabled

Online>
```

Example 2: *In this example, the management port has its IP address set up automatically by a DHCP server.*

```
Online> QM <Return>

Management Ethernet Interface:
IP Configuration Method: DHCP
Network Name: HSM-Mngmnt
IP address: 192.168.1.3
Subnet mask: 255.255.255.0
Default Gateway: 192.168.1.1
MAC address: 00:d0:fa:04:27:64
Port speed:  100baseTX full-duplex
payShield Manager connection: Enabled

Online>
```

Configure Auxiliary Port (CA)

Variant ☑	Key Block ☑	
Online ☒	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **CA**

Function: To configure the Auxiliary port, which is an Ethernet port currently used only for transmission of SNMP traffic from the HSM.

The new settings come into effect a few seconds after the command has completed.

It is recommended that the Host Ethernet Ports, the Management Ethernet Port, and the Auxiliary Ethernet Port are all on different IP subnets from each other.

Authorization: The HSM must be in the offline or secure state to run this command.

Inputs:

- Whether IP address is manually or automatically derived.
    - o If manually derived, then the address details must be entered.
    - o If using DHCP, then a network name may be entered.
- Ethernet speed setting.

Outputs: None.

Errors: None.

Example 1: *In this example, the auxiliary port has its IP address set up manually.*

```
Offline> CA <Return>

Auxiliary Ethernet Interface:
IP Configuration Method? [D]HCP or [S]tatic (DHCP): S
<Return>
Enter IP address (192.168.300.200): 192.168.300.90
<Return>
Enter subnet mask (255.255.255.0): <Return>
Enter Default Gateway Address (192.168.300.1): <Return>

  Enter speed setting for this port:

      SPEED OPTIONS:
  0   Autoselect
  1   10BaseT half-duplex
  2   10BaseT full-duplex
  3   100BaseTX half-duplex
  4   100BaseTX full-duplex
  5   1000BaseT half-duplex
  6   1000BaseT full-duplex

  Speed setting (4): 6 <Return>

Would you like to apply the changes now? [Y/N]: Y
<Return>

Offline>
```

Example 2: *In this example, the auxiliary port has its IP address set up automatically by a DHCP server.*

```
Secure> CA <Return>

Auxiliary Ethernet Interface:
IP Configuration Method? [D]HCP or [S]tatic (DHCP):
<Return>
Network Name (B46652712260-Aux): HSM-Aux <Return>

Enter speed setting for this port:

    SPEED OPTIONS:
0   Autoselect
1   10BaseT half-duplex
2   10BaseT full-duplex
3   100BaseTX half-duplex
4   100BaseTX full-duplex
5   1000BaseT half-duplex
6   1000BaseT full-duplex

Speed setting (0): <Return>

Would you like to apply the changes now? [Y/N]: Y
<Return>

Secure>
```

View Auxiliary Port Configuration (QA)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **QA**

Function: To display details of the Auxiliary port parameters.

Authorization: This command does not require any authorization.

Inputs: None.

Outputs:

- IP address.
- Network name, if DHCP configured.
- Subnet mask.
- Default gateway.
- MAC address.
- Ethernet speed setting.

Errors: None.

Example 1:

```
Online> QA <Return>

Auxiliary Ethernet Interface:
IP Configuration Method: static
IP address: 192.168.300.90
Subnet mask: 255.255.255.0
Default Gateway: 192.168.300.1
MAC address: 00:d0:fa:04:43:33
Port speed:  Ethernet 1000baseT full-duplex

Online>
```

Example 2:

In this example, the auxiliary port has its IP address set up automatically by a DHCP server.

```
Online> QA <Return>

Auxiliary Ethernet Interface:
IP Configuration Method: DHCP
Network Name: HSM-Aux
IP address: 192.168.1.3
Subnet mask: 255.255.255.0
Default Gateway: 192.168.1.1
MAC address: 00:d0:fa:04:43:33
Port speed:  100baseTX full-duplex

Online>
```

Configure Alarms (CL)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☒</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **CL**

Function: To enable or disable the motion alarm. The temperature alarm is permanently enabled. The HSM alarm circuitry typically needs to be turned off if the HSM is to be moved. The alarm should be turned on while the HSM is in service or being stored. The alarm setting can optionally be saved to a smartcard.

Authorization: The HSM must be in the secure state to run this command.

Inputs:

- Motion alarm status: Low, Medium, High or Off.
- Save settings to smartcard: Yes or No.

Outputs: None.

Errors:

- Card not formatted to save/retrieve HSM settings.
  Attempt with another card? [Y/N]

Example 1: *In this example, the setting is being made to a **less** secure setting.*

```
Secure> CL <Return>

Please make a selection.  The current setting is in
parentheses.
Motion alarm [Low/Med/High/OFF] (MED): F <Return>
LMKs must be erased before proceeding.
Erase LMKs?? [Y/N]: Y<Return>
Save ALARM settings to smart card? [Y/N]: N <Return>

Secure>
```

Example 2: *In this example, the setting is being made to a **more** secure setting.*

```
Secure> CL <Return>

Please make a selection.  The current setting is in
parentheses.
Motion alarm [Low/Med/High/OFF] (OFF): H <Return>
Save ALARM settings to smart card? [Y/N]: N <Return>

Secure>
```

View Alarm Configuration (QL)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **QL**

Function: To display details of the alarm configuration of the HSM.

Authorization: This command does not require any authorization.

Inputs: None.

Outputs:

- The Temperature alarm status.
- The Motion alarm status.

Errors: None.

Example:

```
Online> QL <Return>

Temperature alarm enabled

Motion alarm enabled high sensitivity

Online>
```

View/Change Instantaneous Utilization Period (UTILCFG)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☑</td><td colspan="2">Offline ☑</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **UTILCFG**

Function: To display the current setting of the period over which utilization statistics is to be collected when Instantaneous Utilization Data is requested. This command also allows the setting to be amended (in Offline/Secure states only).

Authorization: The HSM does not require any authorization to run this command.

Inputs: Amended value for Instantaneous Utilization Period. (It is suggested that the period should not be set to less than 10 seconds, as data collected over very short periods will not be indicative of actual activity.)

Outputs: Text messages as in example below.
Note that resetting of the value requires the HSM to be in Offline or Secure state.

Example:

```
Online> UTILCFG <Return>

Measurement period for instantaneous statistics is 60
seconds

Online>

…

Offline> UTILCFG <Return>

Measurement period for instantaneous statistics is 60
seconds

Change? [Y/N]: Y <Return>
Enter new value in seconds (1-60): 10 <Return>

Offline>
```

Suspend/Resume Collection of Utilization Data (UTILENABLE)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☑</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **UTILENABLE**

Function: To suspend or resume the collection of Utilization Data and the incrementing of the count of seconds over which the data is being collected. This allows data collection to be suspended if, for example, the HSM is taken out of service or temporarily re-purposed. It ensures that tps rates are not diluted by averaging command volumes over the total elapsed time, but only over the time that data is being collected

Authorization: The HSM does not require any authorization to run this command.

Inputs: Whether to change the current state.

Outputs: Text messages as in example below.

Notes: Following a software load, collection of Utilization Data will be suspended. Data collection is automatically suspended while the HSM is not online.

Example:

```
Offline> UTILENABLE <Return>

Utilization statistics gathering is currently turned ON.
Suspend? [Y/N] Y <Return>

Offline> UTILENABLE <Return>

Utilization statistics gathering is currently turned OFF.
Resume? [Y/N] Y <Return>

Offline>
```

Suspend/Resume Collection of Health Check Counts (HEALTHENABLE)

Variant ☑	Key Block ☑	
Online ☒	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **HEALTHENABLE**

Function: To suspend or resume the collection of Health Check counts. This allows data collection to be suspended if, for example, data is not required.

Authorization: The HSM does not require any authorization to run this command.

Inputs: Whether to change the current state.

Outputs: Text messages as in example below.

Notes: Following a software load, collection of Health Check counts will be suspended.

Example:

```
Offline> HEALTHENABLE <Return>

Health check statistics gathering is currently turned
ON.
Suspend? [Y/N] Y <Return>

Offline> HEALTHENABLE <Return>

Health check statistics gathering is currently turned
OFF.
Resume? [Y/N] Y <Return>

Offline>
```

View SNMP Settings (SNMP)

<table>
<tr><td>Variant ☑</td><td colspan="2">Key Block ☑</td></tr>
<tr><td>Online ☑</td><td>Offline ☑</td><td>Secure ☑</td></tr>
<tr><td colspan="3">Authorization: <b>Not required</b></td></tr>
</table>

Command: **SNMP**

Function: To display the current SNMP settings, and to enable/disable provision of Utilization and Health Check data via SNMP.

Authorization: The HSM does not require any authorization to run this command.

Inputs:

- Whether to Enable/Disable provision of Utilization and Health Check data via SNMP.
- Which Ethernet port to use for SNMP traffic.

Outputs: Text messages as in example below.

Notes: The HSM is delivered with no Users set up.

Example:

```
Secure> SNMP <Return>

V3 Users:
    None

SNMP is currently disabled

Enable? [Y/N]: Y <Return>

 0. Management Port
 1. Auxiliary Port

SNMP port [0-1] (ENTER for no change): 0 <Return>
sysName (Less than 256 characters)(payShield 10K):
<Return>
sysDescr (Less than 256 characters)(Thales e-Security
payShield 10K): <Return>
sysLocation (Less than 256 characters)(USA): <Return>
sysContact (Less than 256 characters)(Thales e-Security
Support): <Return>

Save new MIB-2 system settings? [Y/N]: Y <Return>

SNMP MIB-2 system updated

Secure>
```

Add an SNMP User (SNMPADD)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **SNMPADD**

Function: Add an SNMP User (for SNMP version 3).

Authorization:

- The HSM does not require any authorization to run this command.
- The HSM must be in Secure state.

Inputs:

- The SNMP user name,
- Authentication algorithm,
- Privacy algorithm.

Outputs: Text messages as in example below.

Notes: The HSM is delivered with no Users set up.

Example:

```
Secure> SNMPADD <Return>

Enter user name (Less than 20 characters): SHADES
<Return>
Authentication algorithm [[N]one, [M]D5, [S]HA]: S
<Return>
Enter authentication password (>= 8 and < 20 characters):
Password1 <Return>
Privacy algorithm [[N]one, [D]ES, [A]ES]: A <Return>
Enter privacy password (>= 8 and < 20 characters):
Password2 <Return>
The following entry will be added to the table:
    'createUser shades SHA AES'.
Confirm? [Y/N]: Y <Return>
User added successfully
Enter additional users? [Y/N]: N <Return>
Save and exit? [Y/N]: Y <Return>
SNMP configuration updated

Secure>
```

Delete an SNMP User (SNMPDEL)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☒</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **SNMPDEL**

Function: Delete an SNMP User.

Authorization:

- The HSM does not require any authorization to run this command.
- The HSM must be in Secure state.

Inputs: The index of the user to be deleted.

Outputs: Text messages as in example below.

Notes: The HSM is delivered with no Users set up.

Example:

```
Secure> SNMPDEL <Return>

SNMP user table:
        0: User=public, Authentication=none, Privacy=none
        1: User=shades, Authentication=SHA, Privacy=DES
        2: User=none, Authentication=none, Privacy=none
        3: User=md5, Authentication=MD5, Privacy=none

Select user to delete [0-3]: 1 <Return>

User ‘shades’ deleted successfully

Remove additional users? [Y/N]: N <Return>

Save and exit? [Y/N]: Y <Return>

SNMP configuration updated

Secure>
```

Configure SNMP Traps (TRAP)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **TRAP**

Function: To display the current SNMP Trap configuration and to enable/disable individual SNMP Traps.

Authorization: The HSM does not require any authorization to run this command.

Inputs: Whether to Enable/Disable individual trap configurations.

Outputs: Text messages as in the example below.

Notes: The HSM is delivered with no SNMP Traps configured.

Example 1:

```
Offline> TRAP <Return>

Trap table is empty, no SNMP traps are configured.

Enable? [Y/N]: Y <Return>

Offline>
```

Example 2:

```
Offline> TRAP <Return>

Entry    IP Address:Port      User name
 1       192.168.100.133:162  User1

Disable? [Y/N]: N <Return>

Offline>
```

Add a new SNMP Trap (TRAPADD)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **TRAPADD**

Function: Add an SNMP Trap.

Authorization:
- Authorization is not required.
- The HSM must be in the Secure state.

Inputs: Trap configuration data & confirmation.

Outputs: Text messages as in example below.

Errors: User table is empty; please add a V3 user first

Failed to add trap destination

Notes: The HSM is delivered with no SNMP traps configured.

Example 1:

```
Secure> TRAPADD <Return>

Enter IP Address: 192.168.100.133 <Return>
Enter Port (162): <Return>
SNMP user table:
        0: User=User1, Authentication=SHA, Privacy=DES

Select user [0-0]: 0 <Return>

The following entry will be added to the table:
        '192.168.100.133:162, User1'.
Confirm? [Y/N]: Y <Return>

Trap destination added successfully

Configure additional traps? [Y/N]: N <Return>

Save and exit? [Y/N]: Y <Return>

SNMP configuration updated

Secure>
```

Delete an SNMP Trap (TRAPDEL)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **TRAPDEL**

Function: Delete an SNMP Trap.

Authorization:

- Authorization is not required.
- The HSM must be in the Secure state.

Inputs: Confirmation of deletion.

Outputs: Text messages as in example below.

Errors: Trap table is empty; nothing to delete
Failed to delete trap destination.

Notes: The HSM is delivered with no SNMP traps configured.

Example:

```
Secure> TRAPDEL <Return>

SNMP Trap table:
    0: Address=192.168.100.133, Port=162, User=User1

Select trap to delete [0-0]: 0 <Return>

Trap destination deleted successfully

Delete additional traps? [Y/N]: N <Return>

Save and exit? [Y/N]: Y <Return>

SNMP configuration updated

Secure>
```

Fraud Detection Commands

The payShield 10K provides the following commands to support fraud detection operations:

Command	Page
Configure Fraud Detection (A5)	**270**
Re-enable PIN Verification (A7)	**273**

Configure Fraud Detection (A5)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
Authorization: **May be required** Activity: **<u>audit.console</u>**		

Command:	**A5**
Function:	To set the configuration of the HSM fraud detection function.

Authorization: If the Fraud Detection settings are to be edited, the HSM must be:

- in the offline or secure state to run this command, and
- either in the Authorized State, or the activity **audit.console** must be authorized, using the Authorizing Officer cards of the Management LMK.

Inputs:

- Whether and how to respond to Fraud Detection
- Limit on number of PIN verification failures per minute.
- Limit on number of PIN verification failures per hour.
- Limit on number of PIN attacks detected.

Outputs: None.

Errors:

- Not Authorized - the HSM is not authorized to perform this operation.
- Invalid Entry - the value entered is invalid.

Notes:

- If any of the limits set by this command are exceeded, an entry will be made in the Audit Log, and console command A7 must be used to re-enable PIN verification.
- Setting the HSM reaction to Logging only and the limits to zero will result in Fraud Detection not being recorded in the Health Check data. (*The term "Logging" as used in the screen prompt refers to logging in the Health Check data, not in the Audit Log.*)

Example:

```
Offline-AUTH> A5 <Return>

HSM reaction to Exceeding Fraud Limits is : ON

The following limits are set:
PIN verification failures per minute : 100
PIN verification failures per hour   : 1000
PIN Attack Limit                    : 100

HSM reaction to Exceeding Fraud Limits? ([O]n/[L]ogging
only): L <Return>

Note that logging is supported only if enabled via the
HEALTHENABLE console command (or its payShield Manager
equivalent)

Enter limit on PIN verification failures per minute: 200
<Return>
Enter limit on PIN verification failures per hour: 2000
<Return>
Enter PIN Attack Limit: 200 <Return>

Offline-AUTH>
```

Re-enable PIN Verification (A7)

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

Command: **A7**

Function: To reset the configuration of the HSM fraud detection function.

Authorization: The HSM must be in the offline state to run this command. The HSM must be either in the Authorized State, or the activity **audit.console** must be authorized, using the Authorizing Officer cards of the Management LMK.

Inputs: None.

Outputs: None.

Errors:

- Not Authorized - the HSM is not authorized to perform this operation.
- Command only allowed from offline.
- PIN Verification is not currently disabled

Example:

```
Offline-AUTH> A7 <Return>
PIN verification has been re-enabled
Offline-AUTH>
```

Diagnostic Commands

The payShield 10K provides the following console commands to support diagnostic operations:

Command	Page
Diagnostic Test (DT)	**275**
View Software Revision Number (VR)	**279**
View Available Commands (GETCMDS)	**281**
Show Network Statistics (NETSTAT)	**283**
Test TCP/IP Network (PING)	**285**
Trace TCP/IP route (TRACERT)	**286**
View/Reset Utilization Data (UTILSTATS)	**288**
View/Reset Health Check Counts (HEALTHSTATS)	**290**

Diagnostic Test (DT)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **DT**

Function: To perform diagnostic tests.
The DT command tests the following parts of the HSM:

- Battery voltage level
- Various cryptographic algorithms (DES, AES, RSA, SHA-1, etc.)
- Working memory areas
- Power Supplies
- Random Number Generator
- Real-time clock
- Smartcard reader
- Operating temperature
- Operating fan speeds
- Operating voltages

The command also initiates the Health Check Status report.

Authorization: The HSM does not require any authorization for this command.

Inputs: Optional qualifiers to modify scope and detail of output. Options are:

all	run all the commands (default option)
verbose	be verbose in the output
battery	run the battery diagnostics
des	run the DES diagnostics
health	run the health check diagnostics
aes	run the AES KAT
ecdsa	run the ECDSA KAT
md5	run the MD5 KAT
mem	run the memory diagnostics
psu	run the power supply diagnostics
rng	run the random number generator diagnostics
rsa	run the RSA KAT
rtc	run the real-time clock diagnostics
scr	run the smart card reader diagnostics
sha	run the SHA KAT
temp	run the temperature diagnostics
fans	run the fans diagnostics
volt	run the voltage diagnostics

Note that the multiple options can be combined (e.g." dt temp verbose"; "dt volt rsa")
Note that whilst the command code ("dt") is not case sensitive, the options listed above are.

Outputs: Status report on each item.

Errors: None.

Notes:

- The diagnostics are run automatically on a daily basis at the time specified using the ST Console command.

Example 1:

```
Secure>DT <Return>

Battery:         OK
AES:             OK
DES:             OK
ECDSA:           OK
HMAC:            OK
MD5:             OK
Memory:          OK
Power Supply:    OK
RNG:             OK
RSA:             OK
Real-Time Clock: SYNCHRONIZED (system time was synchronized
with the RTC)
SHA:             OK
SCR:             OK
Temperature:     OK
Fans:            OK
Voltages:        OK

Health Check Status

TCP Server:                     Up
UDP Server:                     Up
FICON Server:                   Not Enabled
Local/Remote Manager Server:    Up
Host Ethernet Link 1:           Up
Host Ethernet Link 2:           Up
Unit Tampered?:                 No
Fraud limits exceeded?:         No
PIN attack limit exceeded?:     No

Diagnostics complete

Offline>
```

Example 2:

```
Online> DT verbose <Return>

Battery:         OK
    Voltage: 3500 mV
    HSM will enter tamper state if voltage drops below 2500
mV

    Running AES Known Answer Test
    PASSED AES Known Answer Test
AES:             OK

    Running DES Known Answer Test
    PASSED DES Known Answer Test
DES:             OK

    Running ECDSA Known Answer Tests
    PASSED Cryptodev ECDSA Known Answer Tests
    PASSED OpenSSL ECDSA Known Answer Tests
    PASSED OpenSSL ECDHC Known Answer Tests
ECDSA:           OK

    Running MD5 Known Answer Test
    PASSED MD5 Known Answer Test
MD5:             OK

    Running Memory Test
    PASSED Memory Test
Memory:          OK
Power Supply:    OK

    Running RNG self-tests (Attempt: 1)
    PASSED RNG self-tests
RNG:             OK

    Running RSA Known Answer Test
    PASSED RSA Known Answer Test
RSA:             OK
Real-Time Clock: OK
   Current Time: FNov 16 12:09:54 2018


    Running SHA Known Answer Test
    PASSED SHA Known Answer Test
SHA:             OK
SCR:             OK
Temperature:     OK


    MSP      :  33.1C 91.6F          (Min=30.0C 86.0F
Max=35.1C 95.2F)
    MP 1     :  56.2C 133.2F         (Min=46.0C 114.8F
Max=61.6C 142.9F)
    MP 2     :  56.2C 133.2F         (Min=46.3C 115.3F
Max=62.9C 145.2F)
    Crypto   :  41.0C 105.8F         (Min=37.1C 98.8F
Max=42.8C 109.0F)
    Sensor 1 :  43.9C 111.0F         (Min=42.1C 42.1F
Max=46.3C 115.3F)
    Sensor 2 :  38.6C 101.5F         (Min=36.6C 97.9F
Max=40.4C 104.7F)
```

```
    Sensor 3 :  35.2C 95.4F          (Min=33.1C 91.6F
Max=36.6C 36.6F)
Fans:            OK
   Fan 1:             8000 RPM (target: 8000 RPM)
   Fan 2:             7868 RPM (target: 8000 RPM)
Voltages:        OK

    V12          :  11.46   (Min=11.43      Max=11.48)
    V5           :  5.052   (Min=5.032      Max=5.067)
    MP Core      :  1.028   (Min=1.016      Max=1.038)
    Crypto Core  :  1.053   (Min=1.052      Max=1.060)
    Battery      :  3.595   (Min=3.593      Max=3.599)


Health Check Status

TCP Server:                     Up
UDP Server:                     Up
FICON Server:                   Not Enabled
Local/Remote Manager Server:    Up
Host Ethernet Link 1:           Up
Host Ethernet Link 2:           Not Enabled
Unit Tampered?:                 No
Fraud limits exceeded?:         No
PIN attack limit exceeded?:     No

Diagnostics complete

Online>
```

View Software Revision Number (VR)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **VR**

Function: To display details of the software release number, revision number and build number.

Authorization: The HSM does not require any authorization to run this command.

Inputs: None.

Outputs: Software revision numbers, serial numbers, license details and FIPS algorithm information.

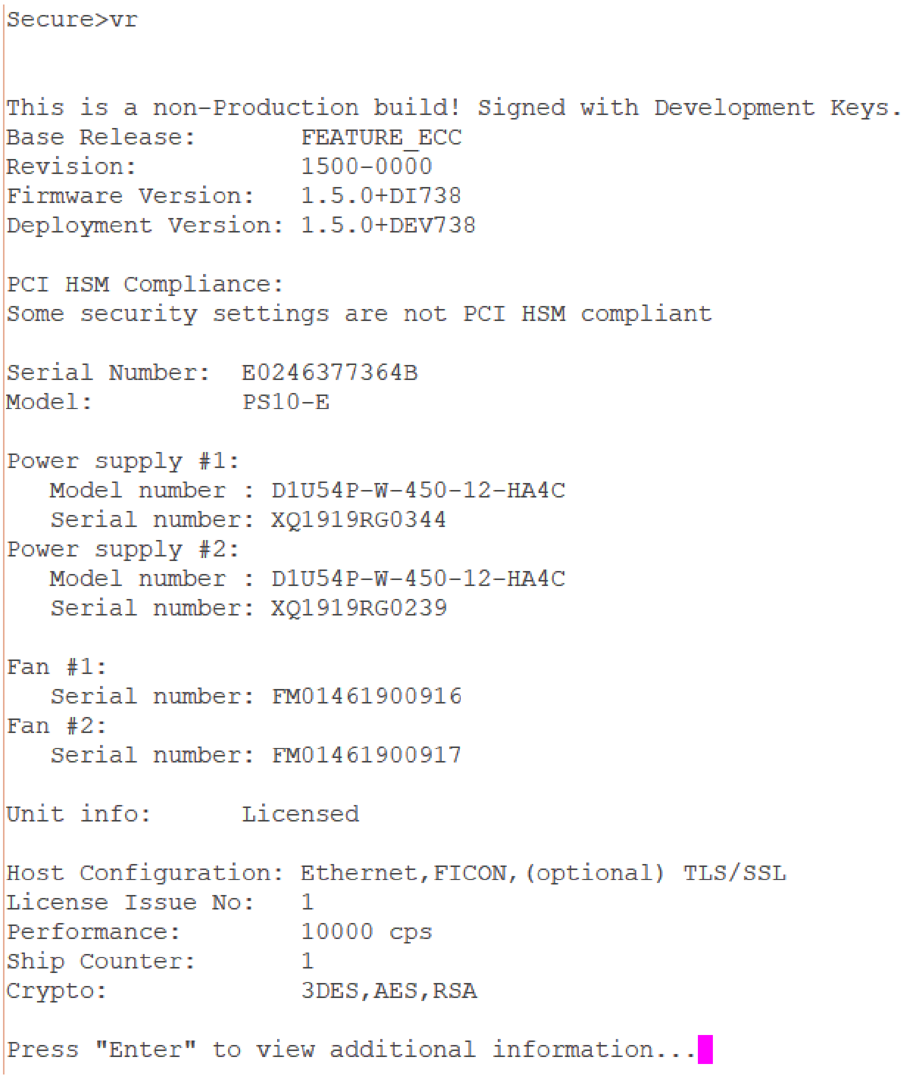
Errors: None.

Notes: The software revision reported by the VR command will have one of the following forms:

- xxxx-10xx – this indicates that this software has been PCI HSM certified and that the appropriate security settings have been set (e.g. by using the CS Console command) to the required values.
- xxxx-00xx – this indicates that either:
  - this version of software is not PCI HSM certified, or
  - this version of software is PCI HSM certified but one or more of the appropriate security settings have not been set (e.g. by using the CS Console command) to the required values.

Example: *Software which has not been PCI HSM certified. TLS protection of host communications is enabled.*

```
Online> VR <Return>
```



```
Secure>vr


This is a non-Production build! Signed with Development Keys.
Base Release:       FEATURE_ECC
Revision:           1500-0000
Firmware Version:   1.5.0+DI738
Deployment Version: 1.5.0+DEV738

PCI HSM Compliance:
Some security settings are not PCI HSM compliant

Serial Number:  E0246377364B
Model:          PS10-E

Power supply #1:
   Model number : D1U54P-W-450-12-HA4C
   Serial number: XQ1919RG0344
Power supply #2:
   Model number : D1U54P-W-450-12-HA4C
   Serial number: XQ1919RG0239

Fan #1:
   Serial number: FM01461900916
Fan #2:
   Serial number: FM01461900917

Unit info:      Licensed

Host Configuration: Ethernet,FICON,(optional) TLS/SSL
License Issue No:   1
Performance:        10000 cps
Ship Counter:       1
Crypto:             3DES,AES,RSA

Press "Enter" to view additional information...
```

The example above reflects non-PCI compliant settings. A PCI compliant example would reflect the following under the PCI HSM Compliance field:

```
PCI HSM Compliance:
Refer to the PCI web site
(https://www.pcisecuritystandards.org/approved_companies_pro
viders/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.
```

View Available Commands (GETCMDS)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☑</td><td colspan="2">Offline ☑</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **GETCMDS**

Function: To display a list of enabled host & console commands. Commands listed in the output are licensed AND enabled. Commands omitted from the output are either not licensed, or not enabled. Console command CONFIGCMDS can be used to enable/disable individual commands.

GETCMDS can optionally generate a hash (message digest) over the set of enabled commands, thus providing a simple mechanism to verify that two (or more) HSMs have the same set of commands enabled.

Note: Some of the commands listed may require additional license options enabled.

Authorization: The HSM does not require any authorization to run this command.

Inputs: [-lh]

-l	Display available host & console commands.
-h	Display hash over enabled commands.

Outputs: A list of available HSM commands (depending on options) or a hash value.

Errors: None.

Example:

```
Online> GETCMDS -h –l <Return>

List of available Host commands:

A0   A2   A4   A6   A8   AA   AC   AE   AG   AI   AK   AM   AO   AQ   AS
AU   AW   AY   B0   B2   B8   BA   BC   BE   BG   BI   BK   BM   BQ   BS
BU   BW   BY   C0   C2   C4   C6   C8   CA   CC   CE   CG   CI   CK   CM
CO   CQ   CS   CU   CW   CY   D0   D2   D4   D6   D8   DA   DC   DE   DG
DI   DK   DM   DO   DQ   DS   DU   DW   DY   E0   E2   E4   E6   E8   EA
EC   EE   EG   EI   EK   EM   EO   EQ   ES   EU   EW   EY   F0   F2   F4
F6   F8   FA   FC   FE   FG   FI   FK   FM   FO   FQ   FS   FU   FW   FY
G0   G2   G4   G6   G8   GA   GC   GE   GG   GI   GK   GM   GO   GQ   GS
GU   GW   GY   H0   H2   H4   H6   H8   HA   HC   HE   HG   HI   HK   HM
HO   HQ   HS   HU   HW   HY   I0   I2   I4   I6   I8   IA   IC   IE   IG
II   IK   IM   IO   IQ   IU   IW   IY   J0   J2   J4   J6   J8   JA   JC
JE   JG   JI   JK   JO   JS   JU   JW   JY   K0   K2   K8   KA   KC   KE
KG   KI   KK   KM   KO   KQ   KS   KU   KW   KY   L0   L2   L4   L6   L8
LA   LC   LE   LG   LI   LK   LM   LO   LQ   LS   LU   LW   LY   M0   M2
M4   M6   M8   MA   MC   ME   MG   MI   MK   MM   MO   MQ   MS   MU   MW
MY   N0   NC   NE   NG   NI   NK   NO   NY   OA   OC   OE   OI   OK   OU
OW   P0   P2   P4   P6   P8   PA   PC   PE   PG   PI   PK   PM   PO   PQ
PS   PU   PW   PY   Q0   Q2   Q4   Q6   Q8   QA   QC   QE   QI   QK   QM
QO   QQ   QS   QU   QW   QY   R2   R4   R6   R8   RA   RC   RE   RG   RI
RK   RM   RO   RQ   RS   RU   RW   RY   SY   T0   T2   T4   T6   TA   U0
U2   U4   U6   U8   V0   V2   V4   V6   V8   W0   W2   W4   W6   W8   X0
X2   X4   X6   X8   XK   XM   XO   XQ   XS   XU   XW   Y0   Y2   Y4   Y6
Y8   Z0   ZA   ZE   ZK   ZM   ZU
List of available Console commands:

A       A5      A6      A7      AUDITLOG        AUDITOPTIONS
C       CA      CH      CK      CL      CLEARERR
CLEARAUDIT      CM      CO      CONFIGACL       CONFIGCMDS
```

```
    CONFIGPB
CP      CS      CV      DC      DM      DO
DT      EC      ED      EJECT   ERRLOG  FC
FK      GC      GETCMDS GETTIME GK      GS
GT      HEALTHENABLE    HEALTHSTATS     IK      IV      KD
KE      KG      KK      KM      KN      KT
LK      LO      LN      MI      N       NP
NETSTAT PING    PV      QA      QH      QL
QM      QP      QS      R       RC      RESET
RS      SD      SE      SETTIME SG      SI
SK      SL      SP      SNMP    SNMPADD SNMPDEL
SS      ST      SV      T       TD      TRAP
TRAPADD TRAPDEL TRACERT UPLOAD  UTILCFG UTILENABLE
UTILSTATS       V       VA      VC      VR      VT
XA      XD      XE      XH      XI      XK
XR      XT      XX      XY      XZ      $

Host/Console Command Hash Value:  cf7e8a
```

Show Network Statistics (NETSTAT)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **NETSTAT**

Function: The HSM records details about network activity on both its Management and Host Ethernet ports for diagnostic and security purposes. As a diagnostic aid, it can provide useful information when configuring the unit. If reviewed periodically, it can also provide evidence of unexpected network activity, which may require further investigation.

The HSM collects information about each 'endpoint' that communicates with it. The information recorded will depend on the particular protocol that was used to send the packet.

Authorization: The HSM does not require any authorization to run this command.

Inputs: **Syntax:**

```
netstat [-vWeenNcCF] [<Af>] –r
netstat {-V|--version|-h|--help}
netstat [-vWnNcaeol] [<Socket> ...]
netstat { [-vWeenNac] -i | [-cWnNe] -M | -s }
```

Options:

-r, --route	display routing table
-i, --interfaces	display interface table
-g, --groups	display multicast group memberships
-s, --statistics	display networking statistics (like SNMP)
-M, --masquerade	display masqueraded connections
-v, --verbose	be verbose
-W, --wide	don't truncate IP addresses
-n, --numeric	don't resolve names
--numeric-hosts	don't resolve host names
--numeric-ports	don't resolve port names
--numeric-users	don't resolve user names
-N, --symbolic	resolve hardware names
-e, --extend	display other/more information
-p, --programs	display PID/Program name for sockets
-c, --continuous	continuous listing
-l, --listening	display listening server sockets
-a, --all, --listening	display all sockets (default: connected)
-o, --timers	display timers
-F, --fib	display Forwarding Information Base (default)
-C, --cache	display routing cache instead of FIB
-Z, --context	display SELinux security context for sockets

Outputs: Text messages as appropriate.

The reported state can have the following values:

ESTABLISHED
The socket has an established connection.
SYN_SENT
The socket is actively attempting to establish a connection.
SYN_RECV
A connection request has been received from the network.
FIN_WAIT1
The socket is closed, and the connection is shutting down.
FIN_WAIT2
Connection is closed, and the socket is waiting for a shutdown from the remote end.
TIME_WAIT
The socket is waiting after close to handle packets still in the network.
CLOSED
The socket is not being used.
CLOSE_WAIT
The remote end has shut down, waiting for the socket to close.
LAST_ACK
The remote end has shut down, and the socket is closed. Waiting for acknowledgement.
LISTEN
The socket is listening for incoming connections.
CLOSING
Both sockets are shut down but we still don't have all our data sent.
UNKNOWN
The state of the socket is unknown

Example:

```
Offline> NETSTAT <Return>

Available Ethernet Interfaces:
Management Interface : 192.168.220.116
Auxiliary Interface  : 169.254.254.1
Host Interface 1     : 192.168.220.16
Host Interface 2     : 192.168.192.149

Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address       Foreign Address
State
tcp        0    236 192.168.220.116:ssh
193.240.102.135:49921 ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type    State      I-Node   Path
unix  40     [ ]     DGRAM              2925     /dev/log
unix  2      [ ]     DGRAM              1735
unix  2      [ ]     DGRAM              11668
unix  2      [ ]     DGRAM              57209
unix  3      [ ]     STREAM  CONNECTED  143125
/var/ipc/agentx

Offline>
```

Test TCP/IP Network (PING)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☑</td><td colspan="2">Offline ☑</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **PING**

Function: To test the specified network node, and the route to it.

Authorization: The HSM does not require any authorization to run this command.

Inputs: **Syntax:**

ping [-q] [-c *count*] [-I *interface*] [-p *pattern*]
    [-s *packetsize*] [-t *ttl*] [-w *maxwait*] host

Options:

-c *count* Stop after sending (and receiving) this many ECHO_RESPONSE packets.

-I *interface* The interface that PING is to be sent from.

interface Value	HSM Port
h1	Host Port #1
h2	Host Port #2
m	Management Port (default)

-p *pattern* Fill out the packet with this many "padding" bytes (maximum is 16). You should find this useful for diagnosing data-dependent problems in a network. For example, -p ff causes the sent packet to be filled with ones.

-q Be quiet: display nothing except for the summary lines at startup time and when finished.

-s *packetsize* Send this many data bytes. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.

-t *ttl* Use the specified time-to-live. It represents how many hops the packet can go through before being discarded (when it reaches 0). The default is 255.

-w *maxwait* Specify a timeout, in seconds, before ping exits regardless of how many packets have been sent or received.

Outputs: Text messages as appropriate.

Example:

```
Offline> PING –I h1 192.168.100.123 <Return>

PING 192.168.100.123 (192.168.100.123): 56 data bytes
64 bytes from 192.168.100.123: seq=0 ttl=32 time=16 ms
64 bytes from 192.168.100.123: seq=1 ttl=32 time=4 ms
64 bytes from 192.168.100.123: seq=2 ttl=32 time=4 ms
64 bytes from 192.168.100.123: seq=3 ttl=32 time=4 ms
64 bytes from 192.168.100.123: seq=4 ttl=32 time=4 ms
64 bytes from 192.168.100.123: seq=5 ttl=32 time=101 ms
64 bytes from 192.168.100.123: seq=6 ttl=32 time=4 ms
64 bytes from 192.168.100.123: seq=7 ttl=32 time=4 ms
64 bytes from 192.168.100.123: seq=8 ttl=32 time=4 ms
64 bytes from 192.168.100.123: seq=9 ttl=32 time=4 ms

Offline>
```

Trace TCP/IP route (TRACERT)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **TRACERT**

Function: To view the path taken from the HSM to the specified address.

Authorization: The HSM does not require any authorization to run this command.

Inputs: **Syntax:**

```
tracert [-dFIlnr] [-f first_ttl]
     [-g gateway] [-i interface] [-m max_ttl] [-p port]
     [-q nqueries] [-s src_addr] [-t tos] [-w wait_time]
     host [packetsize]
```

Options:

-d Turn on socket-level debugging.

-F Set the "don't fragment" bit.

-f *first_ttl* Set the initial time-to-live used in the first outgoing probe packet.

-g *gateway* Specify a loose source route gateway (8 maximum).

-I Use ICMP ECHO instead of UDP datagrams.

-i *interface*

interface Value	HSM Port
h1	Host Port #1
h2	Host Port #2
m	Management Port (default)

-l ("el") Display the TTL (time-to-live) value of the returned packet. This is useful for checking for asymmetric routing.

-m *max_ttl* Set the maximum TTL (maximum number of hops) used in outgoing probe packets. The default is 30 hops (the same default as is used for TCP connections).

-n Print hop addresses numerically only. By default, addresses are printed both symbolically and numerically. This option saves a nameserver address-to-name lookup for each gateway found on the path.

-p *port* The base UDP port number to be used in probes (default is 33434). The tracert utility hopes that nothing is listening on UDP ports base to base + nhops -1 at the destination host (so an ICMP PORT_UNREACHABLE message is returned to terminate the route tracing). If something is listening on a port in the default range, you can use this option to pick an unused port range.

-q *nqueries* The number of probes per ttl to *nqueries* (default is three probes).

-r Bypass the normal routing tables and send directly to a host on an attached network. If the host isn't on a directly attached network, an error is returned. You can use this option to "ping" a local host through an interface that has no route through it (for example, after the interface was dropped by routed).

-s *src_addr* The IP address (must be given as an IP number, not a hostname) to be used as the source address in outgoing probe packets. If the host has more than one IP address, you can use this option to force the source address to be something other than the IP address of the interface that the probe packet is sent on. If the IP address you specify isn't one of this machine's interface addresses, an error is returned and nothing is sent.

-t *tos* The type-of-service (TOS) to be used in probe packets (default is zero). The value must be a decimal integer in the range 0 to 255. You can use this option to see if different TOSs result in different paths.
Not all TOS values are legal or meaningful. You should find the values -t 16 (low delay) and -t 8 (high throughput) useful.

-w *wait_time* The time (in seconds) to wait for a response to a probe (default is 5).

host The destination hostname or IP number.

packetsize The probe datagram length (default is 40 bytes).

Outputs: Text messages as appropriate.

Example:

```
Offline> TRACERT  -I h1 –g 10.10.10.1   10.10.11.2
<Return>

traceroute to 10.10.11.2 (10.10.11.2), 64 hops max, 40
byte packets
10.10.10.1 (10.10.10.1)  5.000 ms  7.000 ms  5.000 ms
10.10.11.2 (10.10.11.2)  5.000 ms  6.000 ms  6.000 ms

Offline>
```

View/Reset Utilization Data (UTILSTATS)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **UTILSTATS**

Function: To display Utilization Data at the Console. Options to print the data to an HSM-attached printer and to reset accumulated data to zero.

Authorization: The HSM does not require any authorization to run this command.

Notes:

- Utilization statistics are also reset when new software is installed on the HSM.
- The precise meaning of a HSM loading range identified below as, for example, "*10-20%*" is "*from exactly 10% to just under 20%*".
- Statistics are provided irrespective of which host interface the commands are received over.

Inputs:

- Whether to print output to HSM-attached printer
- Whether to reset data

Outputs: Text messages as in example below.

Note that the number of seconds displayed is not necessarily the number of seconds between the start and end times: rather, it is the number of seconds during this period when data collection was enabled using the UTILENABLE command and the HSM was online.

Example:

```
Online> UTILSTATS <Return>

HSM Serial Number:            A4665271570Q

Report Generation Time: 05-Dec-2018 19:42.37
Report Start Time:            04-Dec-2018 09:25.01
Report End Time:        05-Dec-2018 19:42.37
Total number of secs:         123,456

HSM Loading:
0-10%:      56,789
10-20%:     24,109
20-30%:     21,445
30-40%:     12,382
40-50%:     3,288
50-60%:     2,917
60-70%:     2,123
70-80%:     403
80-90%:     0
90-100%:    0
100%: 0

Press "Enter" to continue... <Return>




Host Command Volumes:
        Cmd Code  Total Transactions  Average TPS
        A0        225                 4.79
        A4        99                  2.11
        A6        342                 7.28
        A8        408                 8.68
        AA        141                 3.00
        AC        135                 2.87
        AE        84                  1.79
        AG        66                  1.40
        AS        18                  0.38
        AU        94                  2.00
        AW        94                  2.00
        AY        94                  2.00
        B0        50                  1.06
        BA        14                  0.30
        BC        34                  0.72
        BE        42                  0.89
        BG        5                   0.11
        BI        11                  0.23
        BK        128                 2.72

Press "Enter" to continue... <Return>

        Cmd Code  Total Transactions  Average TPS
        BM        10                  0.21
        LA        2                   0.04

Instantaneous HSM Load: 17%
Instantaneous Host Command Volumes:
Cmd Code    Total Transactions  Average TPS
BM         10                  0.21
LA         2                   0.04

Send output to printer? [Y/N]: Y <Return>
Reset All Stats? [Y/N]: Y <Return>
All utilization statistics will be reset to 0. Confirm?
[Y/N]: Y <Return>

Online>
```

View/Reset Health Check Counts (HEALTHSTATS)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **May be required** Activity: **diagnostics**		

Command: **HEALTHSTATS**

Function: To display Health Check counts at the Console. Options to print the data to a HSM-attached printer and to reset accumulated data to zero.

Authorization: The HSM does not require any authorization to run this command to view the data.
The HSM must be in Offline/Secure Authorized state (or the activity **diagnostics** must be authorized) for the Management LMK to reset the Health Check Counts

Notes:

- Accumulated health check counts are also reset when new software is installed on the HSM.
- If collection of health check data has been suspended at any time, the counts relating to Fraud Detection (i.e. failed PIN verifications and PIN Attacks) will not represent the values of those counts which will be used by the HSM to trigger return of Error 39 or deletion of LMKs.

Inputs:

- Whether to print output to HSM-attached printer
- Whether to reset data (requires Offline/Secure Authorized state).

Outputs: Text messages as in example below.

Example:

```
Offline-AUTH> HEALTHSTATS <Return>

HSM Serial Number:            A4665271570Q

Report Generation Time:        05-Dec-2018 23:22.28
Report Start Time:             01-Dec-2018 01:11.21
Report End Time:               25-Dec-2018 23:22.28
Number of reboots:                                3
Number of tampers:                                1
PIN verification failures/minute limit exceeded: 57
PIN verification failures/hour limit exceeded:    4
PIN Attack Limit exceeded:                        0

Send output to printer? [Y/N]: Y <Return>

Reset All Stats? [Y/N]: Y <Return>
All Utilization statistics will be reset to 0. Confirm?
[Y/N]: Y <Return>

Offline-AUTH>
```

Local Master Keys

Types of LMKs

A **Variant LMK** is a set of 20 double- or triple-length TDES keys, with different "pairs" and variants of those "pairs" being used to encrypt different types of keys.

Note that the term "pair" is used regardless of whether the LMK consists of double-length keys, or triple-length keys. The standard LMK format supported in all previous versions of Thales (Racal) HSM firmware consists of 20 double-length TDES keys.

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

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

Note that the term "Key Block LMK" refers to the 'key block' method of encrypting keys; a Key Block LMK is not itself stored in the key block format.

Multiple LMKs

It is possible to install multiple LMKs within a single HSM. The precise details of the number and type of installed LMKs are controlled via the HSM's license file:

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

Attribute	Description
LMK ID	A 2-digit number which uniquely indicates the location of each LMK within the table. All references to LMKs are made by specifying the LMK Identifier.
Key Scheme	• "Variant" for traditional Racal/Thales LMK – key encryption performed using the *variant* method. • "Key Block" for enhanced security – key encryption performed using the *key block* method.
Algorithm	• "3DES (2key)" or "3DES (3key)" is used by Variant LMKs. • "3DES (3key)" or "AES (256-bit)" is used by Key Block LMKs. Other algorithm types may be supported in future software releases.
Status	• "Test" indicates that the LMK is used for testing purposes. • "Live" indicates that the LMK is used for live production purposes. When installing LMKs, the HSM will prevent any mixing of Test and Live LMKs within the same slot (i.e. LMK Value and Old/New LMK Value must have the same status).
Comments	User-entered text, which can be used to help identify LMKs.

Authorization	Indicates the authorization status of the HSM for this particular LMK – either a flag (for Authorized State) or a list of authorized activities.
Old/New Status	Flag for each LMK held in Key Change Storage indicating whether they are to be used as an 'old' LMK (loaded via 'LO' command), or a 'new' LMK (loaded via 'LN' command).
LMK Check Value	The check value of the LMK.
Old/New LMK Check Value	The check value of the 'old' or 'new' LMK held in Key Change Storage.

Use the console command VT (View LMK Table) to view the contents of the HSM's LMK table (but not the actual LMK values).

LMK Commands

The HSM provides the following console commands to support LMK operations:

Command	Page
Generate LMK Component (GK)	**294**
Load LMK (LK)	**297**
Load 'Old' LMK into Key Change Storage (LO)	**303**
Load 'New' LMK into Key Change Storage (LN)	**307**
Verify LMK Store (V)	**311**
Duplicate LMK Component Sets (DC)	**312**
Delete LMK (DM)	**313**
Delete 'Old' or 'New' LMK from Key Change Storage (DO)	**314**
View LMK Table (VT)	**315**
Generate Test LMK (GT)	**318**

Generate LMK Component(s) (GK)

Variant ☑		Key Block ☑
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **GK**

Function: To generate component(s) of an LMK, and store the component(s) on smartcards.
This command may be used to generate components for the following types of LMKs:

- Double-length (2DES) Variant LMK
- Triple-length (3DES) Variant LMK
- Triple-length (3DES) Key Block LMK
- 256-bit AES Key Block LMK.

When creating a Variant LMK or a 3DES Key Block LMK, this command generates the data for a single LMK component card.

When creating an AES Key Block LMK, this command generates the data for all the required number of LMK component cards.

Authorization: The HSM must be in the secure state to run this command.

Inputs:

- LMK Scheme (Variant or Key Block).
- LMK Algorithm:
  - Double-length (2DES) or triple-length (3DES) if Variant scheme is selected
  - Triple-length (3DES) or AES if Key Block scheme is selected.
- LMK Status (Test or Live).
- For an AES Key Block LMK:
  - Number of components.
  - Number of components required to reconstitute the LMK.

Outputs:

- LMK components written to smartcards.
- LMK component check value.

Errors:

- Card not formatted – use the FC command to format the card.
- Not a LMK card –card is not formatted for LMK or key storage.
- Warning – card not blank. Proceed? [Y/N] – LMK card is not blank.
- Overwrite LMK set? [Y/N] – card already contains an LMK component.
- Smartcard error; command/return: 0003 – invalid PIN is entered.
- Invalid PIN; re-enter – a PIN of less than 4 or greater than 8 is entered.

Notes:

- PINs must be entered within 60 seconds of being requested.
- If the CS setting "Card/Password authorization" is set to "Card", then the HSM will write a random password to the 1st and 2nd LMK component cards. These passwords will be required in order to put the HSM into the Authorized State.

Example 1:
(Triple-length
Variant LMK)

This example generates a triple-length Variant LMK component set, and writes the components to a smartcard.

```
Secure> GK <Return>
Variant scheme or key block scheme? [V/K]: V <Return>
Enter algorithm type [2=2DES, 3=3DES]: 3 <Return>

Key status? [L/T]: L <Return>
LMK component set [1-9]: 1 <Return>
Enter secret value A: AAAA AAAA AAAA AAAA <Return>
Enter secret value B: BBBB BBBB BBBB BBBB <Return>
Enter secret value C: CCCC CCCC CCCC CCCC <Return>
Enter value D:      DDDD DDDD <Return>
Insert blank card and enter PIN: ******** <Return>
Writing keys...
Checking keys...
Device write complete, check: ZZZZZZ

Remove the smartcard and store it securely.

Make another copy? [Y/N]: N <Return>
1 copies made.

Repeat the procedure to generate further component sets.

Secure>
```

Example 2:
(Double-length
Variant LMK)

This example generates a double-length variant LMK component set, and writes the components to a smartcard.

```
Secure> GK <Return>
Variant scheme or key block scheme? [V/K]: V <Return>
Enter algorithm type [2=2DES, 3=3DES]: 2 <Return>

Key status? [L/T]: L <Return>
LMK component set [1-9]: 1 <Return>
Enter secret value A: AAAA AAAA AAAA AAAA <Return>
Enter secret value B: BBBB BBBB BBBB BBBB <Return>
Enter value C:      CCCC CCCC <Return>
Insert blank card and enter PIN: ******** <Return>
Writing keys...
Checking keys...
Device write complete, check: ZZZZZZ

Remove the smartcard and store it securely.

Make another copy? [Y/N]: N <Return>
1 copies made.

Repeat the procedure to generate further component sets.

Secure>
```

Example 3:
(Triple-length 3DES Key Block LMK)

This example generates a 3DES key block LMK component, and writes the component to a smartcard.

```
Secure> GK <Return>
Variant scheme or key block scheme? [V/K]: K <Return>
Enter algorithm type [D=DES,A=AES]: D
Key status? [L/T]: L <Return>
LMK component set [1-9]: 1 <Return>
Enter secret value A: AAAA AAAA AAAA AAAA <Return>
Enter secret value B: BBBB BBBB BBBB BBBB <Return>
Enter secret value C: CCCC CCCC CCCC CCCC <Return>
Insert blank card and enter PIN: ******** <Return>
Writing keys...
Checking keys...
Device write complete, check: ZZZZZZ

Remove the smartcard and store it securely.

Make another copy? [Y/N]: N <Return>
1 copies made.

Repeat the procedure to generate further components.

Secure>
```

Example 4:
(AES Key Block LMK)

This example generates a set of AES key block LMK components, and writes each component to a smartcard.

```
Secure> GK <Return>
Variant scheme or key block scheme? [V/K]: K <Return>
Enter algorithm type [D=DES,A=AES]: A <Return>
Enter the number of components to generate: [2-9]: 5
<Return>
Enter the number of components required to reconstitute
the LMK: [2-5]: 2 <Return>
Key status? [L/T]: L <Return>

Check value for the LMK: ZZZZZZ

Insert blank card and enter PIN: ******** <Return>
Writing keys...
Checking keys...
Device write complete, check: ZZZZZZ

Remove the smartcard and store it securely.

Insert blank card and enter PIN: ******** <Return>
Writing keys...
Checking keys...
Device write complete, check: ZZZZZZ

Remove the smartcard and store it securely.

The above sequence is repeated to generate each component
card.

Secure>
```

Load LMK (LK)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **LK**

Function: To load LMK components from smartcards.

Authorization: The HSM must be in the secure state to run this command.

Inputs:

- Confirm remote access (if already commissioned for remote access using the payShield Manager)
- LMK Identifier: 2 numeric digits.
- Optional comments
- Smartcards (RLMKs are supported) with LMK components.
- PINs for the Smartcards or passwords. The PIN must be entered within 60 seconds.
- Whether to make this LMK the Default/Management LMK - see Notes below.

Outputs:

- Individual LMK component check value(s).
- Final LMK check value.

Notes:

- For PCI HSM compliance, PINs and smartcards must be used to authenticate the Security Officers.
- Use of this command will always create an entry in the Audit Log.
- If there is not already a Default and/or Management LMK installed (i.e. the LMK IDs identified in the security settings as being the default and management LMKs are empty), you will be asked if you wish to make this new LMK the Default/Management LMK.
- An error is returned if an attempt is made to load an LMK with a single component where:
    - The LMK is not a test LMK, and
    - The security setting to enforce multiple key components has been set to YES.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Load failed check comparison - card is blank.
- Not a LMK card - card is not formatted for LMK or key storage.
- Card not formatted - card is not formatted.
- Smartcard error; command/return: 0003 - invalid PIN is entered.
- Invalid PIN; re-enter - a PIN of less than 5 or greater than 8 digits is entered.
- Invalid key – a standard Thales test key cannot be given live status.
- Incompatible key status – the components have different status ("live" or "test").
- Invalid key - Multiple key components required – an attempt has been made to load an LMK (other than a test LMK) using a single component when the security setting to enforce multiple components has been set to YES.

Example 1:
(Double-length
Variant LMK)

This example loads a double-length Variant LMK from smartcards and installs it in the HSM. There is already Default and Management LMKs installed.

```
Secure> LK <Return>
Enter LMK id: 00 <Return>
Enter comments: Live LMK for ABC Bank <Return>
LMK in selected location must be erased before
proceeding
Erase LMK? Y <Return>
Load LMK from components or shares
Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>

Check: AAAAAA
Load more components? [Y/N]: Y <Return>

Remove the smartcard. Insert the second and subsequent
smartcards and repeat the loading procedure. When all
components have been loaded and the HSM displays the LMK
Check value, record the check value.

LMK Check: ZZZZZZ
LMK id: 00
LMK key scheme: Variant
LMK algorithm: 3DES (2key)
LMK status: Live
Comments: Live LMK for ABC Bank
Confirm details? [Y/N]: Y <Return>
Use the LO/LN command to load LMKs into key change
storage.
Secure>
```

Example 2:
(Triple-length
Variant LMK)

This example loads a triple-length Variant LMK from smartcards and installs it in the HSM. There are already Default and Management LMKs installed.

```
Secure> LK <Return>
Enter LMK id: 01 <Return>
Enter comments: Process System One <Return>
LMK in selected location must be erased before
proceeding
Erase LMK? Y <Return>
Load LMK from components or shares
Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>

Check: AAAAAA
Load more components? [Y/N]: Y <Return>

Remove the smartcard. Insert the second and subsequent
smartcards and repeat the loading procedure. When all
components have been loaded and the HSM displays the LMK
Check value, record the check value.

LMK Check: ZZZZZZ
LMK id: 01
LMK key scheme: Variant
LMK algorithm: 3DES (3key)
LMK status: Live
```

```
Comments: Process System One
Confirm details? [Y/N]: Y <Return>
Use the LO/LN command to load LMKs into key change
storage.
Secure>
```

Example 3:
(Any LMK type)

In this example, the PIN is not entered within 60 seconds.

```
Secure> LK <Return>
Enter LMK id [0-9]: 0 <Return>
Enter comments: <Return>
Load LMK from components or shares
Insert card and press ENTER: <Return>
Enter PIN:
Terminated
Secure>
```

Example 4:
(Double- or triple-length Variant LMK)

In this example, the security setting requiring use of multiple components has been set to YES, but the user has attempted to load a non-Test LMK using only one component.

```
Secure> LK <Return>
Enter LMK id [0-4]: 0 <Return>
Enter comments: <Return>
Load LMK from components or shares
Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>

Check: AAAAAA
Load more components? [Y/N]: N <Return>
LMK Check: ZZZZZZ
Invalid key - Multiple key components required
Secure>
```

Example 5:
(3DES Key Block
LMK)

This example loads a 3DES key block LMK from smartcards and installs it in the HSM. There is already Default and Management LMKs installed.

```
Secure> LK <Return>
Enter LMK id: 01 <Return>
Enter comments: Live LMK for XYZ Bank <Return>
LMK in selected location must be erased before
proceeding
Erase LMK? Y <Return>
Load LMK from components or shares
Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>

Check: AAAAAA
Load more components? [Y/N]: Y <Return>
```

Remove the smartcard. Insert the second and subsequent smartcards and repeat the loading procedure. When all components have been loaded and the HSM displays the LMK Check value, record the check value.

```
LMK Check: ZZZZZZ
LMK id: 01
LMK key scheme: KeyBlock
LMK algorithm: 3DES(3key)
LMK status: Live
Comments: Live LMK for XYZ Bank
Confirm details? [Y/N]: Y <Return>
Use the LO/LN command to load LMKs into key change
storage.
Secure>
```

Example 6:
(AES Key Block LMK)

This example loads an AES key block LMK from smartcards and installs it in the HSM. There is already Default and Management LMKs installed.

```
Secure> LK <Return>
Enter LMK id: 02 <Return>
Enter comments: Live LMK for XYZ Bank <Return>
LMK in selected location must be erased before
proceeding
Erase LMK? Y <Return>
Load LMK from components or shares
Insert card and press ENTER: <Return>
PIN: ******** <Return>
Check: AAAAAA

Remove the smartcard. Insert the second and subsequent
smartcards and repeat the loading procedure. When all
components have been loaded and the HSM displays the LMK
Check value, record the check value.

LMK Check: ZZZZZZ
LMK id: 02
LMK key scheme: KeyBlock
LMK algorithm: AES-256
LMK status: Live
Comments: Live LMK for XYZ Bank
Confirm details? [Y/N]: Y <Return>
Use the LO/LN command to load LMKs into key change
storage.
Secure>
```

Example 7:
(AES Key Block LMK - no Default or Management LMK already installed.)

This example loads an AES key block LMK from smartcards and installs it in the HSM. There is no Default or Management LMK already installed.

```
Secure> LK <Return>
Enter LMK id: 02 <Return>
Enter comments: Live LMK for XYZ Bank <Return>

Load LMK from components or shares
Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>
Check: AAAAAA

Remove the smartcard. Insert the second and subsequent
smartcards and repeat the loading procedure. When all
components have been loaded and the HSM displays the LMK
Check value, record the check value.

LMK Check: ZZZZZZ
LMK id: 02
LMK key scheme: KeyBlock
LMK algorithm: AES-256
LMK status: Live
Comments: Live LMK for XYZ Bank
Confirm details? [Y/N]: Y <Return>
Use the LO/LN command to load LMKs into key change
storage.
Do you want to make this LMK the default LMK? [Y/N]: Y
<Return>
Do you want to make this LMK the management LMK? [Y/N]:
Y <Return>
Secure>
```

Load 'Old' LMK into Key Change Storage (LO)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Required** Activity: **admin.console**		

Command: **LO**

Function: To load an old LMK component set into Key Change Storage for use in translations from old to new keys. Note that the current LMK must be installed before an "old" LMK can be installed. Also note that it is possible to install a Variant LMK as the "old" LMK, and with a Key Block LMK as the "new" LMK.

Authorization: The HSM must be in the secure state to run this command. Additionally, the HSM must be either in the Authorized State, or the activity **admin.console** must be authorized, using the Authorizing Officer cards of the specified LMK.

Inputs:

- LMK identifier: 2 numeric digits.
- Smartcards (RLMKs are supported) with old LMK components.
- PINs for the Smartcards or passwords. PINs must be entered within 60 seconds of being requested.

Outputs:

- Individual LMK Component check value(s).
- Final LMK key check value.

Errors:

- No LMK loaded – there is no LMK loaded in main memory.
- Invalid LMK identifier – entered identifier out of range
- Key Block LMK not permitted – it is not permitted to load a Key Block LMK into key change storage if a variant LMK is loaded in main memory.
- Load failed check comparison – card is blank.
- Not a LMK card – card is not formatted for LMK or key storage.
- Card not formatted – card is not formatted.
- Smartcard error; command/return: 0003 – invalid PIN is entered.
- Invalid PIN; re-enter – a PIN of less than 4 or greater than 8 is entered.
- Command only allowed from Secure-Authorized – the HSM is not in Secure State, or the HSM is not authorized to perform this operation, or both.
- Invalid key – a standard Thales test key cannot be given live status.
- Incompatible cards – the component cards have different formats.
- Incompatible key status – the components have different status ("live" or "test").
- Invalid key - Multiple key components required – an attempt has been made to load an LMK (other than a Test LMK) using a single component when the security setting to enforce multiple components has been set to YES.

Notes:

- For PCI HSM compliance, PINs and smartcards must be used to authenticate the Security Officers.
- Use of this command will always create an entry in the Audit Log.
- It is not permitted to load a Key Block LMK into the "old" LMK slot of a Variant LMK.
- It is not permitted to load an AES Key Block LMK into the "old" LMK slot of a 3DES Key Block LMK.
- If multiple LMKs are loaded on the HSM, each can have a corresponding old LMK. The ID of the LMK being processed is defined in the command input.

Example 1:
(Double-length
Variant LMK)

This example loads a double-length Variant LMK from smartcards and installs it as 'old' LMK 00.

```
Secure-AUTH> LO <Return>
Enter LMK id: 00 <Return>
Enter comments: Old LMK for ABC Bank <Return>
Load old LMK from components or shares
Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>
Check: AAAAAA
Load more components? [Y/N]: Y <Return>
```

Remove the smartcard. Insert the second and subsequent smartcards and repeat the loading procedure until all old component sets have been loaded. When all components have been loaded and the HSM displays the LMK Check value, ensure that this is the expected value.

```
LMK Check: ZZZZZZ
LMK id: 00
LMK key scheme: Variant
LMK algorithm: 3DES (2key)
LMK status: Live
Comments: Old LMK for ABC Bank
Confirm details? [Y/N]: Y <Return>
Secure-AUTH>
```

Example 2: (Triple-length Variant LMK)

This example loads a triple-length Variant LMK from smartcards and installs it as 'old' LMK 00.

```
Secure-AUTH> LO <Return>
Enter LMK id: 00 <Return>
Enter comments: Old LMK for Process System One <Return>
Load old LMK from components or shares
Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>
Check: AAAAAA
Load more components? [Y/N]: Y <Return>
```

Remove the smartcard. Insert the second and subsequent smartcards and repeat the loading procedure until all old component sets have been loaded. When all components have been loaded and the HSM displays the LMK Check value, ensure that this is the expected value.

```
LMK Check: ZZZZZZ
LMK id: 00
LMK key scheme: Variant
LMK algorithm: 3DES (3key)
LMK status: Live
Comments: Old LMK for Process System One
Confirm details? [Y/N]: Y <Return>
Secure-AUTH>
```

Example 3: (Double- or triple-length Variant LMK)

This example attempts to load a non-Test LMK using a single component when the security setting to enforce multiple components has been set to YES.

```
Secure-AUTH> LO <Return>
Enter LMK id: 00 <Return>
Enter comments: Old LMK for ABC Bank <Return>
Load old LMK from components or shares
Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>
Check: AAAAAA
Load more components? [Y/N]: N <Return>
Check: AAAAAA
Invalid key - Multiple key components required
Secure-AUTH>
```

Example 4: (3DES Key Block LMK)

This example loads a 3DES key block LMK from smartcards and installs it as 'old' LMK 01.

```
Secure-AUTH> LO <Return>
Enter LMK id: 01 <Return>
Enter comments: Old LMK for XYZ Bank <Return>
Load old LMK from components or shares
Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>
Check: AAAAAA
Load more components? [Y/N]: Y <Return>
```

Remove the smartcard. Insert the second and subsequent smartcards and repeat the loading procedure until all old component sets have been loaded. When all components have been loaded and the HSM displays the LMK Check value, ensure that this is the expected value.

```
LMK Check: ZZZZZZ
LMK id: 01
LMK key scheme: KeyBlock
LMK algorithm: 3DES (3key)
LMK status: Live
Comments: Old LMK for XYZ Bank
Confirm details? [Y/N]: Y <Return>
Secure-AUTH>
```

Example 5:
(AES Key Block LMK)

This example loads an AES key block LMK from smartcards and installs it as 'old' LMK 02.

```
Secure-AUTH> LO <Return>
Enter LMK id: 02 <Return>
Enter comments: Old LMK for XYZ Bank <Return>
Load old LMK from components or shares

Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>
Check: AAAAAA
```

Remove the smartcard. Insert the second and subsequent smartcards and repeat the loading procedure until all old component sets have been loaded. When all components have been loaded and the HSM displays the LMK Check value, ensure that this is the expected value.

```
LMK Check: ZZZZZZ
LMK id: 02
LMK key scheme: KeyBlock
LMK algorithm: AES-256
LMK status: Live
Comments: Old LMK for XYZ Bank
Confirm details? [Y/N]: Y <Return>
Secure-AUTH>
```

Load 'New' LMK into Key Change Storage (LN)

Variant ☑		Key Block ☑
Online ☒	Offline ☒	Secure ☑
Authorization: **Required** Activity: **admin.console**		

Command:	**LN**
Function:	To load a new LMK component set into Key Change Storage for use in translations from the current LMK to a "new" LMK. Note that the current LMK must be installed before a "new" LMK can be installed. Also note that it is possible to install a Key Block LMK as the "new" LMK, with a Variant LMK as the current LMK.
Authorization:	The HSM must be in the secure state to run this command. Additionally, the HSM must be either in the Authorized State, or the activity **admin.console** must be authorized, using the Authorizing Officer cards of the specified LMK.
Inputs:	• LMK identifier: 2 numeric digits. • Smartcards (regular HSM or payShield Manager smartcards) with new LMK components. • PINs for the Smartcards or passwords. PINs must be entered within 60 seconds of being requested.
Outputs:	• Individual LMK Component check value(s). • Final LMK key check value.
Errors:	• No LMK loaded – there is no LMK loaded in main memory. • Invalid LMK identifier – entered identifier out of range • Key Block LMK not permitted – it is not permitted to load a key block LMK into key change storage if a variant LMK is loaded in main memory. • Load failed check comparison – card is blank. • Not a LMK card – card is not formatted for LMK or key storage. • Card not formatted – card is not formatted. • Smartcard error; command/return: 0003 – invalid PIN is entered. • Invalid PIN; re-enter – a PIN of less than 4 or greater than 8 is entered. • Command only allowed from Secure-Authorized – the HSM is not in Secure State, or the HSM is not authorized to perform this operation, or both. • Invalid key – a standard Thales test key cannot be given live status. • Incompatible cards – the component cards have different formats. • Incompatible key status – the components have different status ("live" or "test"). • Invalid key - Multiple key components required – an attempt has been made to load an LMK (other than a Test LMK) using a single component when the security setting to enforce multiple components has been set to YES.
Notes:	• For PCI HSM compliance, PINs and smartcards must be used to authenticate the Security Officers. • Use of this command will always create an entry in the Audit Log. • It is not permitted to load a Variant LMK into the "new" LMK slot of a Key Block LMK. • It is not permitted to load a 3DES Key Block LMK into the "new" LMK slot of an AES Key Block LMK. • If multiple LMKs are loaded on the HSM, each can have a corresponding 'new' LMK. The ID of the LMK being processed is defined in the command input.

Example 1:
(Double-length
Variant LMK)

This example loads a double-length Variant LMK from smartcards and installs it as 'new' LMK 00.

```
Secure-AUTH> LN <Return>
Enter LMK id: 00 <Return>
Enter comments: New LMK for ABC Bank <Return>
Load new LMK from components or shares
Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>
Check: AAAAAA
Load more components? [Y/N]: Y <Return>
```

Remove the smartcard. Insert the second and subsequent smartcards and repeat the loading procedure until all new component sets have been loaded. When all components have been loaded and the HSM displays the LMK Check value, ensure that this is the expected value.

```
LMK Check: ZZZZZZ
LMK id: 00
LMK key scheme: Variant
LMK algorithm: 3DES(2key)
LMK status: Live
Comments: New LMK for ABC Bank
Confirm details? [Y/N]: Y <Return>
Secure-AUTH>
```

Example 2:
(Triple-length Variant LMK)

This example loads a triple-length Variant LMK from smartcards and installs it as 'new' LMK 00.

```
Secure-AUTH> LN <Return>
Enter LMK id: 00 <Return>
Enter comments: New LMK for Process System One <Return>
Load new LMK from components or shares
Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>
Check: AAAAAA
Load more components? [Y/N]: Y <Return>
```

Remove the smartcard. Insert the second and subsequent smartcards and repeat the loading procedure until all new component sets have been loaded. When all components have been loaded and the HSM displays the LMK Check value, ensure that this is the expected value.

```
LMK Check: ZZZZZZ
LMK id: 00
LMK key scheme: Variant
LMK algorithm: 3DES (3key)
LMK status: Live
Comments: New LMK for Process System One
Confirm details? [Y/N]: Y <Return>
Secure-AUTH>
```

Example 3:
(Double- or triple-length Variant LMK)

This example attempts to load a non-Test LMK using a single component when the security setting to enforce multiple components has been set to YES.

```
Secure-AUTH> LN <Return>
Enter LMK id: 00 <Return>
Enter comments: New LMK for ABC Bank <Return>
Load new LMK from components. Or shares
Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>
Check: AAAAAA
Load more components? [Y/N]: N <Return>
Check: AAAAAA
Invalid key - Multiple key components required
Secure-AUTH>
```

Example 4:
(3DES Key Block LMK)

This example loads a 3DES key block LMK from smartcards and installs it as 'new' LMK 01.

```
Secure-AUTH> LN <Return>
Enter LMK id: 01 <Return>
Enter comments: New LMK for XYZ Bank <Return>
Load new LMK from components or shares
Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>
Check: AAAAAA
Load more components? [Y/N]: Y <Return>
```

Remove the smartcard. Insert the second and subsequent smartcards and repeat the loading procedure until all new component sets have been loaded. When all components have been loaded and the HSM displays the LMK Check value, ensure that this is the expected value.

```
LMK Check: ZZZZZZ
LMK id: 01
LMK key scheme: KeyBlock
LMK algorithm: 3DES(3key)
LMK status: Live
Comments: New LMK for XYZ Bank
Confirm details? [Y/N]: Y <Return>
Secure-AUTH>
```

Example 5:
(AES Key Block LMK)

This example loads an AES key block LMK from smartcards and installs it as 'new' LMK 02.

```
Secure-AUTH> LN <Return>
Enter LMK id: 02 <Return>
Enter comments: New LMK for XYZ Bank <Return>
Load new LMK from components or shares
Insert card and press ENTER: <Return>
Enter PIN: ******** <Return>
Check: AAAAAA
```

Remove the smartcard. Insert the second and subsequent smartcards and repeat the loading procedure until all new component sets have been loaded. When all components have been loaded and the HSM displays the LMK Check value, ensure that this is the expected value.

```
LMK Check: ZZZZZZ
LMK id: 02
LMK key scheme: KeyBlock
LMK algorithm: AES-256
LMK status: Live
Comments: New LMK for XYZ Bank
Confirm details? [Y/N]: Y <Return>
Secure-AUTH>
```

Verify LMK Store (V)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **V**

Function: To confirm that the check value is identical to the value that was recorded when the LMK set was installed.
For Variant LMKs, the length of the displayed check value is determined by the CS (Configure Security) setting "Restrict Key Check Value to 6 hex chars".
For Key Block LMKs, the length of the displayed check value is always 6 hex digits.

Authorization: The HSM does not require any authorization to run this command.

Inputs:
- LMK Identifier: 2 numeric digits.

Outputs:
- Master key check value.

Errors:
- Invalid LMK identifier - no LMK loaded or entered identifier out of range.

Example:

```
Online> V <Return>
Enter LMK id: 03 <Return>
Check: ZZZZZZ
Online>
```

Duplicate LMK Component Sets (DC)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☒</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **DC**

Function: To copy an LMK component onto another smartcard.

Authorization: The HSM must be in the secure state to run this command.

Inputs:

- Smartcard (RLMKs are supported) with LMK component.
- PIN for the smartcard. PINs must be entered within 60 seconds of being requested.

Outputs:

- LMK check value.

Errors:

- Load failed check comparison - card is blank
- Not a LMK card - card is not formatted for LMK or key storage.
- Card not formatted - card is not formatted
- Smartcard error; command/return: 0003 - invalid PIN is entered
- Invalid PIN; re-enter - a PIN of less than 4 or greater than 8 is entered.
- Warning - card not blank. Proceed? [Y/N] - LMK card is not blank
- Overwrite LMK set? [Y/N] - the smartcard already contains an LMK component. It can be overwritten if desired.

Example:

```
Secure> DC <Return>
Insert card to be duplicated and press ENTER: <Return>
Enter PIN: ******** <Return>
Insert blank card and enter PIN: ******** <Return>
Writing keys...
Checking keys...
Device write complete, check: ZZZZZZ
Secure>
```

Delete LMK (DM)

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

Command: **DM**

Function: To delete a selected LMK and (if loaded) the LMK in the corresponding location in key change storage.

Authorization: The HSM must be in the secure state to run this command. Additionally, the HSM must be either in the Authorized State, or the activity **admin.console** must be authorized, using the Authorizing Officer cards of the specified LMK.

Inputs:

- LMK Identifier: 2 numeric digits.

Outputs:

- Display of relevant entry from LMK table and the key change storage table.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Command only allowed from Secure-Authorized - the HSM is not in Secure State, or the HSM is not authorized to perform this operation, or both.
- LMK id xx is the Default and Management LMK ID – the default and Management LMKs cannot be deleted.

Notes:

- LMKs which are the Default or Management LMK cannot be deleted. The Default and Management LMK must be re-assigned to a new LMK before the desired LMK can be deleted. (The LMK ID of the Management and default LMKs can be viewed by running the QS command.)

Example:

```
Secure-AUTH> DM <Return>
Enter LMK id: 01 <Return>

LMK table entry:
ID Auth     Scheme    Algorithm  Status Check  Comments
01 Yes(1)   KeyBlock  3DES(3key) Test   ZZZZZZ Test LMK
for XYZ Bank

Key change storage table entry:
ID          Scheme    Algorithm  Status Check  Comments
01          Variant   3DES(2key) Test   ZZZZZZ Old test
LMK for XYZ Bank

Confirm LMK deletion [Y/N]: Y <Return>
LMK deleted from main memory and key change storage

Secure>
```

Delete 'Old' or 'New' LMK from Key Change Storage (DO)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☒</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **DO**

Function: To delete a selected LMK from key change storage. This command may only be used if an LMK is loaded in the corresponding location in main LMK memory.

Authorization: The HSM must be in the secure state to run this command.

Inputs:

- LMK Identifier: 2 numeric digits.

Outputs:

- Display of relevant entry from the key change storage table.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.

Example:

```
Secure> DO <Return>
Enter LMK id: 01 <Return>

Key change storage table entry:
ID    Scheme    Algorithm  Status Check  Comments
01    Variant   3DES(2key) Test   ZZZZZZ Old test LMK for
XYZ Bank

Confirm LMK deletion [Y/N]: Y <Return>
LMK deleted from key change storage

Secure>
```

View LMK Table (VT)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☑</td><td colspan="2">Offline ☑</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **VT**

Function: To display the LMK table and the corresponding table for key change storage.

Authorization: The HSM does not require any authorization to run this command.

Inputs: None.

Outputs:

- Displayed LMK table and key change storage table.
- For each LMK currently installed, the following information is displayed:
  - ID – identifier selected during installation of this LMK.
  - Auth – current authorized status:
    - No – not authorized state/activities not active;
    - Yes – authorized state is active;
    - Yes (nX) – 'n' authorized activities are active (if HSM is configured for multiple authorized activities), with X identifying whether ***H***ost or ***C***onsole commands.
    - (Note that LMKs in key change storage cannot be authorized.)
  - Old/New – Status of key in Key Change Storage
    - Old – key is treated as an 'old' LMK
    - New – key is treated as a 'new' LMK
    - (Note that only LMKs held in Key Change Storage have the Old/New status.)
  - Scheme – The LMK scheme:
    - Variant – indicating a Variant LMK
    - Key Block – indicating a Key Block LMK
  - Algorithm – the LMK algorithm:
    - 3DES (2key) – indicating a double-length TDES Variant LMK
    - 3DES (3key) – indicating a triple-length TDES Variant or triple-length (3DES) Key Block LMK
    - AES-256 – indicating an AES Key Block LMK.
  - Status – the LMK status, selected during generation of the LMK.
    - Live – LMK is a 'live' LMK.
    - Test – LMK is a 'test' LMK.
  - Check – the check value of the LMK.
  - Comments – the comments entered during installation of this LMK.

Errors: None.

Example 1: *The HSM is configured for single authorized state, but has not been authorized*:

```
Secure> VT <Return>

LMK table:
ID Authorized  Scheme   Algorithm  Status Check  Comments
00 No          Variant  3DES(2key) Test   268604 test
variant

Key change storage table:No keys loaded in key change
storage

Secure>
```

Example 2: *The HSM is configured for single authorized state, and both host and console commands are authorized for LMK 01*:

```
Secure> VT <Return>

LMK table:

ID Authorized  Scheme   Algorithm  Status Check  Comments
00 No          Variant  3DES(2key) Test   268604 test
variant
01 Yes(1H,1C)  Variant  3DES(2key) Test   268604 test
variant
02 Yes(1H,1C)  Variant  3DES(3key) Live   554279
Production 1
Key change storage table:No keys loaded in key change
storage

Secure>
```

Example 3: *The HSM is configured for single authorized state, and only host commands are authorized for LMK 01 (console command authorization has automatically expired after 12 hours)*:

```
Secure> VT <Return>

LMK table:

ID Authorized  Scheme   Algorithm  Status Check  Comments
00 No          Variant  3DES(2key) Test   268604 test
variant
01 Yes(1H,0C)  KeyBlock AES-256    Live   963272 Mngmnt
LMK
Key change storage table:No keys loaded in key change
storage

Secure>
```

Example 4: *The HSM is configured for multiple authorized activities. Output shows how many host and console commands are authorized for each LMK:*

```
Online-AUTH> VT <Return>

LMK table:
ID Authorized  Scheme   Algorithm  Status Check  Comments
00 Yes(0H,1C)  Variant  3DES(3key) Live   726135 test variant
02 Yes(1H,0C)  KeyBlock AES-256    Test   6620CA Mngmnt LMK
Key change storage table:
ID Old/New     Scheme   Algorithm  Status Check  Comments
00 New         KeyBlock 3DES(3key) Live   331873 test variant 2
02 New         KeyBlock AES-256    Test   9D04A0 New mngmnt LMK

Online-AUTH>
```

Generate Test LMK (GT)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **GT**

Function: To generate one of the standard Thales Test LMKs, and write the component(s) to smartcard(s).
The payShield 10K supports four different types of LMK:

- 2DES Variant LMK
- 3DES Variant LMK
- 3DES Key Block LMK
- AES Key Block LMK

All three DES-based Test LMKs can be stored on a single smartcard; the AES Test LMK requires two smartcards.

Note: This command simply generates a smart card with the known and documented test LMK stored on it. The command does not generate a new test LMK.

Authorization: The HSM does not require any authorization to run this command.

Inputs:

- Type of Test LMK to be generated.
- Prompts for smartcards to be inserted & PINs to be entered.

Outputs:

- Confirmation of Test LMK components being written to smartcards.
- Prompts to make additional copies.

Errors:

- Card not formatted – use the FC command to format the card.
- Not a LMK card –card is not formatted for LMK or key storage.
- Warning – card not blank. Proceed? [Y/N] – LMK card is not blank.
- Overwrite LMK set? [Y/N] – card already contains an LMK component.
- Invalid selection.
- Invalid PIN.

Example 1: *This example writes the standard 2DES Variant Thales Test LMK to a single smartcard:*

```
Online> GT <Return>

Generate Standard Thales Test LMK Set:
  1 - 2DES Variant
  2 - 3DES Variant
  3 - 3DES KeyBlock
  4 - AES KeyBlock
Select Standard Thales Test LMK set to be generated: 1
<Return>
Insert blank card and enter PIN: **** <Return>
Writing keys...
Checking keys...
Device write complete, check: ZZZZZZ

Make another copy? [Y/N]: N <Return>
1 copies made.

Do you want to generate another Standard Thales Test LMK
set [Y/N]: N <Return>

Online>
```

Example 2: *This example writes the two components of the standard AES Key Block Thales Test LMK to two separate smartcards:*

```
Online> GT <Return>

Generate Standard Thales Test LMK Set:
  1 - 2DES Variant
  2 - 3DES Variant
  3 - 3DES KeyBlock
  4 - AES KeyBlock
Select Standard Thales Test LMK set to be generated: 4
<Return>
Insert blank card and enter PIN: **** <Return>
Writing keys...
Checking keys...
Device write complete, check: ZZZZZZ
Insert blank card and enter PIN: **** <Return>
Writing keys...
Checking keys...
Device write complete, check: ZZZZZZ

Do you want to generate another Standard Thales Test LMK
set [Y/N]: N <Return>

Online>
```

Operational Commands

Authorization Commands

The payShield 10K needs to be authorized for certain commands to be executed - usually those involving clear text data.

There are two methods of authorizing the HSM – using:

- a single Authorized State;
- multiple Authorized Activities.

*Note: The console command CS (*Configure Security*) setting "Enable multiple authorized activities" determines which method is to be used; by default, multiple Authorized Activities are used.*

If the HSM needs to be placed in Authorized State using the Authorizing Officer cards (or passwords) corresponding to a particular LMK, then the command will only be authorized for that particular LMK identifier. For example, if the "FK" console command ("Form Key from Components") is authorized using the passwords corresponding to the LMK with identifier "00", then only keys encrypted using LMK "00" may be formed using the command.

It is possible to authorize the HSM using multiple Authorizing Officer cards (or passwords), so that the HSM may be simultaneously authorized for different LMKs.

Note: For PCI HSM compliance, PINs and smartcards must be used to authenticate the Security Officers: passwords must not be used.

The payShield 10K provides the following console commands to support the authorization of the HSM:

Command	Page
Enter the Authorized State (A)	**321**
Cancel Authorized Activity (C)	**334**
Authorize Activity (A)	**324**
Cancel Authorized Activity (C)	**334**
View Authorized Activities (VA)	**336**

Enter the Authorized State (A)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **A**

Function: To set the HSM into the Authorized State.
The HSM prompts for either Smartcards or Passwords, as applicable, which must correspond to the LMK being authorized.

Authorization: The HSM does not require any authorization to run this command.

Inputs:

- LMK Identifier: 1 or 2 numeric digits.
- PIN (if applicable): 5 to 8 alphanumeric characters. The PIN must be entered within 60 seconds. (4-digit PINs on legacy cards will also be accepted.)
- Either:
    - Smartcards (RLMKs are supported) with authorizing both passwords.
    - Password: 16 alphanumeric characters.

Outputs:

- Text messages as shown in examples.

Notes:

- If the CS setting "Card/Password authorization" is set to "Card", then the passwords required to put the HSM into the Authorized State will be read from smartcards. Note that only the first 2 LMK component cards contain passwords.
- This command is only available when the console command CS (Configure Security) setting "Enable multiple authorized activities [Y/N]" is set to "N".
- For PCI HSM compliance, authentication must use smartcards and PINs, not passwords.
- Use of this command will always cause an entry to be made in the Audit Log.
- Console commands remain authorized for 12 hours (720 minutes).

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Card not formatted - card is not formatted.
- Not an LMK card - card is not formatted for LMK or key storage.
- Smartcard error; command/return: 0003 - invalid PIN is entered.
- Invalid PIN; re-enter - a PIN of less than 5 or greater than 8 digits is entered.
- Data invalid; please re-enter - the password is an invalid length.

Example 1: *This example authorizes the HSM using smartcards.*

```
Online> A <Return>
Enter LMK id [0-9]: 00 <Return>
First Officer:
Insert card and enter PIN: ******** <Return>
Second Officer:
Insert card and enter PIN: ******** <Return>
AUTHORIZED
Console authorizations will expire in 720 minutes (12
hours).
Online-AUTH>
```

Example 2: *This example authorizes the HSM using passwords.*

```
Online> A <Return>
Enter LMK id [0-4]: 1 <Return>
```

```
First Officer:
Password: **************** <Return>
Second Officer:
Password: ******************* <Return>            ←
Password too long
Data invalid; please re-enter: **************** <Return>
AUTHORIZED
Console authorizations will expire in 720 minutes (12
hours).

Online-AUTH>
```

Cancel the Authorized State (C)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **C**

Function: To cancel the Authorized State.
There is an equivalent command available to the host (Host command 'RA')

Authorization: The HSM does not require any authorization to run this command.

Inputs:

- LMK Identifier: 2 numeric digits.

Outputs:

- Text messages as shown in example.

Notes:

- This command is only available when the console command CS (Configure Security) setting "Enable multiple authorized activities [Y/N]" is set to "N".
- Use of this command will always cause an entry to be made in the Audit Log.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.

Example 1:

```
Online-AUTH> C <Return>
Enter LMK id [0-9]: 00 <Return>
NOT AUTHORIZED for LMK id 00
Online>
```

Authorize Activity (A)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☑</td><td colspan="2">Offline ☑</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **A**

Function: To authorize the HSM to perform certain specified activities.

In command line mode, the operator specifies which activities are to be authorized.

In menu mode, the operator is prompted to enter the activities.

In both cases, the specified activities are authorized by submitting two Security Officer cards or passwords, which must correspond to the LMK being authorized.

Authorized activities can be made persistent, in which case they are retained even if the power to the HSM is cycled.

Authorization: The HSM does not require any authorization to run this command.

Inputs:

- LMK Identifier: 2 numeric digits
- Activities to be authorized.
- Timeout value: Number of minutes before HSM will revoke chosen authorized activity. Where the security setting *Enforce Authorization Time Limit* has been set to "YES" (i.e. to the PCI HSM compliant value) then console commands can be authorized for a maximum period of 12 hours (720 minutes).
- PIN (if applicable): 5 to 8 alphanumeric characters. The PIN must be entered within 60 seconds of being requested. (4-digit PINs on legacy cards will also be accepted.)
- Either:
  - o Smartcards (RLMKs are supported) with authorizing both passwords.
  - o Password: 16 alphanumeric characters.
- Use "-h" to display help.

Outputs:

- Text messages as shown in examples.

Syntax: Syntax: **A** [<*Activity*>] [<*Activity*>] ...

Activity: <*Category*>.[<*Sub-category*>].[<*Interface*>][:<*Timeout*>]

Category = generate|component|genprint|import|export|pin|audit|admin|diag| misc| command

Sub-category (for 'generate|import|export') = key type code, e.g. 001 for ZPK.

Sub-category (for 'pin') = mailer|clear

Interface = host|console

Timeout = value in minutes or 'p' for persistent. (A maximum of 12 hours (720 minutes) is applied to Console commands.}

Names may be shortened but must remain unique.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Card not formatted - card is not formatted.
- Not a LMK card - card is not formatted for LMK or key storage.
- Smartcard error; command/return: 0003 - invalid PIN is entered.
- Invalid PIN; re-enter - a PIN of less than 4 or greater than 8 is entered.

- Data invalid; please re-enter: the password is an invalid length.

Notes:

- If the CS setting "Card/Password authorization" is set to "Card", then the passwords required to put the HSM into the Authorized State will be read from smartcards. Note that only the first 2 LMK component cards contain passwords.
- This command is only available when the console command CS (Configure Security) setting "Enable multiple authorized activities [Y/N]" is set to "Y".
- For PCI HSM compliance, the following security settings must be set:
  - user authentication must be by smartcard and PIN, and not by using passwords.
  - Authorization time limit for Console commands must be enforced.
- Where the security setting *Enforce Authorization Time Limit* has been set to "YES" (i.e. to the PCI HSM compliant value) then console commands can be authorized for a maximum period of 12 hours (720 minutes).
- Use of this command will always cause an entry to be made in the Audit Log.
- Activities are described in terms of four fields: Category, Sub-Category, Interface and Timeout. If the Timeout field is omitted, the activity remains authorized until cancelled either by the console command "C" or the host command "RA".
- Omitting either the Sub-Category and/or the Interface field is equivalent to authorizing multiple activities consisting of all possible combinations of valid values for the missing fields. For clarification:

  pin.mailer

  is equivalent to:

  pin.mailer.host

  pin.mailer.console

  and:

  pin

  is equivalent to:

  pin.clear.console

  pin.clear.host

  pin.mailer.console

  pin.mailer.host
- When authorizing activities, two (or more) activities may overlap, for example:

  pin

  pin.mailer
- There is no requirement to attempt to reduce activities to the minimum set. The list of authorized activities simply consists of all those entered (and authorized) by the user.

- There is one case when it will be necessary to overwrite an existing activity: when only the Timeout field changes. For example, suppose that the following activity is authorized:

  export.001.console:11

  and the user uses the 'A' command to authorize the following activity:

  export.001.console:60

  then this should overwrite the first one (even if the newer activity has a shorter *Timeout* value).
- Note: When omitting the sub-category, but including the interface, there should be two delimiters "." between them:

  Example: export..host allows export of any (valid) key using a host command.
- The option to make an authorization persistent (i.e. to survive across a re-boot of the HSM) is only available for Host commands and where the authorization is also permanent.

Example 1:
(Variant or Key
Block LMK)

This example authorizes a single activity via the menu.

```
Online> A <Return>
Enter LMK id [0-9]: 0 <Return>
No activities are authorized for LMK id 00.
List of authorizable activities:
generate    genprint    component   import
export      pin   audit admin
diagnostic  misc  command
Select category: pin <Return>
clear mailer
Select sub-category, or <RETURN> for all: mailer <Return>
host  console
Select interface, or <RETURN> for all: <Return>
Enter time limit for pin.mailer, or <RETURN> for
permanent: <Return>
Make activity persistent? [Y/N]: N <Return>
Enter additional activities to authorize? [y/N]: N
<Return>

The following activities are pending authorization for
LMK id 00:
pin.mailer

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

The following activities are authorized for LMK id 00:
pin.mailer

Online-AUTH>
```

Example 2:
(Variant or Key
Block LMK)

This example authorizes activities via the command line, with no time limits specified.

```
Online> A gene comp genp i e p au ad di m comm<Return>
```

```
Enter LMK id [0-4]: 0 <Return>

Console authorizations will expire in 720 minutes (12
hours).

The following activities are pending authorization for
LMK id 00:

admin..console:720
admin..host
audit..console:720
audit..host
command..console:720
command..host
component..console:720
component..host
diagnostic..console:720
diagnostic..host
export..console:720
export..host
generate..console:720
generate..host
genprint..console:720
genprint..host
import..console:720
import..host
misc..console:720
misc..host
pin..console:720
pin..host

First officer:
Insert card and enter PIN: ********<Return>

Second officer:
Insert card and enter PIN: ********<Return>

The following activities are authorized for LMK id 00:

admin..console:720  (720 mins remaining)
admin..host
audit..console:720  (720 mins remaining)
audit..host
command..console:720  (720 mins remaining)
command..host
component..console:720  (720 mins remaining)
component..host
diagnostic..console:720  (720 mins remaining)
diagnostic..host
export..console:720  (720 mins remaining)
export..host
generate..console:720  (720 mins remaining)
generate..host
genprint..console:720  (720 mins remaining)
genprint..host
import..console:720  (720 mins remaining)
import..host
misc..console:720  (720 mins remaining)
misc..host
```

```
pin..console:720  (720 mins remaining)
pin..host

Online-AUTH>
```

Example 3:
(Variant LMK)

This example authorizes three activities additional Example 1 via the menu.

```
Online-AUTH> A <Return>
Enter LMK id [0-9]: 00 <Return>
The following activities are authorized for LMK id 00:
pin.mailer
List of authorizable activities:
generate    genprint    component   import
export      pin   audit admin
diagnostic  misc  command
Select category: generate <Return>
000   100   200   001
002   400   003   006
008   009   109   209
309   409   509   709
00a   00b   rsa
Select sub-category, or <RETURN> for all: 000 <Return>
host  console
Select interface, or <RETURN> for all: C <Return>
Enter time limit for generate.000.console, or <RETURN>
for permanent: 60 <Return>

Enter additional activities to authorize? [y/N]: Y
<Return>
List of authorizable activities:
generate    genprint    component   import
export      pin   audit admin
diagnostic  misc  command
Select category: export <Return>
000   100   200   001
002   400   003   006
008   009   109   209
309   409   509   709
00a   00b   rsa
Select sub-category, or <RETURN> for all: 001 <Return>
host  console
Select interface, or <RETURN> for all: H <Return>
Enter time limit for export.001.host, or <RETURN> for
permanent: <Return>
Make activity persistent? [Y/N]: n <Return>

Enter additional activities to authorize? [y/N]: Y
<Return>
List of authorizable activities:
generate    genprint    component   import
export      pin   audit admin
diagnostic  misc  command
Select category: admin <Return>
host  console
Select interface, or <RETURN> for all: c <Return>
Enter time limit for admin, or <RETURN> for permanent:
240 <Return>

Enter additional activities to authorize? [y/N]: n
<Return>
The following activities are pending authorization for
LMK id 00:
admin..console:240
export.001.host
generate.000.console:60
```

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

The following activities are authorized for LMK id 00:
admin:240 (240 mins remaining)
export.001.host
generate.000.console:60 (60 mins remaining)
pin.mailer

Online-AUTH>
```

Example 4:
(Variant LMK)

This example authorizes three activities additional to Example 1 via the command line, including time limits.

```
Online-AUTH> A gene.000.con:60 exp.001.host:p admin:240
<Return>
Enter LMK id [0-19]: 00 <Return>

The following activities are pending authorization for
LMK id 00:

admin:240
export.001.host:persistent
generate.000.console:60

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

The following activities are authorized for LMK id 01:

admin:240  (240 mins remaining)
export.001.host:persistent
generate.000.console:60  (60 mins remaining)

Online-AUTH>
```

Example 5:
(Variant or Key Block LMK)

This example authorizes a single activity via the command line.

```
Online> A pin.clear <Return>
Enter LMK id [0-9]: 01 <Return>

Console authorizations will expire in 720 minutes (12
hours).

The following activities are pending authorization for
LMK id 01:

pin.clear.console:720
pin.clear.host

First Officer:
```

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

The following activities are authorized for LMK id 01:

pin.clear.console:720  (720 mins remaining)
pin.clear.host

Online-AUTH>
```

Example 6:
(Key Block LMK)

This example authorizes an additional three activities via the menu.

```
Online-AUTH> A <Return>
Enter LMK id [0-9]: 01 <Return>
The following activities are authorized for LMK id 01:
pin.clear
List of authorizable activities:
generate    genprint    component   import
export      pin   audit admin
diagnostic  misc  command
Select category: export <Return>
01    B0    C0    11
12    13    D0    21
22    E0    E1    E2
E3    E4    E5    E6
31    32    K0    51
52    M0    M1    M2
M3    M4    M5    61
62    63    64    65
P0    71    72    73
V0    V1    V2
Select sub-category, or <RETURN> for all: 72 <Return>
host  console
Select interface, or <RETURN> for all: C <Return>
Enter time limit for export.72.console, or <RETURN> for
permanent: 60 <Return>

Enter additional activities to authorize? [y/N]: Y
<Return>
List of authorizable activities:
generate    genprint    component   import
export      pin   audit admin
diagnostic  misc  command
Select category: admin <Return>
host  console
Select interface, or <RETURN> for all: <Return>
Enter time limit for admin, or <RETURN> for permanent:
240 <Return>

Enter additional activities to authorize? [y/N]: Y
<Return>
List of authorizable activities:
generate    genprint    component   import
export      pin   audit admin
diagnostic  misc  command
Select category: misc <Return>
```

```
host  console
Select interface, or <RETURN> for all: c <Return>
Enter time limit for admin, or <RETURN> for permanent:
<Return>
Make activity persistent? [Y/N]: n <Return>

Enter additional activities to authorize? [y/N]: n
<Return>
The following activities are pending authorization for
LMK id 00:
misc..console
admin:240
export.72.console:60

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

The following activities are authorized for LMK id 01:
misc..console
admin:240 (240 mins remaining)
export.72.console (60 mins remaining)
pin.clear

Online-AUTH>
```

Example 7:
(Key Block LMK)

This example authorizes an additional three activities via the command line.

```
Online-AUTH> a exp.001.con:60 admin:240 misc..console
<Return>
Enter LMK id [0-1]: 01 <Return>

Console authorizations will expire in 720 minutes (12
hours).

The following activities are pending authorization for
LMK id 01:

admin:240
export.001.console:60
misc..console:720

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

The following activities are authorized for LMK id 01:

admin:240  (228 mins remaining)
export.001.console:60  (60 mins remaining)
export.001.host:persistent
generate.000.console:60  (48 mins remaining)
misc..console:720  (720 mins remaining)
pin.clear.console:720  (712 mins remaining)
```

```
                pin.clear.host

                Online-AUTH>
```

Cancel Authorized Activity (C)

<table>
<tr><td>Variant ☑</td><td colspan="2">Key Block ☑</td></tr>
<tr><td>Online ☑</td><td>Offline ☑</td><td>Secure ☑</td></tr>
<tr><td colspan="3">Authorization: <b>Not required</b></td></tr>
</table>

Command: **C**

Function: To cancel one or more Authorized Activities.

Authorization: The HSM does not require any authorization to run this command.

Inputs:

- LMK Identifier: 2 numeric digits.

Outputs:

- Text messages as shown in examples.

Notes:

- This command is only available when the console command CS (Configure Security) setting "Enable multiple authorized activities [Y/N]" is set to "Y".

Syntax: **C** [<*Activity*>] [<*Activity*>] ...

Activity: <*Category*>[.<*Sub-category*>][.<*Interface*>][:<*Timeout*>]

Category = generate|component|genprint|import|export|pin|audit|admin|diag| misc| command

Sub-category (for 'generate|import|export') = key name, e.g. TPK, MK-AC, etc.

Sub-category (for 'pin') = mailer|clear

Interface = host|console

Timeout = value in minutes or 'p' for persistent

Names may be shortened but must remain unique.

When canceling an authorized activity which includes a timeout, the original value of the timeout should be specified.

Note: When omitting the sub-category, but including the interface, there should be two delimiters "." between them:

Example: export..host allows export of any (valid) key using a host command.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Invalid input.

Notes:

- Use of this command will always cause an entry to be made in the Audit Log.

Example 1:
(Variant or Key
Block LMK)

This example cancels an existing activity via the menu.

```
Online-AUTH> C <Return>
Enter LMK id [0-9]: 00 <Return>
Cancel pin.mailer? [y/N] Y <Return>
No activities are authorized for LMK id 00.
Online>
```

Note: This example assumes that the activities in the Authorize Activity command Example 1 (above) are active.

Example 2:
(Variant or Key
Block LMK)

This example cancels an existing activity via the command line.

```
Online-AUTH> C pin.mailer <Return>
Enter LMK id [0-1]: 00 <Return>
No activities are authorized for LMK id 00.
Online>
```

Note: This example assumes that the activities in the Authorize Activity command Example 2 (above) are active.

Example 3:
(Variant LMK)

This example cancels an existing activity via the menu.

```
Online-AUTH> C <Return>
Enter LMK id [0-4]: 00 <Return>
Cancel admin:240 (194 mins remaining) ? [y/N] Y <Return>
Cancel export.001.host? [y/N] N <Return>
Cancel generate.000.console:60 (14 mins remaining)?
[y/N] Y <Return>
Cancel pin.mailer? [y/N] N <Return>
The following activities are authorized for LMK id 00:
export.001.host
pin.mailer
Online-AUTH>
```

Note: This example assumes that the activities in the Authorize Activity command Example 3 (above) are active.

Example 4:
(Variant LMK)

This example cancels an existing activity via the command line.

```
Online-AUTH> C gene.000.c admin <Return>
Enter LMK id [0-9]: 00 <Return>
The hollowing activities are authorized for LMK id 00.
export.001.host
pin.mailer
Online-AUTH>
```

Note: This example assumes that the activities in the Authorize Activity command Example 4 (above) are active.

Example 5:
(Variant or Key
Block LMK)

This example cancels an existing activity via the command line.

```
Online-AUTH> C pin.clear <Return>
Enter LMK id [0-9]: 01 <Return>
No activities are authorized for LMK id 01.
Online>
```

Note: This example assumes that the activities in the Authorize Activity command Example 5 (above) are active.

View Authorized Activities (VA)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **VA**

Function: To view all active authorized activities.

Authorization: The HSM does not require any authorization to run this command.

Inputs:

- LMK identifier: 2 numeric digits.

Outputs:

- List of active authorized activities.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.

Example 1: (Multiple authorized activities enabled)

This example applies when multiple authorized activities has been enabled..

```
Online-AUTH> VA <Return>
Enter LMK id: 00 <Return>
The following activities are authorized for LMK id 00:
admin:240 (228 mins remaining)
export.001.host:persistent
generate.000.console:60 (48 mins remaining)

Online-AUTH>
```

Note: This example assumes the activities in the Authorize Activity command Example 4 (above) were authorized 12 minutes ago.

Example 2: (Multiple authorized activities disabled)

This example applies when multiple authorized activities has not been enabled..

```
Online-AUTH> VA <Return>
Enter LMK id [0-9]: 0 <Return>
LMK id 00 is authorized.
Console authorization expires in 716 minute(s).

Online-AUTH>
```

Note: This example assumes that authorized state was enabled 4 minutes ago.

Logging Commands

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

The Error log stores fault information for use by Thales support personnel. The error log is used to log unexpected software errors, hardware failures and alarm events. Whenever an error occurs, that error code is stored, along with the time, date and severity level. Additional errors that have the same error code cause the time and date of that code to be updated. In this way, each error type remains in the log (with the most recent time and date) and is not lost. The severity levels are:

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

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

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

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

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

The payShield 10K provides the following console commands to support storage and retrieval of HSM settings:

Command	**Page**
Display the Error Log (ERRLOG)	**338**
Clear the Error Log (CLEARERR)	**340**
Display the Audit Log (AUDITLOG)	**341**
Clear the Audit Log (CLEARAUDIT)	**343**
Audit Options (AUDITOPTIONS)	**344**

Display the Error Log (ERRLOG)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **ERRLOG**

Function: To display the entries in the error log.

Authorization: The HSM does not require any authorization to run this command.

Inputs: None.

Outputs:

- A listing of the errors in the error log, or text message: "Error log is empty".

Errors: None.

Notes: In software versions up to v2.1, power supply errors are added to the error log only when the HSM is restarted. From v2.2 onwards, power supply errors are logged as soon as they are detected.

Example 1: *In this example, there are no entries in the error log.*

```
Offline> ERRLOG <Return>
Error log is empty
Offline>
```

Example 2: *In this example, the Security setting "Allow Error light to be extinguished when viewing Error Log?" is set to NO.*

```
Offline> ERRLOG <Return>
Error Log (3 entries)
--------------------------
1: May 01 09:35:00  ERROR (1): Invalid queue size (Severity: 2,
Code = 00000001, Sub-code = 00000002)
2: May 01 09:35:02  ERROR (1): Key3 cannot be specified without
key2 (Severity: 0, Code = 00000004, Sub-code = 00000003)
3: May 06 13:55:00  ERROR: [Power Supply:    FAILED (PSU 2
Failed) ] (Severity: 3, Code = 0x00000001, Sub-Code =
0x0000000E)

Please copy this log to a text file and send it
to your regional Thales E-Security Support center.

Offline>
```

Example 3: *In this example, the Security setting "Allow Error light to be extinguished when viewing Error Log?" is set to YES.*

```
Offline> ERRLOG <Return>
Error Log (3 entries)
--------------------------
1: May 01 09:35:00  ERROR (1): Invalid queue size (Severity: 2,
Code = 00000001, Sub-code = 00000002)
2: May 01 09:35:02  ERROR (1): Key3 cannot be specified without
key2 (Severity: 0, Code = 00000004, Sub-code = 00000003)
3: May 06 13:55:00  ERROR: [Power Supply:    FAILED (PSU 2
Failed) ] (Severity: 3, Code = 0x00000001, Sub-Code =
0x0000000E)

Please copy this log to a text file and send it
to your regional Thales E-Security Support center.

Confirm error log has been read and error light should be
extinguished? [Y/N]: Y <Return>

Offline>
```

Example 4: *Entries in the HSM error log have a hash-based integrity check using HMAC. In this example the verification of integrity of the entry failed. A message indicates that an error happened during the verification process and the entry is shown as Unparsed.*

```
Offline> ERRLOG <Return>
Error Log (3 entries)
--------------------------
973: May 31 15:17:35 ERROR: [FAN 1 is now present] (Severity:
3, Code = 0x00000003, Sub-Code = 0x00000018)
Error hmac missmatch - Unable to verify text integrity
 974: UNPARSED [[FAN1 is missing, setting FAN??? speed to 16000
RPM] (Severity: 3, Code = 0x00000003, Sub-Code = 0x00000018]
 975: May 31 17:33:14 ERROR: [FAN 1 is now NOT present]
(Severity: 3, Code = 0x00000003, Sub-Code = 0x00000018)

Please copy this log to a text file and send it
to your regional Thales E-Security Support center.

Confirm error log has been read and error light should be
extinguished? [Y/N]: Y <Return>

Offline>
```

Clear the Error Log (CLEARERR)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☒</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **CLEARERR**

Function: To clear the entries in the error log.

Authorization: The HSM must be in the secure state to run this command.

Inputs: None.

Outputs:

- A confirmation message.

Errors: None.

Example:

```
Secure> CLEARERR <Return>
Error log Cleared
Secure>
```

Display the Audit Log (AUDITLOG)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **AUDITLOG**

Function: To display the entries in the audit log.

Authorization: The HSM does not require any authorization to run this command.

Inputs: None.

Outputs:

- A listing of the entries in the audit log.
  - For authorizations, the period of authorization of Console commands will be indicated by attaching text of the form ":123" (representing 123 minutes) to the identity of the authorized activity.
- The following text messages can be output:
  - Audit Log (in entries)
  - Continue displaying audit log entries? Yes/No/Continuous

Notes:

- Certain items are always recorded in the Audit Log, irrespective of the selections made using AUDITOPTIONS.
  These are:
  - Serial numbers of smartcards used to authenticate users at the HSM or to payShield Manager.
  - Authorization of activities
  - Cancellation of authorization.
  - Key and component entry at the Console or payShield Manager.

  When key and component entry are forcibly logged in this way, the log entry indicates successful completion of the action.
  The user can, as in earlier versions of software, use AUDITOPTIONS to specify that the key and component entry commands are logged: this will normally result in 2 entries in the audit log – one resulting from the AUDITOPTIONS setting indicating that the command was initiated, and the forcible logging indicating the successful completion of the command. If the command does not complete successfully (e.g. because it was cancelled by the user) then there will be no forcible logging, but the entry indicating the command was initiated will still be there if the command was specified in AUDITOPTIONS.
- The Audit Log is now displayed with the most recent entries shown first: up to software version 2.1 the Audit Log was displayed with oldest entries first. This change has been made because, with a maximum length of 50,000 records, it can take a long time to display the complete Audit Log because of the speed limitations of serial connections.

Errors: None.

Example 1:

```
Offline> AUDITLOG <Return>
Audit log is empty
Offline>
```

Example 2:

```
Offline> AUDITLOG <Return>
Audit Log (10 entries)
Counter   Time      Date         Command/Event
---------------------------------------------------------
-----
0000000268  13:55:00  02/Jul/2013  Diagnostic self test
failure: Power
0000000267  16:45:07  01/Jul/2013  Authorized activity
admin..host was cancelled for LMK id 0
0000000266  16:45:05  01/Jul/2013  Authorized activity
admin..console:123 was cancelled
0000000265  15:54:02  01/Jul/2013  Key I/O command BK
executed
0000000264  15:35:55  01/Jul/2013  Activity
component..console:123 was authorized for LMK id 0
0000000263  15:08:48  01/Jul/2013  Smartcard activated:
20025151
0000000262  15:08:48  01/Jul/2013  Smartcard activated:
20025132
0000000261  10:42:32  01/Jul/2013  Host command CA,
response 00
0000000260  10:36:03  01/Jul/2013  Host command CA,
response 69
0000000259  10:34:57  01/Jul/2013  System restarted
0000000258  10:32:48  01/Jul/2013  Keylock turned to
Online
0000000257  10:32:21  01/Jul/2013  Console command CH
0000000256  09:01:56  01/Jul/2013  Diagnostic self tests
passed.

Offline>
```

After 20 entries are displayed continuously, the following text is displayed:

```
Continue displaying audit log entries? [Y/N/C]:
```

Clear the Audit Log (CLEARAUDIT)

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

Command: **CLEARAUDIT**

Function: To clear the entries in the audit log.

Authorization: The HSM must be in the secure state to run this command. Additionally, the HSM must be either in the Authorized State, or the activity **audit.console** must be authorized, using the Authorizing Officer cards of the Management LMK.

Inputs: None.

Outputs:

- One of the following text messages:
  - Audit Log Cleared
  - Audit Log is empty

Errors:

- Command only allowed from Secure-Authorized - the HSM is not in Secure State, or the HSM is not authorized to perform this operation, or both.

Example 1:

```
Secure-AUTH> CLEARAUDIT <Return>
Warning! The HSM's audit log contains entries that have
not yet been printed.
Please confirm that you wish to delete the entire audit
log. [Y/N]: Y <Return>
Audit Log Cleared

Secure-AUTH>
```

Audit Options (AUDITOPTIONS)

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

Command: **AUDITOPTIONS**

Function: To configure the HSM's auditing functionality.
The HSM can be configured to monitor and record the following events:

- Execution of individual host command
- Execution of individual console command
- User interactions, including:
  - System restart (e.g. power cycle)
  - State transitions (i.e. Offline, Online, Secure)
  - LMK installation / erasure
  - Authorization activation/cancelling
- The running and result of automatic self tests.
- Error responses to Host commands
- Host connection failures resulting from deployment of Access Control Lists.

Authorization: The HSM must be in the secure state to use this command to change the items to be audited. Additionally, the HSM must be either in the Authorized State, or the activity **audit.console** must be authorized, using the Authorizing Officer cards of the Management LMK.
The current list of items being audited can be viewed in online state.

Inputs:

- Changes to configuration:
  - Audited console commands:
    - o +CXX to enable auditing of console command XX
    - o –CXX to disable auditing of console command XX

    The "?" character can be used as a wildcard when specifying the commands.
  - Audited host commands
    - o +HXX to enable auditing of host command XX
    - o –HXX to disable auditing of host command XX

    The "?" character can be used as a wildcard when specifying the commands.
  - Audit Error responses to Host Commands (Y/N)
  - Audit user actions (Y/N)
  - Audit counter value
  - Audit Utilization Data Resets (Y/N)
  - Audit Automatic Self testing (Y/N)
  - Audit ACL connection failures (Y/N)

Outputs:

- Current & new configuration details:
  - List of audited console commands
  - List of audited host commands
  - List of user actions
  - Results of automatic self tests
  - Audit counter value

Notes:

- Certain items are always recorded in the Audit Log, irrespective of the selections made using AUDITOPTIONS.
  These are:

  - Serial numbers of smartcards used to authenticate users at the HSM or to payShield Manager.
  - Authorization of activities
  - Cancellation of authorization.
  - Key and component entry at the Console or payShield Manager. This relates to the following Console commands (or HSM equivalents):

BK	Form a Key from Components
CV	Generate a Card Verification Value
D	Form a ZMK from Encrypted Components
DE	Form a ZMK from Clear Components
FK	Form Key from Components
IK	Import a Key
IV	Import a CVK or PVK
LK	Load LMK
LO	Move Old LMKs into Key Change Storage
PV	Generate a Visa PIN Verification Value

When key and component entry are forcibly logged in this way, the log entry indicates successful completion of the action.

The user can, as in earlier versions of software, use AUDITOPTIONS to specify that the key and component entry commands are logged: this will normally result in 2 entries in the audit log – one resulting from the AUDITOPTIONS setting indicating that the command was initiated, and the forcible logging indicating the successful completion of the command. If the command does not complete successfully (e.g. because it was cancelled by the user) then there will be no forcible logging, but the entry indicating the command was initiated will still be there if the command was specified in AUDITOPTIONS.

- **Audit Error Responses to Host Commands**: this setting allows any relevant error responses to Host commands to be logged. In this context, "relevant" means error responses which may indicate situations that require investigation by the payShield 10K Administrators or Security Officers. The use of this setting will therefore not log non-00 error responses which are purely for information or which indicate "business as usual" (e.g. a customer entering an incorrect PIN at a terminal).

- Auditing items (such as heavily used Host commands) which result in a high rate of update to the Audit Log will impact negatively on performance of the HSM.

- After completing the AUDITOPTIONS command, a reboot of the HSM may be required in order to activate the new settings.

Errors:

- Command only allowed from Offline-Authorized - the HSM is not in Offline (or Secure) State, or the HSM is not authorized to perform this operation, or both.
- Invalid Entry - the value entered is invalid.
- Card not formatted to save/retrieve HSM settings - Attempt with another card? [Y/N]

Example:

```
Secure-AUTH>auditoptions

Audit User Actions: YES
Audit Error Responses to Host Commands: YES
Audit utilization data resets: NO
Audit diagnostic self tests: NO
Audit ACL connection failures: NO
Audit Counter Value:
0000000223
List of Audited Console Commands:
List of Audited Host Commands:

Audit User Actions? [Y/N]: y

Audit Error Responses to Host Commands? [Y/N]: n

Audit Utilization Data Resets? [Y/N]: y

Audit Automatic Self Testing? [Y/N]: y

Audit ACL connection failures? [Y/N]: y

Current Audit Counter value is: 0000000223
Enter new value (decimal digits only) or <Return> for no
change:

Modify Audited Command List? [Y/N]: y
Enter command code (e.g. +CDE) or Q to Quit: +CDE
Enter command code (e.g. +CDE) or Q to Quit:
Enter command code (e.g. +CDE) or Q to Quit: q

Audit User Actions: YES
Audit Error Responses to Host Commands: NO
Audit utilization data resets: YES
Audit diagnostic self tests: YES
Audit ACL connection failures: YES
Audit Counter Value:
0000000223
List of Audited Console Commands:
List of Audited Host Commands:

Save Audit Settings to Smartcard? [Y/N]: n


Secure-AUTH>
```

Time and Date Commands

The SETTIME command is used to set the system time and date used by the payShield 10K for the audit log entries. The user should use this command to adjust the time for the local timezone. The time and date can be queried using the GETTIME command.

The payShield 10K provides the following console commands to support storage and retrieval of HSM settings:

Command	Page
Set the Time (SETTIME)	**348**
Query the Time and Date (GETTIME)	**349**
Set Time for Automatic Self-Tests (ST)	**350**

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Required** Activity: **admin.console**		

Command: **Set the Time (SETTIME)**

Function: To set the system time and date used by the HSM.

Authorization: The HSM must be in the secure state to run this command. Additionally, the HSM must be either in the Authorized State, or the activity **admin.console** must be authorized, using the Authorizing Officer cards of the Management LMK.

Inputs:

- The time in hours and minutes.
- The date in year, month and day.

Outputs:

- Text messages, as in the example below.

Errors:

- Command only allowed from Secure-Authorized - the HSM is not in Secure State, or the HSM is not authorized to perform this operation, or both.
- Response invalid. Re-enter - an invalid value has been entered.

Example:

```
Secure-AUTH> SETTIME <Return>
Enter hours [HH](24 hour format): 10 <Return>
Enter minutes [MM]: 08 <Return>
Enter year [YYYY] (2009 or above): 2014 <Return>
Enter month [MM]: 02 <Return>
Enter day [DD]: 12 <Return>
The system time has been modified.
Secure-AUTH>
```

⚠ Setting the date or time back may prevent the payShield Manager from allowing a user to login. Care must be taken when changing the date back such that it is not earlier than the creation date/time of any of the smartcards that will be used to access the HSM.

Query the Time and Date (GETTIME)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **GETTIME**

Function: To query the system time and date.

Authorization: The HSM does not require any authorization to run this command.

Inputs: None.

Outputs:

- The year, month and date.
- The time in hours, minutes and seconds.

Errors: None.

Example:

```
Online> GETTIME <Return>
System date and time: Feb 12 10:08:19 2014
Online>
```

Set Time for Automatic Self-Tests (ST)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☑</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **ST**

Function: Reports the time of day when the daily automatic self-tests required for PCI HSM compliance will be run, and allows this time to be changed.

Authorization: The HSM does not require any authorization to run this command.

Inputs: Time of day.

Outputs: None

Errors: None.

Notes:

- The default time for running the diagnostics is 0900.

Example:

```
Secure> ST <Return>

Self test run time is 09:00.

Change? [Y/N]: y <Return>

Enter hour [HH] (24 hour format): 13 <Return>
Enter minute [MM]: 55 <Return>

Self test run time changed to 13:55.

Secure>
```

Settings, Storage and Retrieval Commands

Commands are provided to save the payShield 10K's Alarm, Host and Security settings to a smartcard and to restore the settings to the HSM. Besides the dedicated command to Save HSM Settings to Smartcard, the following individual configuration commands have the option to save settings to smartcard:

- CL (Configure Alarms) to save the Alarm configuration.
- CH (Configure Host Port) to save the Host port configuration.
- CS (Configure Security) to save the Security configuration.
- AUDITOPTIONS (Audit Options) to save the Audit configuration.

The payShield 10K provides the following console commands to support storage and retrieval of HSM settings:

Command	Page
Save HSM Settings to a Smartcard (SS)	**352**
Retrieve HSM Settings from a Smartcard (RS)	**353**

Save HSM Settings to a Smartcard (SS)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
	Authorization: **Required** Activity: **admin.console**	

Command: **SS**

Function: To save the Alarm, Host Port, Security, Audit, Command, and PIN Block settings to a smartcard (RACCs are supported).

Authorization: The HSM must be in the secure state to run this command. Additionally, the HSM must be either in the Authorized State, or the activity **admin.console** must be authorized, using the Authorizing Officer cards of the Management LMK.

Outputs:

- Confirmation messages that Alarm, Host, Security, Audit, Command, and PIN Block settings are saved.

Errors:

- Card not formatted to save/retrieve HSM settings.
  Attempt with another card? [Y/N] - card is not formatted for storing HSM settings.
- Card not formatted. Attempt with another card? [Y/N] - card is not formatted.
- Command only allowed from Secure-Authorized - the HSM is not in Secure State, or the HSM is not authorized to perform this operation, or both.

Example:

```
Secure-AUTH> SS <Return>
Insert card and press ENTER: <Return>
ALARM settings saved to the smartcard.
HOST settings saved to the smartcard.
SECURITY settings saved to the smartcard.
AUDIT settings saved to the smartcard.
COMMAND settings saved to the smart card.
PIN BLOCK settings saved to the smart card.
Secure-AUTH>
```

Retrieve HSM Settings from a Smartcard (RS)

Variant ☑		Key Block ☑
Online ☒	Offline ☒	Secure ☑
	Authorization: **Required** Activity: **admin.console**	

Command: **RS**

Function: To read the Alarm, Host Port, Security, Audit, Command, and PIN Block settings from a smartcard. The user is then prompted to use these to overwrite the existing HSM settings. If the settings on the smartcard were saved using a configuration command (CL, CH, CS and AUDITOPTIONS), then only those settings are overwritten.

Authorization: The HSM must be in the secure state to run this command. Additionally, the HSM must be either in the Authorized State, or the activity **admin.console** must be authorized, using the Authorizing Officer cards of the Management LMK.

Inputs:

- Whether to overwrite each of the groups of saved settings.

Outputs:

- The Alarm, Host, Security, Audit, Command, and PIN Block settings stored on the smartcard are listed.

Errors:

- Card not formatted to save/retrieve HSM settings. Attempt with another card? [Y/N] - card is not formatted for storing HSM settings.
- Card not formatted. Attempt with another card? [Y/N] - card is not formatted.
- Command only allowed from Secure-Authorized - the HSM is not in Secure State, or the HSM is not authorized to perform this operation, or both.

Example:

```
Secure-AUTH> RS <Return>
Insert card and press ENTER: <Return>
Temperature Alarm: ON
Motion Alarm: HIGH
Self Test Run Time: 09:00
Overwrite alarm settings with the settings above? [Y/N]: Y
<Return>
ALARM settings retrieved from smartcard

Message header length: 4
Protocol: ETHERNET
Character format: ASCII
UDP active: YES
TCP active: YES
TLS active: YES
Number of TCP connections: 1
Well-Known-Port: 1500
Well-Known-TLS-Port: 2500
Number of host interfaces: 1

Overwrite host settings with the settings above? [Y/N]: n
<Return>

PIN length: 04
Old encrypted PIN length: 05
Echo: OFF
Atalla ZMK variant support: OFF
Transaction key support: AUSTRALIAN
User storage key length: SINGLE
Select clear PINs: NO
Enable ZMK translate command: NO
Enable X9.17 for import: YES
Enable X9.17 for export: YES
Solicitation batch size: 1024
Single-DES: ENABLED
Prevent single-DES keys from masquerading as double or triple-
length keys: NO
ZMK length: DOUBLE
Decimalization tables: PLAINTEXT
Decimalization table checks enabled: YES
PIN encryption algorithm: A
Authorized state required when importing DES key under RSA key:
YES
Minimum HMAC length in bytes: 10
Enable PKCS#11 import and export for HMAC keys: NO
Enable ANSI X9.17 import and export for HMAC keys: NO
Enable ZEK/TEK encryption of ASCII data or Binary data or None:
BINARY
Restrict key check values to 6 hex chars : YES
Enable multiple authorized activities: YES
Enable variable length PIN offset: NO
Enable weak PIN checking: NO
Enable PIN block format 34 as output format for PIN
translations to ZPK: NO
Enable PIN block account number translations: NO
Default LMK identifier: 00
Management LMK identifier: 00
Use HSM clock for date/time validation: YES
Additional padding to disguise key length: NO
Key export and import in trusted format only: NO
```

```
Protect MULTOS cipher data checksums: YES
Enforce Atalla variant match to Thales key type: NO
Card/password authorization: C
Enable use of Tokens in PIN Translation: NO
Enable use of Tokens in PIN Verification: NO
Restrict PIN block usage for PCI Compliance: NO
Enforce key type separation for PCI Compliance: NO
Enforce Authorization Time Limit: YES
Overwrite security settings with the settings above? [Y/N]: Y
<Return>
SECURITY settings retrieved from smartcard.

User Action: ENABLED
Audit Counter: 00000183
24 Audited Mgmt commands
0 Audited Host commands
Audit Host Errors: DISABLED
0 Audited Console commands
Overwrite auditlog settings with the settings above? [Y/N]: n
<Return>

0 Blocked Host commands
0 Blocked Console commands
Overwrite command settings with the settings above? [Y/N]: n
<Return>

Pin Block Format 01: ENABLED
Pin Block Format 02: ENABLED
Pin Block Format 03: ENABLED
Pin Block Format 04: ENABLED
Pin Block Format 05: ENABLED
Pin Block Format 34: ENABLED
Pin Block Format 35: ENABLED
Pin Block Format 41: ENABLED
Pin Block Format 42: ENABLED
Pin Block Format 46: ENABLED
Pin Block Format 47: ENABLED
Pin Block Format 48: ENABLED
Overwrite pin block settings with the settings above? [Y/N]: n
<Return>

Secure-AUTH>
```

Key Management Commands

The payShield 10K provides the following host commands to support generic key management operations:

Command	Page
Generate Key Component (GC)	**357**
Generate Key and Write Components to Smartcard (GS)	**360**
Encrypt Clear Component (EC)	**364**
Form Key from Components (FK)	**367**
Generate Key (KG)	**374**
Import Key (IK)	**378**
Export Key (KE)	**382**
Generate a Check Value (CK)	**386**
Set KMC Sequence Number (A6)	**388**

Generate Key Component (GC)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Required** Activity: **<u>component.{*key*}.console</u>**		

Command: **GC**

Function: To generate a key component and display it in plain and encrypted forms.

	Variant LMK	Key Block LMK
Authorization:	The HSM must be in the Authorized State, or the activity **component.{*key*}.console** must be authorized, where 'key' is the key type code of the key component being generated.	The HSM must be in the Authorized State, or the activity **component.{*key*}.console** must be authorized, where 'key' is the key usage code of the key component being generated.
Inputs:	• LMK Identifier: 00-99. • Key Length: 1 (single), 2 (double), 3 (triple). • Key Type: See the Key Type Table in the *Host Programmer's Manual*. • Key Scheme:	• LMK Identifier: 00-99. • Key Algorithm (if AES LMK): 3DES or AES • Key Length: Single/Double/Triple length DES key or (if AES LMK) 128/192/256-bit AES key. • Key Scheme: • Key Usage: See the Key Usage Table in the *Host Programmer's Manual*. • Mode of Use: See the Mode of Use Table in the *Host Programmer's Manual*. • Component Number: 1-9. • Exportability: See the Exportability Table in the *Host Programmer's Manual*. • Optional Block data.
Outputs:	• Clear text key component. • Key component encrypted under an appropriate variant of the selected LMK. • Component check value.	• Clear text key component. • Key Block containing the component encrypted under the selected LMK. • Component check value.

Notes:

- When generating key components encrypted by a Key Block LMK, the "Component Number" field stored within the component's key block header can be used to help identify individual components. Note, however, that this field is not examined or used by the HSM's FK command when forming a key from these components.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Invalid key type; re-enter - the key type is invalid. See the Key Type Table the *Host Programmer's Manual*.
- Invalid key scheme for key length - the Key Scheme is inappropriate for Key length.
- Invalid key scheme - an invalid key scheme is entered.
- Internal failure 12: function aborted - the contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.
- Various key block field errors – the value entered is invalid, or incompatible with previously entered values.

Example 1:
(Variant LMK)

This example generates a double length DES key component in plaintext & encrypted form.

```
Online-AUTH> GC <Return>
Enter LMK id: 00 <Return>
Enter key length [1,2,3]: 2 <Return>
Enter key type: 001 <Return>
Enter key scheme: U <Return>

Clear Component: XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX
Encrypted Component: UYYYY YYYY YYYY YYYY YYYY YYYY
YYYY YYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 2:
(3DES Key Block LMK)

This example generates a double length DES key component in plaintext & encrypted form.

```
Online-AUTH> GC <Return>
Enter LMK id: 01 <Return>
Enter key length [1,2,3]: 2 <Return>
Enter key scheme: S <Return>
Enter key usage: P0 <Return>
Enter mode of use: N <Return>
Enter component number [1-9]: 2 <Return>
Enter exportability: E <Return>
Enter optional blocks? [Y/N]: N <Return>

Clear component: XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX
Encrypted component: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 3:
(AES Key Block LMK)

This example generates a double length DES key component in plaintext & encrypted form.

```
Online-AUTH> GC <Return>
Enter LMK id: 02 <Return>
Enter algorithm [3DES/AES]: 3 <Return>
Enter key length [1,2,3]: 2 <Return>
Enter key scheme: S <Return>
Enter key usage: P0 <Return>
Enter mode of use: N <Return>
Enter component number [1-9]: 2 <Return>
Enter exportability: E <Return>
Enter optional blocks? [Y/N]: N <Return>

Clear component: XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX
Encrypted component: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 4:
(AES Key Block
LMK)

This example generates a 128-bit AES key component in plaintext & encrypted form.

```
Online-AUTH> GC <Return>
Enter LMK id: 02 <Return>
Enter algorithm [3DES/AES]: A <Return>
Enter key length [128,192,256]: 128 <Return>
Enter key scheme: S <Return>
Enter key usage: K0 <Return>
Enter mode of use: N <Return>
Enter component number [1-9]: 2 <Return>
Enter exportability: E <Return>
Enter optional blocks? [Y/N]: N <Return>

Clear component: XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX
Encrypted component: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Generate Key and Write Components to Smartcard (GS)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
Authorization: **Required** Activity: **component.{*key*}.console**		

Command:	**GS**	
Function:	Generates a key in 2 to 3 component and write the components to smartcards.	
	Variant LMK	Key Block LMK
Authorization:	The HSM must be in the Authorized State, or the activity **component.{*key*}.console** must be authorized, where 'key' is the key type code of the key being generated.	The HSM must be in the Authorized State, or the activity **component.{*key*}.console** must be authorized, where 'key' is the key usage code of the key being generated.
Inputs:	• LMK Identifier: 00-99. • Key Length: 1 (single), 2 (double), 3 (triple). • Key Type: See the Key Type Table in the *Host Programmer's Manual*. • Key Scheme. • Number of components: 2-3. • Smartcard PINs. PINs must be entered within 60 seconds of being requested.	• LMK Identifier: 00-99. • Key Algorithm (if AES LMK): 3DES or AES • Key Length: Single/Double/Triple length DES key or (if AES LMK) 128/192/256-bit AES key. • Key Scheme. • Number of components: 2-3. • Key Usage: See the Key Usage Table in the *Host Programmer's Manual*. • Mode of Use: See the Mode of Use Table in the *Host Programmer's Manual*. • Key Version Number: 00-99. • Exportability: See the Exportability Table in the *Host Programmer's Manual*. • Optional Block data. • Smartcard PINs. PINs must be entered within 60 seconds of being requested.
Outputs:	• Key encrypted under an appropriate variant of the selected LMK. • Key check value.	• Key Block containing the key encrypted under the selected LMK. • Key check value.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Invalid PIN; re-enter - a PIN of less than 4 or greater than 8 is entered.
- Smartcard error; command/return: 0003 - invalid PIN is entered.
- Warning - card not blank. Proceed? [Y/N] - the smartcard entered is not blank.
- Overwrite key component? [Y/N] - the smartcard already contains a key component. It can be overwritten if desired.
- Device write failed - the component could not be verified.
- Invalid key scheme for key length - the Key scheme is inappropriate for Key length.
- Invalid key type; re-enter - the key type is invalid. See the Key Type Table in the *Host Programmer's Manual*.

- Invalid key scheme - an invalid key scheme is entered.
- Invalid entry - an invalid number of components has been entered.
- Not an LMK card - card is not formatted for LMK or key storage.
- Card not formatted - card is not formatted.
- Command only allowed from Authorized - the HSM is not authorized to perform this operation.
- Internal failure 12: function aborted - the contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.
- Various key block field errors – the value entered is invalid, or incompatible with previously entered values.

Example 1:
(Variant LMK)

This example writes two double length DES key components to two smartcards, and encrypts the formed key.

```
Online-AUTH> GS <Return>
Enter LMK id: 00 <Return>
Enter key length [1,2,3]: 1 <Return>
Enter key type: 001 <Return>
Enter key scheme: 0 <Return>
Enter number of components [2-3]: 2 <Return>
Insert card 1 and enter PIN: ******** <Return>
Make additional copies? [Y/N]: N <Return>
Insert card 2 and enter PIN: ******** <Return>
Make additional copies? [Y/N]: N <Return>
Encrypted key: YYYY YYYY YYYY YYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 2:
(3DES Key Block
LMK)

This example generates and writes two double length 3DES key components to two smartcards, and encrypts the formed key.

```
Online-AUTH> GS <Return>
Enter LMK id: 01 <Return>
Enter key length [1,2,3]: 2 <Return>
Enter key scheme: S <Return>
Enter number of components [2-3]: 2 <Return>
Enter key usage: P0 <Return>
Enter mode of use: N <Return>
Enter key version number: 00 <Return>
Enter exportability: E <Return>
Enter optional blocks? [Y/N]: Y <Return>
Enter optional block identifier: 00 <Return>
Enter optional block data: L <Return>
Enter more optional blocks? [Y/N]: N <Return>
Insert card 1 and enter PIN: ******** <Return>
Make additional copies? [Y/N]: N <Return>
Insert card 2 and enter PIN: ******** <Return>
Make additional copies? [Y/N]: N <Return>
Encrypted key: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 3:
(AES Key Block
LMK)

This example generates and writes two double length 3DES key components to two smartcards, and encrypts the formed key.

```
Online-AUTH> GS <Return>
Enter LMK id: 02 <Return>
Enter algorithm [3DES/AES]: 3 <Return>
Enter key length [1,2,3]: 2 <Return>
Enter key scheme: S <Return>
Enter number of components [2-3]: 2 <Return>
Enter key usage: P0 <Return>
Enter mode of use: N <Return>
Enter key version number: 00 <Return>
Enter exportability: E <Return>
Enter optional blocks? [Y/N]: Y <Return>
Enter optional block identifier: 00 <Return>
Enter optional block data: L <Return>
Enter more optional blocks? [Y/N]: N <Return>
Insert card 1 and enter PIN: ******** <Return>
Make additional copies? [Y/N]: N <Return>
Insert card 2 and enter PIN: ******** <Return>
Make additional copies? [Y/N]: N <Return>
Encrypted key: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 4:
(AES Key Block
LMK)

This example generates and writes two128-bit AES key components to two smartcards, and encrypts the formed key.

```
Online-AUTH> GS <Return>
Enter LMK id: 02 <Return>
Enter algorithm [3DES/AES]: A <Return>
Enter key length [128,192,256]: 128 <Return>
Enter key scheme: S <Return>
Enter number of components [2-3]: 2 <Return>
Enter key usage: P0 <Return>
Enter mode of use: N <Return>
Enter key version number: 00 <Return>
Enter exportability: E <Return>
Enter optional blocks? [Y/N]: Y <Return>
Enter optional block identifier: 00 <Return>
Enter optional block data: L <Return>
Enter more optional blocks? [Y/N]: N <Return>
Insert card 1 and enter PIN: ******** <Return>
Make additional copies? [Y/N]: N <Return>
Insert card 2 and enter PIN: ******** <Return>
Make additional copies? [Y/N]: N <Return>
Encrypted key: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Encrypt Clear Component (EC)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Required** Activity: **component.*{key}*.console**		

Command:	**EC**	
Function:	To encrypt a clear text component and display the result at the console. If the component does not have odd parity, odd parity will be forced before encryption by the selected LMK.	
	Variant LMK	Key Block LMK
Authorization:	The HSM must be in the Authorized State, or the activity **component.*{key}*.console** must be authorized, where 'key' is the key type code of the component being encrypted.	The HSM must be in the Authorized State, or the activity **component.*{key}*.console** must be authorized, where 'key' is the key usage code of the component being encrypted.
Inputs:	• LMK Identifier: 00-99. • Key Type: See the Key Type Table in the *Host Programmer's Manual*. • Key Scheme. • Clear Component: 16/32/48 hex digits.	• LMK Identifier: 00-99. • Component Algorithm (if AES LMK): 3DES or AES • Component Length: Single/Double/Triple length DES key or (if AES LMK) 128/192/256-bit AES key. • Key Scheme. • Key Usage: See the Key Usage Table in the *Host Programmer's Manual*. • Mode of Use: See the Mode of Use Table in the *Host Programmer's Manual*. • Component Number: 1-9. • Exportability: See the Exportability Table in the *Host Programmer's Manual*. • Optional Block data. • Clear Component: 16/32/48 hex digits.
Outputs:	• Component encrypted under an appropriate variant of the selected LMK. • Component check value.	• Key Block containing the component encrypted under the selected LMK. • Component check value.
Errors:	• Invalid LMK identifier - no LMK loaded or entered identifier out of range. • Data invalid; please re-enter - the input data does not contain 16 or 32 or 48 hexadecimal characters. Re-enter the correct number of hexadecimal characters. • Invalid key type; re-enter - the key type is invalid. See the Key Type Table in the *Host Programmer's Manual*. • Invalid key scheme - an invalid key scheme is entered. • Command only allowed from Authorized - the HSM is not authorized to perform this operation. • Internal failure 12: function aborted - the contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.	

- Various key block field errors – the value entered is invalid, or incompatible with previously entered values.

Example 1:
(Variant LMK)

This example encrypts a plaintext double length DES key component.

```
Online-AUTH> EC <Return>
Enter LMK id: 00 <Return>
Enter key type: 001 <Return>
Enter key Scheme: U <Return>
Enter component: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Encrypted component: U YYYY YYYY YYYY YYYY YYYY YYYY
YYYY YYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 2:
(3DES Key Block LMK)

This example encrypts a plaintext double length DES key component.

```
Online-AUTH> EC <Return>
Enter LMK id: 01 <Return>
Enter component length [1,2,3]: 2 <Return>
Enter key scheme: S <Return>
Enter key usage: P0 <Return>
Enter mode of use: N <Return>
Enter component number [1-9]: 2 <Return>
Enter exportability: E <Return>
Enter optional blocks? [Y/N]: Y <Return>
Enter optional block identifier: 00 <Return>
Enter optional block data: L <Return>
Enter more optional blocks? [Y/N]: N <Return>
Enter component: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Encrypted component: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 3:
(AES Key Block LMK)

This example encrypts a plaintext double length DES key component.

```
Online-AUTH> EC <Return>
Enter LMK id: 02 <Return>
Enter algorithm [3DES/AES]: 3 <Return>
Enter component length [1,2,3]: 2 <Return>
Enter key scheme: S <Return>
Enter key usage: D0 <Return>
Enter mode of use: N <Return>
Enter component number [1-9]: 2 <Return>
Enter exportability: E <Return>
Enter optional blocks? [Y/N]: Y <Return>
Enter optional block identifier: 00 <Return>
Enter optional block data: L <Return>
Enter more optional blocks? [Y/N]: N <Return>
Enter component: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Encrypted component: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 4:
(AES Key Block
LMK)

This example encrypts a plaintext 128-bit AES key component.

```
Online-AUTH> EC <Return>
Enter LMK id: 02 <Return>
Enter algorithm [3DES/AES]: A <Return>
Enter component length [128,192,256]: 128 <Return>
Enter key scheme: S <Return>
Enter key usage: K0 <Return>
Enter mode of use: N <Return>
Enter component number [1-9]: 2 <Return>
Enter exportability: E <Return>
Enter optional blocks? [Y/N]: Y <Return>
Enter optional block identifier: 00 <Return>
Enter optional block data: L <Return>
Enter more optional blocks? [Y/N]: N <Return>
Enter component: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Encrypted component: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Form Key from Components (FK)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Required** Activity: **component.{*key*}.console**		

Command: **FK**

Function: To build a key from components. If clear components are used, they will not be checked for parity, but odd parity will be forced on the final key before encryption under the selected LMK.

	Variant LMK	Key Block LMK
Authorization:	The HSM must be in the Authorized State, or the activity **component.{*key*}.console** must be authorized, where 'key' is the key type code of the key being formed.	The HSM must be in the Authorized State, or the activity **component.{*key*}.console** must be authorized, where 'key' is the key usage code of the key being formed.
Inputs:	• LMK Identifier: 00-99. • Key Length: 1 (single), 2 (double), 3 (triple). • Key Type: See the Key Type Table in the *Host Programmer's Manual*. • Key Scheme. Must be U, T, or None/Z. • Component Type: X (xor), H (half), E (encrypted), S (smartcard), T (third). • Number of Components: 1-9 if the security setting "AU Components" has been set to "NO", otherwise 2-9. • Clear Components: 16/32/48 hex digits.	• LMK Identifier: 00-99. • Key Algorithm (if AES LMK): 3DES or AES • Key Length: Single/Double/Triple length DES key or (if AES LMK) 128/192/256-bit AES key. • Key Scheme. • Component Type (for AES keys): X (xor), E (encrypted), S (smartcard), • Component Type (for DES keys): X (xor), E (encrypted), S (smartcard), H (half), T (third). • Number of Components: 1-9 if the security setting "Enforce Multiple Key Components" has been set to "NO", otherwise 2-9. • Key Usage: See the Key Usage Table the *Host Programmer's Manual*. • Mode of Use: See the Mode of Use Table in the *Host Programmer's Manual*. • Key Version Number: 00-99. • Exportability: See the Exportability Table in the *Host Programmer's Manual*. • Optional Block data. • Clear Components: 16/32/48 hex digits.
Outputs:	• Key encrypted under an appropriate variant of the selected LMK. • Key Check Value.	• Key Block containing the component encrypted under the selected LMK. • Key Check Value.

Notes:

- PINs must be entered within 60 seconds of being requested.
- When using key components encrypted by a Key Block LMK, the FK command ignores the "Component Number" field stored within each component key block.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.

- Incompatible header values - the field values are incompatible between components.
- Incompatible key status optional blocks - there is a mismatch between the values contained in one or more key status optional blocks.
- Command only allowed from Authorized - the HSM is not authorized to perform this operation.
- Invalid key scheme - an invalid key scheme is entered.
- Invalid key type; re-enter - the key type is invalid. See the Key Type Table in the *Host Programmer's Manual*.
- Key all zero - the key is invalid.
- Invalid entry - an invalid number of components has been entered.
- Data invalid; please re-enter - the amount of input data is incorrect. Re-enter the correct number of hexadecimal characters.
- Invalid PIN; re-enter - a PIN of less than 4 or greater than 8 is entered.
- Smartcard error; command/return: 0003 - invalid PIN is entered.
- No component card - no key component on the provided smartcard.
- Not a LMK card - card is not formatted for LMK or key storage.
- Card not formatted - card is not formatted.
- Internal failure 12: function aborted - the contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.
- Various key block field errors – the value entered is invalid, or incompatible with previously entered values.

Notes:

- Component type H is not permitted for Triple – DES keys.
- Use of this command will always create an entry in the Audit Log.

Example 1:
(Variant LMK)

This example forms a key from plaintext component.

```
Online-AUTH> FK <Return>
Enter LMK id: 00 <Return>
Enter key length[1,2,3]: 2 <Return>
Enter key type: 002 <Return>
Enter key scheme: U <Return>
Component type [X,H,E,S,T]: X <Return>
Enter number of components [1-9]: 2 <Return>

Enter component 1: **** **** **** **** **** **** ****
**** <Return>
Component 1 check value: XXXXXX
Continue? [Y/N]: y <Return>

Enter component 2: **** **** **** **** **** **** ****
**** <Return>
Component 2 check value: XXXXXX
Continue? [Y/N]: y <Return>

Encrypted key: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 2:
(Variant LMK)

This example forms a key from components on a smartcard.

```
Online-AUTH> FK <Return>
Enter LMK id: 00 <Return>
Enter key length[1,2,3]: 2 <Return>
Enter key type: 002 <Return>
Enter key scheme: U <Return>
Component type [X,H,E,S,T]: S <Return>
```

```
Enter number of components (1-9): 2 <Return>

Insert card 1 and enter PIN: ******** <Return>
Component 1 check value: XXXXXX
Continue? [Y/N]: y <Return>

Insert card 2 and enter PIN: ******** <Return>
Component 2 check value: XXXXXX
Continue? [Y/N]: y <Return>

Encrypted key: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 3:
(Variant LMK)

This example forms a key from encrypted components.

```
Online-AUTH> FK <Return>
Enter LMK id: 00 <Return>
Enter key length[1,2,3]: 2 <Return>
Enter key type: 002 <Return>
Enter key scheme: U <Return>
Component type [X,H,E,S,T]: E <Return>
Enter number of components (1-9): 2 <Return>

Enter component 1: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX <Return>
Component 1 check value: XXXXXX
Continue? [Y/N]: y <Return>

Enter component 2: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX <Return>
Component 2 check value: XXXXXX
Continue? [Y/N]: y <Return>

Encrypted key: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 4:
(Variant LMK)

The security settings require that multiple components are used to form keys, but the user attempts to form a key from one component.

```
Online-AUTH> FK <Return>
Enter LMK id: 00 <Return>
Enter key length[1,2,3]: 2 <Return>
Enter key type: 002 <Return>
Enter key scheme: U <Return>
Component type [X,H,E,S,T]: E <Return>
Enter number of components (2-9): 1 <Return>

Invalid Entry
Enter number of components (2-9): 2 <Return>

Enter component 1: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX <Return>
Component 1 check value: XXXXXX
Continue? [Y/N]: y <Return>

Enter component 2: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX <Return>
Component 2 check value: XXXXXX
Continue? [Y/N]: y <Return>

Encrypted key: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 5:
(3DES Key Block
LMK)

This example forms a single length DES key from plaintext components.

```
Online-AUTH> FK <Return>
Enter LMK id: 01 <Return>
Enter key length [1,2,3]: 1 <Return>
Enter key scheme: S <Return>
Component type [X,H,E,S,T]: X <Return>
Enter number of components [1-9]: 2 <Return>
Enter key usage: P0 <Return>
Enter mode of use: N <Return>
Enter key version number: 99 <Return>
Enter exportability: E <Return>
Enter optional blocks? [Y/N]: N <Return>

Enter component 1: **** **** **** **** <Return>
Component 1 check value: XXXXXX
Continue? [Y/N]: y <Return>

Enter component 2: **** **** **** **** <Return>
Component 2 check value: XXXXXX
Continue? [Y/N]: y <Return>

Encrypted key: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 6:
(3DES Key Block
LMK)

This example forms a double length 3DES key from components on a smartcard.

```
Online-AUTH> FK <Return>
Enter LMK id: 01 <Return>
Enter Key Length[1,2,3]: 2 <Return>
Enter key scheme: S <Return>
Component type [X,H,E,S,T]: S <Return>
Enter number of components (1-9): 2 <Return>

Insert card 1 and enter PIN: ******** <Return>
Component 1 check value: XXXXXX
Continue? [Y/N]: y <Return>

Insert card 2 and enter PIN: ******** <Return>
Component 2 check value: XXXXXX
Continue? [Y/N]: y <Return>

Encrypted key: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 7:
(AES Key Block
LMK)

This example forms a double length 3DES key from plaintext components.

```
Online-AUTH> FK <Return>
Enter LMK id: 02 <Return>
Enter algorithm [3DES/AES]: 3 <Return>
Enter key length [1,2,3]: 2 <Return>
Enter key scheme: S <Return>
Component type [X,H,E,S,T]: X <Return>
Enter number of components [1-9]: 2 <Return>
Enter key usage: P0 <Return>
Enter mode of use: N <Return>
Enter key version number: 99 <Return>
Enter exportability: E <Return>
Enter optional blocks? [Y/N]: N <Return>

Enter component 1: **** **** **** **** **** **** ****
**** <Return>
Component 1 check value: XXXXXX
Continue? [Y/N]: y <Return>

Enter component 2: **** **** **** **** **** **** ****
**** <Return>
Component 2 check value: XXXXXX
Continue? [Y/N]: y <Return>

Encrypted key: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 8:
(AES Key Block LMK)

This example forms a 128-bit AES key from components on a smartcard.

```
Online-AUTH> FK <Return>
Enter LMK id: 02 <Return>
Enter algorithm [3DES/AES]: A <Return>
Enter key length [128,192,256]: 128 <Return>
Enter key scheme: S <Return>
Component type [X,E,S]: S <Return>
Enter number of components [1-9]: 2 <Return>
Enter key version number: 00 <Return>
Enter optional blocks? [Y/N]: N <Return>

Insert card 1 and enter PIN: ******** <Return>
Component 1 check value: XXXXXX
Continue? [Y/N]: y <Return>

Insert card 2 and enter PIN: ******** <Return>
Component 2 check value: XXXXXX
Continue? [Y/N]: y <Return>

Encrypted key: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 8:
(AES Key Block LMK)

This example forms a 128-bit AES key from encrypted components.

```
Online-AUTH> FK <Return>
Enter LMK id: 02 <Return>
Enter algorithm [3DES/AES]: A <Return>
Enter key length [128,192,256]: 128 <Return>
Enter key scheme: S <Return>
Component type [X,E,S]: E <Return>
Enter number of components [1-9]: 3 <Return>
Enter key version number: 00 <Return>
Enter optional blocks? [Y/N]: Y <Return>
Enter optional block identifier: 03 <Return>
Enter optional block data: 2005:12:21:00 <Return>
Enter more optional blocks? [Y/N]: Y <Return>
Enter optional block identifier: 04 <Return>
Enter optional block data: 2007:12:21:00 <Return>
Enter more optional blocks? [Y/N]: N <Return>

Enter component 1: S XXXXXXXX……XXXXXX <Return>
```

```
Component 1 check value: XXXXXX
Continue? [Y/N]: y <Return>

Enter component 2: S XXXXXXXX……XXXXXX <Return>
Component 2 check value: XXXXXX
Continue? [Y/N]: y <Return>

Enter component 3: S XXXXXXXX……XXXXXX <Return>
Component 3 check value: XXXXXX
Continue? [Y/N]: y <Return>

Encrypted key: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Generate Key (KG)

<table>
<tr><td colspan="2">Variant ☑</td><td>Key Block ☑</td></tr>
<tr><td>Online ☑</td><td>Offline ☑</td><td>Secure ☑</td></tr>
<tr><td>Variant LMK</td><td colspan="2">Authorization: **Determined by KTT(G&E)**
Activity: **generate.{*key*}.console** and **export.{*key*}.console**</td></tr>
<tr><td>Key Block LMK</td><td colspan="2">Authorization: **If export to non-KB.**
Activity: **export.{key}.console**</td></tr>
</table>

Command: **KG**

Function: To generate a random key and return it encrypted under the LMK and optionally under a ZMK (for transmission to another party).

<table>
<tr><th></th><th>Variant LMK</th><th>Key Block LMK</th></tr>
<tr><td>Authorization:</td><td>This command examines the 'Generate' flag of the given key type within the Key Type Table to determine the authorization requirement. If the flag is 'A', the HSM must either be in the Authorized State, or the activity <b>generate.{<i>key</i>}.console</b> must be authorized, where 'key' is the key type code of the key being generated.
If the generated key is required to be exported under the ZMK, this command also examines the 'Export' flag of the given key type within the Key Type Table. If the flag is 'A', the HSM must either be in the Authorized State, or the activity <b>export.{<i>key</i>}.console</b> must be authorized, where 'key' is the key type code of the key being exported.</td><td>The authorization requirement for this command depends solely on the type of export being requested:
<table><tr><th>Exported key scheme</th><th>Authorization</th></tr><tr><td>No export</td><td>None</td></tr><tr><td>'S' (<i>Thales Key Block</i>)</td><td>None</td></tr><tr><td>'R' (<i>TR-31 Key Block</i>)</td><td>None</td></tr><tr><td>'U', 'T' (<i>Variant</i>)</td><td>Required</td></tr><tr><td>'Z', 'X', 'Y' (<i>X9.17</i>)</td><td>Required</td></tr></table>
If authorization is required, the HSM must either be in the Authorized State, or the activity <b>export.{<i>key</i>}.console</b> must be authorized, where 'key' is the key usage code of the key being exported.</td></tr>
<tr><td>Inputs:</td><td>• LMK Identifier: 00-99.
• Key Length: 1 (single), 2 (double), 3 (triple).
• Key Type: See the Key Type Table in the <i>Host Programmer's Manual</i>.
• Key Scheme (LMK).
• Key Scheme (ZMK) (if exporting).
• ZMK (if exporting).
• Key Block values if exporting to TR-31 format</td><td>• LMK Identifier: 00-99.
• Key Algorithm (if AES LMK): 3DES or AES
• Key Length: Single/Double/Triple length DES key or (if AES LMK) 128/192/256-bit AES key.
• Key Scheme (LMK).
• Key Scheme (ZMK) (if exporting).
• ZMK (if exporting).
• Key Usage: See the Key Usage Table in the <i>Host Programmer's Manual</i>.
• Mode of Use: See the Mode of Use Table in the <i>Host Programmer's Manual</i>.
• Key Version Number: 00-99.</td></tr>
</table>

		• Exportability: See the Exportability Table in the *Host Programmer's Manual*. • Optional Block data. • Exportability of exported key (if exporting).
Outputs:	• Key encrypted under an appropriate variant of the selected LMK. • Key/Key Block encrypted under the ZMK (if exporting). • Key Check Value.	• Key Block containing the key encrypted under the selected LMK. • Key/Key Block encrypted under the ZMK (if exporting). • Key Check Value.

Notes:

For legacy reasons, the export of a ZMK, ZEK or DEK from encryption under a key block LMK to encryption under a ZMK (in variant/X9.17 format) will not be permitted. Specifically, such export of keys with key usage = "K0", "52", "D0", "21" or "22" will be prohibited.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Must be in Authorized State or Activity not authorized - the key type provided requires the HSM to be in Authorized State.
- Data invalid; please re-enter - the encrypted ZMK does not contain the correct characters, or the key check value does not contain 6 hexadecimal characters. Re-enter the correct number of hexadecimal characters.
- Key parity error; please re-enter - the ZMK does not have odd parity on each byte. Re-enter the encrypted ZMK and check for typographic errors.
- Invalid key scheme for key length - the Key scheme is inappropriate for Key length.
- Invalid key scheme - the key scheme is invalid.
- Invalid key type; re-enter - the key type is invalid. See the Key Type Table the *Host Programmer's Manual*.
- Internal failure 12: function aborted - the contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.
- Various key block field errors – the value entered is invalid, or incompatible with previously entered values.

Example 1:
(Variant LMK)

This example generates a new double length DES key.

```
Online> KG <Return>
Enter LMK id: 00 <Return>
Enter key length [1,2,3]: 2 <Return>
Enter key type: 002 <Return>
Enter key scheme (LMK): U <Return>
Enter key scheme (ZMK): <Return>
Enter ZMK: <Return>
Key under LMK: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key Check value: ZZZZZZ
Online>
```

Example 2:
(Variant LMK)

This example generates a new double length DES key, and exports it to X9.17 format.

```
Online-AUTH> KG <Return>
Enter LMK id: 00 <Return>
Enter key length [1,2,3]: 2 <Return>
Enter key type: 002 <Return>
Enter key scheme (LMK): U <Return>
Enter key scheme (ZMK): X <Return>
Enter ZMK: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Key under LMK: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key under ZMK: X YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 3:
(Variant LMK)

This example generates a new double length DES key, and exports it to TR-31 format.

```
Online-AUTH> KG <Return>
Enter LMK id: 00 <Return>
Enter key length [1,2,3]: 2 <Return>
Enter key type: 001 <Return>
Enter key scheme (LMK): U <Return>
Enter key scheme (ZMK): R <Return>
Enter ZMK: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Enter key usage: P0 <Return>
Enter mode of use: N <Return>
Enter key version number: 44 <Return>
Enter exportability: N <Return>
Enter optional blocks? [Y/N]: N <Return>
Key under LMK: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key under ZMK: R YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 4:
(3DES Key Block LMK)

This example generates a new double length DES key, and exports it to X9.17 format.

```
Online-AUTH> KG <Return>
Enter LMK id: 01 <Return>
Enter key length [1,2,3]: 2 <Return>
Enter key scheme (LMK): S <Return>
Enter key scheme (ZMK): X <Return>
Enter ZMK: S XXXXXXXX……XXXXXX <Return>
Enter key usage: P0 <Return>
Enter mode of use: N <Return>
Enter key version number: 22 <Return>
Enter exportability: N <Return>
Enter optional blocks? [Y/N]: N <Return>
Key under LMK: S YYYYYYYY……YYYYYY
Key under ZMK: X YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 5:
(3DES Key Block LMK)

This example generates a new double length DES key, and exports it to TR-31 format.

```
Online> KG <Return>
Enter LMK id: 01 <Return>
Enter key length [1,2,3]: 2 <Return>
Enter key scheme (LMK): S <Return>
Enter key scheme (ZMK): R <Return>
Enter ZMK: S XXXXXXXX……XXXXXX <Return>
Enter key usage: 72 <Return>
Enter mode of use: N <Return>
Enter key version number: 33 <Return>
Enter exportability: E <Return>
Enter optional blocks? [Y/N]: Y <Return>
Enter optional block identifier: 03 <Return>
Enter optional block data: 2005:12:21:00 <Return>
Enter more optional blocks? [Y/N]: Y <Return>
Enter optional block identifier: 04 <Return>
Enter optional block data: 2007:12:21:00 <Return>
Enter more optional blocks? [Y/N]: N <Return>
Enter exportability field for exported key block:
<Return>
Key under LMK: S YYYYYYYY……YYYYYY
Key under ZMK: R YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online>
```

Example 6:
(AES Key Block LMK)

This example generates a new double length DES key.

```
Online-AUTH> KG <Return>
Enter LMK id: 02 <Return>
Enter algorithm [3DES/AES]: 3 <Return>
Enter key length [1,2,3]: 2 <Return>
Enter key scheme (LMK): S <Return>
Enter key scheme (ZMK): <Return>
Enter key usage: P0 <Return>
Enter mode of use: N <Return>
Enter key version number: 00 <Return>
Enter exportability: N <Return>
Enter optional blocks? [Y/N]: N <Return>
Key under LMK: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 7:
(AES Key Block LMK)

This example generates a new 128-bit AES key.

```
Online-AUTH> KG <Return>
Enter LMK id: 02 <Return>
Enter algorithm [3DES/AES]: A <Return>
Enter key length [128,192,256]: 128 <Return>
Enter key scheme (LMK): S <Return>
Enter key scheme (ZMK): <Return>
Enter key usage: K0 <Return>
Enter mode of use: N <Return>
Enter key version number: 00 <Return>
Enter exportability: N <Return>
Enter optional blocks? [Y/N]: N <Return>
Key under LMK: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Import Key (IK)

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

Command: **IK**

Function: To import a key from encryption under a ZMK to encryption under an LMK. If the key imported does not have odd parity a warning will be issued and odd parity will be forced on the key before encryption under the specified LMK.

Authorization: The HSM must either be in the Authorized State, or the activity **command.ik.console** must be authorized.
For AES LMKs, keys can only be exported in Thales Key Block format.

	Variant LMK	Key Block LMK
Inputs:	• LMK Identifier: 00-99. • Key Type: See the Key Type Table in the *Host Programmer's Manual*. • Key Scheme (LMK). • ZMK to be used to decrypt the key. • Key/Key Block to be imported.	• LMK Identifier: 00-99. • Key Scheme (LMK). • ZMK to be used to decrypt the key. • Key/Key Block to be imported. For import from Variant/X9.17: • Key Usage: See the Key Usage Table in the *payShield 10K Host Programmer's Manual*. • Mode of Use: See the Mode of Use Table in the *payShield 10K Host Programmer's Manual*. • Key Version Number: 00-99. • Exportability: See the Exportability Table in the *payShield 10K Host Programmer's Manual*. • Optional Block data. For import from a key block format: • Modified Key Usage • Optional Block data.
Outputs:	• Key encrypted under an appropriate variant of the selected LMK. • Key Check Value.	• Key Block containing the key encrypted under the selected LMK. • Key Check Value.

Notes:

- For legacy reasons, the import of a ZMK or DEK from encryption under a ZMK (in variant/X9.17 format) to encryption under a key block LMK will not be permitted. Specifically, such import of keys with key usage = "K0", "52", "D0", "21" or "22" will be prohibited.
- Use of this command will always create an entry in the Audit Log.
- If the option "Enforce Atalla variant match to Thales key type" is set to YES in the CS console command, the following matchings between Atalla variant and Thales variant key types will be enforced:

Key Type	Atalla Variant	Thales Variant (*)	Thales Variant (∅)

TPK ZPK	1 or 01	002 LMK 14-15 001 LMK 06-07	70D LMK 36-37/7 001 LMK 06-07
ZEK	2 or 02	00B LMK 32-33 00A LMK 30-31	00B LMK 32-33 00A LMK 30-31
TAK ZAK CVK	3 or 03	003 LMK 16-17 008 LMK 26-27 402 LMK 14-15/4	003 LMK 16-17 008 LMK 26-27 402 LMK 14-15/4
TMK TPK PVK	4 or 04	002 LMK 14-15 002 LMK 14-15 002 LMK 14-15	80D LMK 36-37/8 70D LMK 36-37/7 002 LMK 14-15
TMK	5 or 05	002 LMK 14-15	80D LMK 36-37/8
BDK type-1	8 or 08	009 LMK 28-29	009 LMK 28-29
MK-AC	9 or 09	109 LMK 28-29/1	109 LMK 28-29/1
MK-SMI	9 or 09	209 LMK 28-29/2	209 LMK 28-29/2
MK-SMC	9 or 09	309 LMK 28-29/3	309 LMK 28-29/3
TEK	26	30B LMK 32-33/3	30B LMK 32-33/3
BDK type-2	30	609 LMK 28-29/6	609 LMK 28-29/6
BDK type-3	8 or 08	809 LMK 28-29/8	809 LMK 28-29/8

* Applies if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N"

ø Applies if the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y"

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Must be in Authorized State or Activity not authorized - the key type provided requires the HSM to be in Authorized State.
- Data invalid; please re-enter - the encrypted ZMK does not contain the correct characters, or the key check value does not contain 6 hexadecimal characters. Re-enter the correct number of hexadecimal characters.
- Key parity error; re-enter key - the parity of the ZMK is not odd.
- Warning: key parity corrected - the parity of the key encrypted under the ZMK is not odd.
- Invalid key scheme - the key scheme is invalid.
- Invalid key type; re-enter - the key type is invalid. See the Key Type Table in the *Host Programmer's Manual*.
- Internal failure 12: function aborted - the contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.
- Various key block field errors – the value entered is invalid, or incompatible with previously entered values.

Example 1:
(Variant LMK)

This example imports a key from X9.17 format.

```
Online> IK <Return>
Enter LMK id: 00 <Return>
Enter Key type: 002 <Return>
Enter Key Scheme: U <Return>
Enter ZMK: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Enter key: X XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Encrypted key: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZZZ
```

Example 2:
(Variant LMK)

This example imports a key from TR-31 format.

```
Online> IK <Return>
Enter LMK id: 00 <Return>
Enter key type: 009 <Return>
Enter key scheme (LMK): U <Return>
Enter ZMK: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Enter key: R XXXXXXXX……XXXXXX <Return>
Key under LMK: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZZZ
Online>
```

Example 3:
(3DES Key Block LMK)

This example imports a key from X9.17 format.

```
Online-AUTH> IK <Return>
Enter LMK id: 01 <Return>
Enter key scheme (LMK): S <Return>
Enter ZMK: S XXXXXXXX……XXXXXX <Return>
Enter key: X XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Enter key usage: P0 <Return>
Enter mode of use: N <Return>
Enter key version number: 27 <Return>
Enter exportability: N <Return>
Enter optional blocks? [Y/N]: N <Return>
Key under LMK: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 4:
(3DES Key Block LMK)

This example imports a key from TR-31 format. Note that a new (more restrictive) value for the imported key block's Key Usage field is entered during the import process.

```
Online> IK <Return>
Enter LMK id: 01 <Return>
Enter key scheme (LMK): S <Return>
Enter ZMK: S XXXXXXXX……XXXXXX <Return>
Enter key: R XXXXXXXX……XXXXXX <Return>
Enter modified key usage: 72 <Return>
Enter optional blocks? [Y/N]: Y <Return>
Enter optional block identifier: 03 <Return>
Enter optional block data: 2005:12:21:00 <Return>
Enter more optional blocks? [Y/N]: Y <Return>
Enter optional block identifier: 04 <Return>
Enter optional block data: 2007:12:21:00 <Return>
Enter more optional blocks? [Y/N]: N <Return>
Key under LMK: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online>
```

Example 5:
(3DES or AES Key Block LMK)

This example imports a key from Thales Key Block format.

```
Online> IK <Return>
Enter LMK id: 01 <Return>
Enter key scheme (LMK): S <Return>
Enter ZMK: S XXXXXXXX……XXXXXX <Return>
Enter key: S XXXXXXXX……XXXXXX <Return>
Key under LMK: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online>
```

Export Key (KE)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☑</td><td colspan="2">Offline ☑</td><td colspan="2">Secure ☑</td></tr>
<tr><td>Variant LMK</td><td colspan="5">Authorization: <b>Determined by KTT(E)</b>
Activity: <b>export.{<i>key</i>}.console</b></td></tr>
<tr><td>Key Block LMK</td><td colspan="5">Authorization: <b>If export to non-KB.</b>
Activity: <b>export.{key}.console</b></td></tr>
</table>

Command: **KE**

Function: To translate a key from encryption under the specified LMK to encryption under a ZMK.

<table>
<tr><th></th><th>Variant LMK</th><th>Key Block LMK</th></tr>
<tr><td>Authorization:</td><td>This command examines the 'Export' flag of the given key type within the <b>Key Type Table</b> to determine whether authorization is required. If required, the HSM must either be in the Authorized State, or the activity <b>export.{<i>key</i>}.console</b> must be authorized, where 'key' is the key type code of the key being exported.</td><td>The authorization requirement for this command depends on the type of export being requested:
<table>
<tr><th>Exported key scheme</th><th>Authorization</th></tr>
<tr><td>'S' (<i>Thales Key Block</i>)</td><td>None</td></tr>
<tr><td>'R' (<i>TR-31 Key Block</i>)</td><td>None</td></tr>
<tr><td>'U', 'T' (<i>Variant</i>)</td><td>Required</td></tr>
<tr><td>'Z', 'X', 'Y' (<i>X9.17</i>)</td><td>Required</td></tr>
</table>
If authorization is required, the HSM must either be in the Authorized State, or the activity <b>export.{<i>key</i>}.console</b> must be authorized, where 'key' is the key usage code of the key being exported.

For AES LMKs, keys can only be exported in Thales Key Block format.</td></tr>
<tr><td>Inputs:</td><td>• LMK Identifier: 00-99.
• Key Type: See the Key Type Table in the <i>Host Programmer's Manual</i>.
• Key Scheme (ZMK).
• ZMK to be used to encrypt the key.
• Key to be exported.
For export to Thales Key Block & TR-31:
• Key Usage: See the Key Usage Table in the <i>Host Programmer's Manual</i>.</td><td>• LMK Identifier: 00-99.
• Key Scheme (ZMK).
• ZMK to be used to encrypt the key.
• Key to be exported.

For export to key block format:
• Exportability of exported key.</td></tr>
</table>

	• Mode of Use: See the Mode of Use Table the *payShield 10K Host Programmer's Manual*. • Key Version Number: 00-99. • Exportability: See the Exportability Table in the *payShield 10K Host Programmer's Manual*. • Optional Block data. *Note export from a Variant LMK to Thales Key Block is not permitted.*	
Outputs:	• Key/Key Block encrypted under the ZMK. • Key Check Value.	• Key/Key Block encrypted under the ZMK. • Key Check Value.

Notes:

For legacy reasons, the export of a ZMK, ZEK or DEK from encryption under a key block LMK to encryption under a ZMK (in variant/X9.17 format) will not be permitted. Specifically, such export of keys with key usage = "K0", "52", "D0", "21" or "22" will be prohibited.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Must be in Authorized State or Activity not authorized - the key type provided requires the HSM to be in Authorized State.
- Data invalid; please re-enter - the encrypted ZMK or key does not contain 16 or 32 hex or 1 alpha + 32 hex or 1 alpha + 48 hex. Re-enter the correct number of hexadecimal characters.
- Key parity error; re-enter key - the ZMK or key does not have odd parity on each byte. Re-enter the key and check for typographic errors.
- Invalid key scheme - the key scheme is invalid.
- Invalid key type; re-enter - the key type is invalid. See the Key Type Table the *payShield 10K Host Programmer's Manual*.
- Internal failure 12: function aborted - the contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.
- Various key block field errors – the value entered is invalid, or incompatible with previously entered values.

Example 1:
(Variant LMK)

This example exports a key to X9.17 format.

```
Online-AUTH> KE <Return>
Enter Key type: 002 <Return>
Enter Key Scheme: X <Return>
Enter ZMK: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Enter key: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Key under ZMK: X YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 2:
(Variant LMK)

This example exports a key to TR-31 format.

```
Online-AUTH> KE <Return>
Enter LMK id: 00 <Return>
Enter key type: 001 <Return>
Enter key scheme (ZMK): R <Return>
Enter ZMK: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Enter key: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Enter key usage: P0 <Return>
Enter mode of use: N <Return>
Enter key version number: 44 <Return>
Enter exportability: N <Return>
Enter optional blocks? [Y/N]: N <Return>
Key under ZMK: R YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 3:
(3DES Key Block LMK)

This example exports a key to X9.17 format.

```
Online-AUTH> KE <Return>
Enter LMK id: 01 <Return>
Enter key scheme (ZMK): X <Return>
Enter ZMK: S XXXXXXXX……XXXXXX <Return>
Enter key: S XXXXXXXX……XXXXXX <Return>
Key under ZMK: X YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZZZ
Online-AUTH>
```

Example 4:
(3DES Key Block LMK)

This example exports a key to TR-31 format.

```
Online> KE <Return>
Enter LMK id: 01 <Return>
Enter key scheme (ZMK): R <Return>
Enter ZMK: S XXXXXXXX……XXXXXX <Return>
Enter key: S XXXXXXXX……XXXXXX <Return>
Enter exportability field for exported key block:
<Return>
Key under ZMK: R YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online>
```

Example 5:
(3DES or AES Key Block LMK)

This example exports a key to Thales Key Block format.

```
Online> KE <Return>
Enter LMK id: 01 <Return>
Enter key scheme (ZMK): S <Return>
Enter ZMK: S XXXXXXXX……XXXXXX <Return>
Enter key: S XXXXXXXX……XXXXXX <Return>
Enter exportability field for exported key block:
<Return>
Key under ZMK: S YYYYYYYY……YYYYYY
Key check value: ZZZZZZ
Online>
```

Generate a Check Value (CK)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
Variant LMK	Authorization: **Required if ≠ 6 digits** Activity: **generate.{*key*}.console**	
Key Block LMK	Authorization: **Not required.**	

Command: **CK**

Function: To generate a key check value (KCV) for a key encrypted under a specified LMK.

	Variant LMK	Key Block LMK
Authorization:	This command only requires authorization when calculating either 8 or 16 digit Key Check Values. If required, the HSM must either be in the Authorized State, or the activity **generate.{*key*}.console** must be authorized, where 'key' is the key type of the key being used. Regardless of the authorization requirement, this command examines the 'Generate' flag of the given key type within the **Key Type Table** to determine whether the check value can be calculated.	The HSM does not require any authorization to run this command. Note: Key Check Values of key blocks are always 6-digits in length.
Inputs:	• LMK Identifier: 00-99. • Key Type: See the Key Type Table in the *Host Programmer's Manual*. • Key Length: 1 (single), 2 (double), 3 (triple). • Key.	• LMK Identifier: 00-99. • Key.
Outputs:	• Key Check Value.	• Key Check Value.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Incompatible LMK schemes - the LMK schemes are different.
- Data invalid; please re-enter - incorrect number of characters.
- Key parity error; re-enter key - the entered key does not have odd parity on each byte. Re-enter the complete line (key and Key-Type code) and check for typographic errors.
- Invalid key type; re-enter - the key type is invalid. See the Key Type Table in the *payShield 10K Host Programmer's Manual*.
- Internal failure 12: function aborted - the contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.
- Various key block field errors – the value entered is invalid, or incompatible with previously entered values.

Example 1:
(Variant LMK)

This example generates a check value of a key.

```
Online-AUTH> CK <Return>
Enter LMK id: 00 <Return>
Enter key type code: 001 <Return>
Enter key length flag [S/D/T]: D <Return>
Enter encrypted key: XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX <Return>
Key check value: ZZZZ ZZZZ ZZZZ ZZZZ
Online-AUTH>
```

Example 2:
(Key Block LMK)

This example generates a check value of a key.

```
Online> CK <Return>
Enter LMK id: 01 <Return>
Enter key block: S XXXXXXXXXXXXXXX……XXXXXXXXX <Return>
Key check value: ZZZZZZ
Online>
```

Set KMC Sequence Number (A6)

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

Command: **A6**

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

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

Inputs: New sequence number value.

Outputs: None.

Errors: Not Authorized - The HSM is not in Authorized State
Not Offline – The HSM must be offline to run this command
Invalid Entry – The value entered is invalid (Counter can have any value between 00000000 and FFFFFFFF).

Example:

```
Offline-AUTH> A6 <Return>
Current KMC sequence number is: 00000000 000000F3
Enter new value or <Enter> for no change: 2BAF <Return>
Current KMC sequence number is: 00000000 00002BAF
Offline-AUTH>
```

Payment System Commands

The payShield 10K provides the following console commands to support some of the card payment systems host commands.

Command	Page
Generate a Card Verification Value (CV)	**390**
Generate a VISA PIN Verification Value (PV)	**392**
Load the Diebold Table (R)	**394**
Encrypt Decimalization Table (ED)	**396**
Translate Decimalization Table (TD)	**398**
Generate a MAC on an IPB (MI)	**400**

Generate a Card Verification Value (CV)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
Authorization: **Required** Activity: **misc.console**		

Command:	**CV**
Function:	To generate a VISA CVV or MasterCard CVC.
Authorization:	The HSM must be either in the Authorized State, or the activity **misc.console** must be authorized, using the Authorizing Officer cards of the relevant LMK.
Inputs:	• LMK identifier: indicates the LMK to use when decrypting the supplied CVK(s). • Encrypted CVK • Primary account number (PAN) for the card: up to 19 decimal digits. • Card Expiry date: 4 decimal digits. • Service code: 3 decimal digits.
Outputs:	• Card Verification Value: 3 decimal digits.
Errors:	• Invalid LMK identifier - no LMK loaded or entered identifier out of range. • Command only allowed from Authorized - the HSM is not authorized to perform this operation. • Data invalid; please re-enter - possibly incorrect key length. Could also be incorrect PAN, card expiry date, or service code length or non-decimal PAN, card expiry date or service code. • Key parity error; please re-enter - the parity of the key entered is not odd. • Internal failure 12: function aborted - the contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department. • Various key block field errors – the value entered is invalid, or incompatible with previously entered values.
Notes:	Use of this command will always create an entry in the Audit Log.

Example 1:
(Variant LMK)

This example generates a CVV using a CVK pair encrypted in variant format.

```
Online-AUTH> CV <Return>
Enter LMK id: 00 <Return>
Enter key A: XXXX XXXX XXXX XXXX <Return>
Enter key B: XXXX XXXX XXXX XXXX <Return>
Enter PAN: 1234567812345678 <Return>
Enter expiry date: 0694 <Return>
Enter service code: 123 <Return>
CVV: 321
Online-AUTH>
```

Example 2:
(Variant LMK)

This example generates a CVV using a double length CVK in variant format.

```
Online-AUTH> CV <Return>
Enter LMK id: 00 <Return>
Enter key A: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Enter PAN: 1234567812345678 <Return>
Enter expiry date: 0694 <Return>
Enter service code: 123 <Return>
CVV: 321
Online-AUTH>
```

Example 3:
(Key Block LMK)

This example generates a CVV using a CVK in key block format.

```
Online-AUTH> CV <Return>
Enter LMK id: 01 <Return>
Enter key block: S XXXXXXXX……XXXXXX <Return>
Enter PAN: 1234567812345678 <Return>
Enter expiry date: 0694 <Return>
Enter service code: 123 <Return>
CVV: 321
Online-AUTH>
```

Generate a VISA PIN Verification Value (PV)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
Authorization: **Required** Activity: **misc.console**		

Command: **PV**

Function: To generate a VISA PIN Verification Value (PVV).

Authorization: The HSM must be either in the Authorized State, or the activity **misc.console** must be authorized, using the Authorizing Officer cards of the relevant LMK.

Inputs:

- LMK identifier: indicates the LMK to use when decrypting the supplied PVK(s).
- Encrypted PVK.
- The PVV data block comprising:
  - The 11 right-most digits of the account number (excluding check digit): 11 decimal digits.
  - The PIN verification key indicator (PVKI): 1 decimal digit.
  - The 4 left-most digits of the clear PIN: 4 decimal digits.

Outputs:

- The PIN Verification Value (PVV): 4 decimal digits.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Command only allowed from Authorized - the HSM is not authorized to perform this operation.
- Data invalid; please re-enter - the PVK A, PVK B or the PVV data block field is not 16 characters long. Re-enter the correct number of characters.
- Key parity error; please re-enter - the PVK A or PVK B does not have odd parity on each byte. Re-enter the encrypted PVK A or PVK B and check for typographic errors.
- Internal failure 12: function aborted - the contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.
- Various key block field errors – the value entered is invalid, or incompatible with previously entered values.

Notes:

- The completion of this activity will always be entered in the audit log irrespective of the AUDITOPTIONS settings,

Example 1:
(Variant LMK)

This example generates a PVV using a PVK pair in variant format.

```
Online-AUTH> PV <Return>
Enter LMK id: 00 <Return>
Enter key A: XXXX XXXX XXXX XXXX <Return>
Enter key B: XXXX XXXX XXXX XXXX <Return>
Enter PVV data block: XXXXXXXXXXX N NNNN <Return>
PVV: NNNN
Online-AUTH>
```

Example 2:
(Variant LMK)

This example generates a PVV using a double length PVK in variant format.

```
Online-AUTH> PV <Return>
Enter LMK id: 00 <Return>
Enter key A: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Enter PVV data block: XXXXXXXXXXX N NNNN <Return>
PVV: NNNN
Online-AUTH>
```

Example 3:
(Key Block LMK)

This example generates a PVV using a PVK in key block format.

```
Online-AUTH> PV <Return>
Enter LMK id: 01 <Return>
Enter key block: S XXXXXXXX……XXXXXX <Return>
Enter PVV data block: XXXXXXXXXXX N NNNN <Return>
PVV: NNNN
Online-AUTH>
```

Load the Diebold Table (R)

Variant ☑	Key Block ☑	
Online ☑	Offline ☒	Secure ☒
Authorization: **Required** Activity: **misc.console**		

Command: **R**

Function: To load the Diebold table into user storage in the HSM.

Authorization: The HSM must be online and must be either in the Authorized State, or the activity **misc.console** must be authorized, using the Authorizing Officer cards of the relevant LMK.

Inputs:

- LMK identifier: indicates the LMK to use when encrypting the supplied values.
- Location in user storage at which to store the Diebold table. See notes below.

Outputs:

- The 512-character encrypted table: 16 lines of 32 hexadecimal characters each.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Command only allowed from Online-Authorized - the HSM is not online, or the HSM is not authorized to perform this operation, or both.
- Invalid index - the specified location in user storage is out of range. Enter a valid value.
- Data invalid; please re-enter - the entered index is not 3 hexadecimal characters long, or a table entry is not 16 hexadecimal characters long. Re-enter the correct number of hexadecimal characters.
- Invalid table: duplicate or missing values - some of the data entered is not a valid entry for a Diebold table. Check the table and re-enter the data, checking for typographic errors.
- Internal failure 12: function aborted - the contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Notes:

- Encryption of the Diebold Table:
  - o If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "N", the Diebold table is encrypted using LMK pair 14-15 variant 0.
  - o If the security setting "Enforce key type 002 separation for PCI HSM compliance" has the value "Y", the Diebold table is encrypted using LMK pair 36-37 variant 6.
- User Storage is structured in different ways depending on whether the security setting "User storage key length" has a fixed length value (setting = S(ingle), D(ouble), T(riple)) or is variable (setting = V(ariable)).
  - o If the length is fixed, the Diebold table is stored as 32 contiguous blocks of 16 characters. The index for the first block must be in the range 000-FE0.
  - o If the length is variable, the Diebold table is stored as a single block of 512 characters. Because this needs to use one of the larger slots capable of handling blocks larger than 100 bytes, the index must be in the range 000-07F.

  See the *payShield 10K Host Programmer's Manual* for further information.
- If the security setting "Enforce key type 002 separation for PCI HSM compliance" is changed, the Diebold Table must be re-entered by using this command. Therefore, it is important that the cleartext version of the table is retained.

Example: *The security setting "User storage key length" has a fixed length value.*

```
Online-AUTH> R <Return>
Enter LMK id: 00 <Return>
Enter index (000 – FE0): XXX <Return>
Now enter table, 16 hex digits/line
Line 01: XXXX XXXX XXXX XXXX <Return>
XXXX XXXX XXXX XXXX OK? [Y/N] Y <Return>
Line 02:
…
…
Line 32: XXXX XXXX XXXX XXXX <Return>
XXXX XXXX XXXX XXXX OK? [Y/N] Y <Return>

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
…
…
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX (16 lines of
encrypted table are displayed)
Online-AUTH>
```

Note: The result of the "R" command gives no indication as to the LMK scheme or LMK identifier used in the command. When this value is used with other (host) commands, the user must ensure that the correct LMK is specified in the command.

Encrypt Decimalization Table (ED)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
Authorization: **Required** Activity: **misc.console**		

Command: **ED**

Function: To encrypt a 16 digit decimalization table for use with host commands using IBM 3624 PIN Generation & Verification.

Authorization: The HSM must be either in the Authorized State, or the activity **misc.console** must be authorized, using the Authorizing Officer cards of the relevant LMK.

Inputs:

- LMK identifier: indicates the LMK to use when encrypting the decimalization table.
- Decimalization table. 16 decimal digits that specify the mapping between hexadecimal & decimal numbers.
- The HSM by default checks that the decimalization table contains at least 8 different digits, with no digit repeated more than 4 times. This feature may be disabled using the Configure Security parameter "Enable decimalization table check". Disabling of this feature is not recommended.

Outputs:

- Encrypted decimalization table:
  - 16 Hex characters when using a Variant LMK or a 3DES Key Block LMK.
  - 32 Hex characters when using an AES LMK.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Not Authorized - the HSM is not authorized to perform this operation.
- Decimalization table invalid - the decimalization table is not all decimal or does not contain at least 8 different digits with no digit repeated more than 4 times.
- Master Key Parity Error - the contents of the HSM storage have been corrupted or erased. Do not continue. Inform the security department.

Example: (Variant or 3DES Key Block LMK)

This example encrypts a decimalization table using a Variant LMK (same applies with 3DES Key Block LMK).

```
Online-AUTH> ED <Return>
Enter LMK id: 00 <Return>
Enter decimalization table: 0123456789012345 <Return>
Encrypted decimalization table: XXXX XXXX XXXX XXXX
Online-AUTH>
```

Example: (AES Key Block LMK)

This example encrypts a decimalization table using an AES LMK.

```
Online-AUTH> ED <Return>
Enter LMK id: 00 <Return>
Enter decimalization table: 0123456789012345 <Return>
Encrypted decimalization table: XXXX XXXX XXXX XXXX XXXX
XXXX XXXX XXXX
Online-AUTH>
```

Note: The result of the "ED" command gives no indication as to the LMK scheme or LMK identifier used in the command. When this value is used with other (host) commands, the user must ensure that the correct LMK is specified in the command.

Translate Decimalization Table (TD)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
Authorization: **Required** Activity: **misc.console**		

Command: **TD**

Function: To translate an encrypted decimalization table from Encryption under an old LMK to encryption under the corresponding new LMK.

Authorization: The HSM must be either in the Authorized State, or the activity **misc.console** must be authorized, using the Authorizing Officer cards of the relevant LMK.

Inputs:

- LMK identifier: indicates the LMK to use when translating the decimalization table.
- Encrypted Decimalization table. This is the result of encrypting a decimalization table using the ED command. The size of the encrypted decimalization table depends on the LMK used to encrypt it: for DES-based Variant and 3DES Key Block LMKs, the size is 16 hex digits. For AES Key Block LMKs, the size is 32 hex digits.
- The HSM by default checks that the decimalization table contains at least 8 different digits, with no digit repeated more than 4 times. This feature may be disabled using the Configure Security parameter "Enable decimalization table check". Disabling of this feature is not recommended.

Outputs:

- Encrypted decimalization table:
  - 16 Hex characters when using a Variant LMK or a 3DES Key Block LMK.
  - 32 Hex characters when using an AES LMK.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Not Authorized - the HSM is not authorized to perform this operation.
- Decimalization Table Invalid - decimalization table not all decimal or does not contain at least 8 different digits with no digit repeated more than 4 times.
- Master Key Parity Error - the contents of the HSM storage have been corrupted or erased. Do not continue. Inform the security department.
- No LMK in Key Change Storage - Key Change storage is empty.

Example:
(Variant or 3DES Key Block LMK)

```
Online-AUTH> TD <Return>
Enter LMK id: 00 <Return>
Enter decimalization table encrypted under old LMK :
XXXXXXXXXXXXXXXX <Return>
Decimalization table encrypted under new LMK       :
YYYYYYYYYYYYYYYY
Online-AUTH>
```

Example:
(AES Key Block LMK)

```
Online-AUTH> TD <Return>
Enter LMK id: 00 <Return>
Enter decimalization table encrypted under old LMK :
XXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX <Return>
Decimalization table encrypted under new LMK       :
YYYYYYYYYYYYYYYY YYYYYYYYYYYYYYYY
Online-AUTH>
```

Note: The result of the "TD" command gives no indication as to the LMK scheme or LMK identifier used in the command. When this value is used with other (host) commands, the user must ensure that the correct LMK is specified in the command.

Generate a MAC on an IPB (MI)

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

Command: **MI**

Function: To generate a MAC on the Cryptogram component of a CAP IPB.

Authorization: The HSM must be either in the Authorized State, or the activity **misc.console** must be authorized, using the Authorizing Officer cards of the relevant LMK.

Inputs:

- LMK identifier: indicates the LMK to use when generating the MAC.
- 8 byte IPB represented as 16 hex ASCII characters.

Outputs:

- 4 byte MAC over the plaintext IPB input data.

Errors:

- Invalid LMK identifier - no LMK loaded or entered identifier out of range.
- Command only allowed from Authorized - the HSM is not authorized to perform this operation.
- IPB is not 8 bytes. Please re-enter - the validation of the IPB failed.
- Warning: Less than 16 '1'bits in IPB - the IPB contains less than 16 '1' bits.

Example:

```
Online-AUTH> MI <Return>
Enter LMK id: 00 <Return>
Enter IPB: FFFFFFFF00000000 <Return>
      MAC: FB1A 3C1A
Online-AUTH>
```

Note: The result of the "MI" command gives no indication as to the LMK scheme or LMK identifier used in the command. When this value is used with other (host) commands, the user must ensure that the correct LMK is specified in the command.

Smartcard Commands

The payShield 10K provides the following console commands to support HSM smartcards. Please note that some of these commands are designed to operate only with the legacy HSM smartcards while other may support both the legacy and new smartcards used in the payShield Manager.

Command	**Page**
Format an HSM Smartcard (FC)	**402**
Create an Authorizing Officer Smartcard (CO)	**404**
Verify the Contents of a Smartcard (VC)	**405**
Change a Smartcard PIN (NP)	**406**
Read Unidentifiable Smartcard Details (RC)	**407**
Eject a Smartcard (EJECT)	**408**

Note: DO NOT REPEATEDLY ENTER INVALID PINS. A LEGACY SMARTCARD "LOCKS" AFTER EIGHT SUCCESSIVE INVALID PINS HAVE BEEN ENTERED. LEGACY SMARTCARDS CAN BE "UNLOCKED" BY REFORMATTING, WHICH DELETES THE ENTIRE CONTENTS OF THE CARD. NEW SMARTCARDS USED BY THE PAYSHIELD MANAGER LOCK AFTER FIVE SUCCESSIVE INVALID PINS HAVE BEEN ENTERED. THEY MAY BE UNLOCKED BY RECOMMISSIOING THEM.

Format an HSM Smartcard (FC)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **FC**

Function: To format an HSM smartcard for use by the HSM.
Different formats are used for LMK storage and saving HSM settings.
payShield Manager cards do not need to be formatted.

Authorization: The HSM does not require any authorization to run this command.

Inputs:

- (LMK cards): Smartcard PIN: 5 to 8 alphanumeric characters.
- Date: 6 numeric character format DDMMYY.
- Time: 6 numeric characters; format hhmmss.
- Issuer ID: maximum 35 alphanumeric characters.
- User ID: maximum 35 alphanumeric characters.

Outputs:

- Text messages:
  - Insert card and press ENTER.
  - Format card for HSM settings/LMKs? [H/L]
  - Enter new PIN for smartcard.
  - Re-enter new PIN.
  - Enter format code.
  - Enter date.
  - Enter time.
  - Enter Issuer ID.
  - Enter User ID.
  - Format complete.
  - Card already formatted, continue? [Y/N].

Note:

- This command only operates with legacy HSM smartcards.

Errors:

- Invalid PIN; re-enter - the PIN entered is fewer than 5 or greater than 8 digits.
- PINs did not agree - the new PINs entered for the card did not match each other.
- Invalid input. Entry must be in numeric format - non numeric value is entered for time or date.

Example 1:

```
Online> FC <Return>
Insert card and press ENTER: <Return>
Card already formatted, continue? [Y/N]: Y <Return>
Format card for HSM settings/LMKs? [H/L]: L <Return>
Erasing card
Formatting card . . .
Enter new PIN for Smartcard: ******* <Return>
Re-enter new PIN: ******* <Return>
Enter time [hhmmss]: 153540 <Return>
Enter date [ddmmyy]: 261093 <Return>
Enter User ID: Joe Small <Return>
Enter Issuer ID: Big Bank plc <Return>
Format complete
Online>
```

Example 2:

```
Online> FC <Return>
Insert card and press ENTER: <Return>
Card already formatted, continue? [Y/N]: Y <Return>
Format card for HSM settings/LMKs? [H/L]: H <Return>
      Erasing card
      Formatting card . . .
Format complete
Online>
```

Create an Authorizing Officer Smartcard (CO)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☑</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **CO**

Function: To copy the Password for an Authorizing Officer to another smartcard (RLMKs are supported) so that it can be used to set the HSM into the Authorized State. Note that only LMK component cards 1 and 2 contain the Password.

Authorization: The HSM must be in the offline or secure state to run this command.

Inputs:

- Smartcard PIN: 5 to 8 alphanumeric characters. PINs must be entered within 60 seconds of being requested.

Outputs:

- Text messages:

Insert Card for Component Set 1 or 2 and enter the PIN.
Insert Card for Authorizing Officer and enter the PIN.
Copy Complete.

Errors:

- Card not formatted - card not formatted
- Not a LMK card - card is not formatted for LMK or key storage.
- Smartcard error; command/return: 0003 - an invalid PIN was entered.
- Invalid PIN; re-enter - PIN is fewer than 5 or greater than 8 digits.
- Card not blank - copy failed.

Example:

```
Offline> CO <Return>
Insert Card for Component Set 1 or 2 and enter PIN:
******** <Return>
Insert Card for Authorizing Officer and enter PIN:
******** <Return>
Copy complete.
Offline>
```

Verify the Contents of a Smartcard (VC)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☑</td><td colspan="2">Offline ☑</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **VC**

Function: To verify the key component or share held on a smartcard. The HSM reads the key component from the smartcard, computes the check value, compares this with the check value stored on the card and displays the result.

Authorization: The HSM does not require any authorization to run this command.

Inputs:

- Smartcard PIN: 5 to 8 alphanumeric characters. PINs must be entered within 60 seconds of being requested.

Outputs:

- Component Set check value:
    - For Variant LMKs, the length of the displayed check value is determined by the CS (Configure Security) setting "Restrict Key Check Value to 6 hex chars".
    - For Key Block LMKs, the length of the displayed check value is always 6 hex digits.
- Comparison: Pass or Fail.
- Text messages:
    - Check:
    - Compare with card:

Errors:

- Card not formatted - card not formatted
- Not a LMK card - card is not formatted for LMK or key storage.
- Smartcard error; command/return: 0003 - an invalid PIN was entered.
- Invalid PIN; re-enter - PIN is fewer than 5 or greater than 8 digits.

Example:

```
Online> VC <Return>
Insert card and enter PIN: ******** <Return>

Scheme: Variant
Check: 012345.
Compare with card: Pass.
Online>
```

If a smartcard is defective or cannot be successfully verified, replace it. Copy a verified smartcard (from the same set of components) onto a replacement.

Note: DISPOSE OF THE FAULTY SMARTCARD IN A SECURE MANNER.

Change a Smartcard PIN (NP)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **NP**

Function: To select a new PIN for a smartcard (RACCs and RLMKs are supported) without changing any of the other details stored on the card.
The old PIN must be submitted before a change is effected and the new PIN must be supplied correctly at two consecutive prompts.

Authorization: The HSM does not require any authorization to run this command.

Inputs:

- Smartcard PIN: 5 to 8 alphanumeric characters. PINs must be entered within 60 seconds of being requested.

Outputs:

- Text messages:
  - Insert Card and press ENTER.
  - Enter current PIN.
  - Enter new PIN for smartcard.
  - Re-enter new PIN.
  - PIN change completed.

Errors:

- Card not formatted - card not formatted
- Not a LMK card - card is not formatted for LMK or key storage.
- Smartcard error; command/return: 0003 - an invalid PIN was entered.
- Invalid PIN; re-enter - PIN is fewer than 5 or greater than 8 digits.
- PINs did not agree - the new PINs entered for the smartcard did not match.

Example:

```
Online> NP <Return>
Insert card and press ENTER: <Return>
Enter current PIN: **** <Return>
Enter new PIN for smartcard: **** <Return>
Re-enter new PIN: **** <Return>
PINs did not agree
Enter new PIN for smartcard: **** <Return>
Re-enter new PIN: **** <Return>
PIN change completed
Online>
```

Read Unidentifiable Smartcard Details (RC)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **RC**

Function: To read otherwise unidentifiable smartcards (RACCs and RLMKs supported).

Authorization: The HSM does not require any authorization to run this command.

Inputs: None.

Outputs:

- Text messages:
  - Insert Card and press ENTER when ready.
  - This card is formatted for saving and retrieving HSM settings.
  - Version, as stored on card: decimal integer.
  - Date, as stored on card; format: YY/MM/DD.
  - Time, as stored on card; format: hh:mm:ss.
  - User ID, as stored on card; free format alphanumeric.
  - Issuer ID, as stored on card; free format alphanumeric.
  - Data Zone Size, as stored on card: decimal integer.
  - Max Data Free, as stored on card: decimal integer.

Errors:

- Card not formatted - card not formatted
- Not a LMK card - card is not formatted for LMK or key storage.

Example 1:

```
Online> RC <Return>
Insert card and press ENTER: <Return>
Format version: 0001
Issue time: 11:53:00
Issue date: 93/10/25
User ID: Bill Weasel
Issuer ID: Big Bank plc
User-data zone size: 0000
Free: 0392
Online>
```

Example 2:

```
Online> RC <Return>
Insert card and press ENTER: <Return>
This card is formatted for saving and retrieving HSM
settings.
Online>
```

Eject a Smartcard (EJECT)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☑</td><td colspan="2">Offline ☑</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **EJECT**

Function: To eject the smartcard from the smartcard reader.

Authorization: The HSM does not require any authorization to run this command.

Inputs: None.

Outputs: None.

Errors: None.

Example:

```
Online> EJECT <Return>
Online>
```

DES Calculator Commands

The payShield 10K provides the following console commands to support the encryption and decryption of data with a given plaintext single, double or triple-length DES key:

Command	Page
Single-Length Key Calculator (N)	**410**
Double-Length Key Calculator ($)	**411**
Triple-Length Key Calculator (T)	**412**

Single-Length Key Calculator (N)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **N**

Function: To encrypt and decrypt the given data block with the given single-length key.

Authorization: The HSM does not require any authorization to run this command.

Inputs:

- Key (no parity required): 16 hexadecimal characters.
- Data block: 16 hexadecimal characters.

Outputs:

- The data encrypted with the key.
- The data decrypted with the key.

Errors:

- Data invalid; please re-enter - the entered data does not comprise 16 hexadecimal characters. Re-enter the correct number of hexadecimal characters.

Example:

```
Online> N <Return>
Enter key: XXXX XXXX XXXX XXXX <Return>
Enter data: XXXX XXXX XXXX XXXX <Return>
Encrypted: YYYY YYYY YYYY YYYY
Decrypted: YYYY YYYY YYYY YYYY
Online>
```

Double-Length Key Calculator ($)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **$**

Function: To encrypt and decrypt the given data block with the given double-length key.

Authorization: The HSM does not require any authorization to run this command.

Inputs:

- The double-length key (odd parity is required): 32 hexadecimal characters.
- Data block: 16 hexadecimal characters.

Outputs:

- The data encrypted with the key.
- The data decrypted with the key.

Errors:

- Data invalid; please re-enter - the entered data does not comprise 32 hexadecimal characters. Re-enter the correct number of hexadecimal characters.

Example:

```
Offline> $ <Return>
Enter key: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>
Enter data: XXXX XXXX XXXX XXXX <Return>
Encrypted: YYYY YYYY YYYY YYYY
Decrypted: YYYY YYYY YYYY YYYY
Offline>
```

Triple-Length Key Calculator (T)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **T**

Function: To encrypt and decrypt the given data block with the given triple-length key.

Authorization: The HSM does not require any authorization to run this command.

Inputs:

- The triple-length key (odd parity is required): 48 hexadecimal characters.
- Data block: 16 hexadecimal characters.

Outputs:

- The data encrypted with the key.
- The data decrypted with the key.

Errors:

- Data invalid; please re-enter - Re-enter the correct number of hexadecimal characters.

Example:

```
Offline> T <Return>
Enter key: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX XXXX XXXX <Return>
Single, Double, or Triple length data? (S,D,T): S
<Return>
Enter data: XXXX XXXX XXXX XXXX <Return>
Encrypted: YYYY YYYY YYYY YYYY
Decrypted: YYYY YYYY YYYY YYYY
Offline>
```

payShield Manager Commands

This section describes the commands used to configure the HSM for use with the payShield Manager.

The payShield 10K provides the following console commands to support the payShield Manager:

Command	Page
Add a RACC to the whitelist (XA)	414
Decommission the HSM (XD)	415
Remove RACC from the whitelist (XE)	416
Commission the HSM (XH)	417
Generate Customer Trust Authority (XI)	418
Make an RACC left or right key (XK)	420
Commission a smartcard (XR)	421
Transfer existing LMK to RLMK (XT)	422
Decommission a smartcard (XX)	424
HSM commissioning status (XY)	425
Duplicate CTA share (XZ)	426

Note that the HSM's private key, the certified public key and the Domain Authority self-signed public key certificate are recovered by use of the HSM Master Key (HRK) if a tamper attempt has occurred.

Add a RACC to the whitelist (XA)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☒</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **XA**

Function: To add a RACC to the whitelist on the HSM.

Authorization: The HSM must be in Secure state to run this command.

Inputs:

- None

Outputs:

- None

Example 1**:**

```
Secure> XA <Return>

Insert payShield Manager Smartcard and press ENTER:
<Return>
Enter PIN:  ****** <Return>

Do you want to add card XYZ123 to the whitelist? Y
<Return>

Card XYZ123 added to whitelist.

Secure>
```

Decommission the HSM (XD)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☒</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **XD**

Function: To decommission the HSM by deleting the payShield Managers keys and groups.

Authorization: The HSM must be in Secure state to run this command.

Inputs:

- None

Outputs:

- None

Example 1**:**

```
Secure> XD <Return>

Do you want to erase the payShield Manager's keys and
groups? [Y/N]: Y <Return>

Secure>
```

Remove RACC from the whitelist (XE)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☒</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **XE**

Function: To remove an RACC from the whitelist.

Authorization: The HSM must be in Secure state to run this command.

Inputs:

- None

Outputs:

- None

Example 1:

```
Secure> XE <Return>

Choice   ID            Type
   1     ABC321        restricted
   2     XYZ123        restricted
Which RACC do you want to remove? 1 <Return>

Card ABC321 removed from whitelist

Secure>
```

Commission the HSM (XH)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **XH**

Function: To commission the HSM

Authorization: The HSM must be in Secure state to run this command.

Inputs:

- None

Outputs:

- None

Example 1:

```
Secure> XH <Return>

Please have all Customer Trust Authority (CTA) payShield
Manager smartcards available
Insert first CTA payShield Manager Smartcard and press
ENTER: <Return>
Enter PIN:  ****** <Return>
Insert CTA payShield Manager Smartcard 2 of 3 and press
ENTER: <Return>
Enter PIN:  ****** <Return>
Insert CTA payShield Manager Smartcard 3 of 3 and press
ENTER: <Return>
Enter PIN:  ****** <Return>

Starting the commissioning of the HSM process...
Please insert left key card and press ENTER: <Return>
Enter PIN:  ****** <Return>
Please insert right key card and press ENTER: <Return>
Enter PIN:  ****** <Return>

Successfully commissioned HSM

Secure>
```

Generate Customer Trust Authority (XI)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **XI**

Function: Generates the Customer Trust Authority and stores them on smartcards.

Authorization: The HSM must be in Secure state to run this command.

Inputs:

- Country
- State
- Locality
- Organization
- Organizational Unit
- Common Name
- Email
- Number of private shares
- Number of shares needed to recover private key

Outputs:

- None

Example 1:

```
Secure> XI <Return>

Please enter the certificate Subject information:
     Country Name (2 letter code) [US]: US <Return>
     State or Province Name (full name) []: Florida
<Return>
     Locality Name (eg, city) []: Plantation <Return>
     Organization Name (eg, company) []: Thales <Return>
     Organizational Unit Name (eg, section) []:
Production <Return>
     Common Name (e.g. server FQDN or YOUR name) [CTA]:
CTA <Return>
     Email Address []: info@thalesesec.com <Return>

Enter number of Customer Trust Authority private key
shares [3-9]: 3 <Return>
Enter number of shares to recover the Customer Trust
Authority private key [3-3]: 3 <Return>

   Issued to: CTA, Issued by: CTA
   Validity : Jan  9 10:28:49 2015 GMT to Jan  3 10:28:49
2040 GMT
   Unique ID: EE3CB7CE8343B464CC04278188CF7EB3 - 3DE05514
(Root)

Insert payShield Manager Smartcard 1 of 3 and press
ENTER: <Return>
Enter new PIN for smartcard:  ****** <Return>
Re-enter new PIN:  ****** <Return>
Working....
CTA share written to smartcard.

Insert payShield Manager Smartcard 2 of 3 and press
ENTER: <Return>
Enter new PIN for smartcard:  ****** <Return>
Re-enter new PIN:  ****** <Return>
Working....
```

```
CTA share written to smartcard.

Insert payShield Manager Smartcard 3 of 3 and press
ENTER: <Return>
Enter new PIN for smartcard:  ****** <Return>
Re-enter new PIN:  ****** <Return>
Working....
CTA share written to smartcard.

Successfully generated a Customer Trust Authority
Secure>
```

Make an RACC left or right key (XK)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **XK**

Function: Defines a RACC as either a left or right key in the whitelist on the HSM.

Authorization: The HSM must be in Secure state to run this command.

Inputs: Left or Right (card type)

Outputs:

- None

Example 1:

```
Secure> XK <Return>

Insert payShield Manager Smartcard and press ENTER:
<Return>
Enter PIN:  ****** <Return>
Do you want to make ABC321 a [L]eft or [R]ight key? L
<Return>

Card ABC321 is now a left key.

Secure>
```

Commission a smartcard (XR)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☒</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **XR**

Function: To commission a smartcard.

Authorization: The HSM must be in Secure state to run this command.

Inputs:

- None

Outputs:

- None

Example 1**:**

```
Secure> XR <Return>

Please have all Customer Trust Authority (CTA) payShield
Manager smartcards available
Insert first CTA payShield Manager Smartcard and press
ENTER: <Return>
Enter PIN:  ******
Insert CTA payShield Manager Smartcard 2 of 3 and press
ENTER: <Return>
Enter PIN:  ******
Insert CTA payShield Manager Smartcard 3 of 3 and press
ENTER: <Return>
Enter PIN:  ******
Enforce a PIN change on first use? [Y/N]: N <Return>
Insert a payShield Manager Smartcard to be commissioned
and press ENTER: <Return>
Enter new PIN for smartcard:  ****** <Return>
Re-enter new PIN:  ****** <Return>
Do you wish to add the smartcard A3 to the HSM whitelist
[Y/N]: Y <Return>
Assign smartcard as a Left or Right Key RACC? [L/R/N]: N
<Return>
Would you like to commission another card? [Y/N]: N
<Return>

Secure>
```

Transfer existing LMK to RLMK (XT)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **XT**

Function: To transfer an existing HSM LMK stored on legacy smartcards to payShield Manager RLMK cards for use through the payShield Manager.

In order to transfer a Variant LMK you will be required to fully reassemble the LMK (bring all the components together). Then, the fully formed Variant LMK is split among shares onto the pre-commissioned payShield Manager RLMK cards.

For Key Block LMKs, they are not stored as components on non-payShield Manager smart cards, but as shares. However, you must bring a quorum of share holders together, reconstitute the LMK, and then split it among shares onto the pre-commissioned payShield Manager RLMK cards.

Authorization: The HSM must be in Secure state to run this command.

Inputs:

- Number of shares to split LMK into
- Number of Components required to reconstitute LMK

Outputs:

- None

Example 1:

```
Secure> XT <Return>

Please have all the local LMK components and enough
commissioned RACCs to receive the LMK ready.

Insert card and press ENTER: <Return>
Enter PIN: ***** <Return>

Check: 268604
Load more components? [Y/N]: N <Return>

LMK Check:      268604
LMK key scheme: Variant
LMK algorithm:  3DES(2key)
LMK status:     Test

Is this the LMK you wish to transfer? [Y/N]: Y <Return>

Enter the number of shares to split the LMK into: [2-9]:
2 <Return>
The number of shares required to reconstitute the LMK:
[2-2]: 2 <Return>

Insert a commissioned card 1 of 2 and press ENTER:
<Return>
Enter PIN:  ****** <Return>

Card Check: E0CBF4
LMK share written to smartcard.

Insert a commissioned card 2 of 2 and press ENTER:
<Return>
Enter PIN:  ****** <Return>
```

```
Card Check: E0CBF4
LMK share written to smartcard.
Want to test the reassembly of the LMK? Y <Return>

Please have all the RLMK shares ready
Insert RLMK card and press ENTER: <Return>
Enter PIN:  ****** <Return>
LMK share 1 read (1 of 2) Card Check: E0CBF4
Insert RLMK card and press ENTER: <Return>
Enter PIN:  ****** <Return>
LMK share 2 read (2 of 2) Card Check: E0CBF4

LMK Check 268604

Secure>
```

Decommission a smartcard (XX)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☑</td><td colspan="2">Offline ☑</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **XX**

Function: To decommission a payShield Manager smartcard.

Authorization: The HSM may be in any state to run this command.

Inputs:

- None

Outputs:

- None

Example 1**:**

```
Secure> XX <Return>

Please insert card to decommission and press ENTER:
<Return>
Warning: Resetting a payShield Manager Smartcard to its
original state
will erase all key material from the card.

Are you sure? [Y/N]: Y <Return>

payShield Manager Smartcard successfully decommissioned
Would you like to decommission another card? [Y/N]: N
<Return>

Secure>
```

HSM commissioning status (XY)

Variant ☑	Key Block ☑	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **XY**

Function: To show the state of the HSM Management commissioning and whitelist.

Authorization: The HSM may be in any state to run this command.

Inputs:

- None

Outputs:

- Thales Trust installed
- Customer Trust Authority installed
- HSM Public Key installed
- Is HRK password user defined
- Is HRK available for use
- Authorized RACCs

Example 1**:** **Note:** The following contains sample output, e.g., Issue to: *TES LC.*

```
Online>xy

Thales Trust installed               : Yes
     1 - Issued to: A4665000000A, Issued by: Development
Factory TTA
         Validity : Sep 26 15:35:30 2018 GMT to Sep 20
15:35:30 2043 GMT
         Unique ID: B655F28FD784A9C2A5169FF4F4DD41EA -
D61B5F4A

Customer Trust Authority Installed      : Yes
     2 - Issued to: TES LC, Issued by: TES LC
         Validity : Oct  5 13:11:12 2018 GMT to Sep 29
13:11:12 2043 GMT
         Unique ID: 9FEACF2E361A2BADA0E2E9238D121E1D -
27871B3A (Root)


HSM Public Key Certificate Installed : Yes
     3 - Issued to: A4665000000A, Issued by: TES LC
         Validity : Oct 30 16:01:34 2018 GMT to Oct 24
16:01:34 2043 GMT
         Unique ID: ABA92BB246260EFF838BD06062331E54 -
27871B3A


Is HRK passphrase user defined       : Yes

Is HRK available for use             : Yes

Authorized RACCs                     : 4
   Serial Number               Certificate
Number           RACC Type
   7307001132072979      BF9BBAA7525818AA       Left
   7307001145072979      392FDA0DD7B25CBA      Left
   7307001152072979      DBD139588ED7A17C       Right
   7307001265072979      223386DBE9391015         Right

Online>
```

Duplicate CTA share (XZ)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **XZ**

Function: To duplicate a CTA share smartcard.

Authorization: The HSM must be in Secure state to run this command.

Inputs:

- None

Outputs:

- None

Example 1**:**

```
Secure> XZ <Return>

Insert a CTA share payShield Manager Smartcard to be
duplicated:
Enter PIN:  ****** <Return>
Working...
Please insert a commissioned payShield Manager smartcard
and press ENTER: <Return>
Enter PIN:  ****** <Return>
Working...
CTA share written to smartcard.

Secure>
```

Secure Host Communications

This section describes the commands used to configure a payShield 10K such that the host connection is protected using TLS (known as Secure Host Communications).

The Certificate Requests and Certificates may be stored on / loaded from a regular USB memory stick.

The required format for the USB memory stick is FAT32. 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.

The HSM's certificate signing request (CSR) structure is compliant with PKCS#10. The client must use the same key type as is included in the HSM's CSR.

The HSM uses certificate formats compliant with X.509.

The payShield 10K provides the following console commands to manage the HSM's private key, the certified public key and the CA self-signed public key certificate to support secure host communications:

Command	**Page**
Generate Certificate Signing Request (SG)	**428**
Import Certificate (SI)	**431**
Export HSM Certificate's Chain of Trust (SE)	**433**
View Installed Certificate(s) (SV)	**435**
Delete Installed Certificate(s) (SD)	**438**
Generate HRK (SK)	**439**
Change HRK Passphrase (SP)	**440**
Restore HRK (SL)	**441**

The HRK enables the recovery of the HSM's private key, the certified public key and the CA self-signed public key certificate used for payShield Manager.

Generate Certificate Signing Request (SG)

Variant ☑		Key Block ☑
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **SG**

Function: To generate the HSM's public/private key pair for use with secure host communications, and extract the public key in the form of a Certificate Signing Request (".CSR").
The private key is stored in tamper protected memory. It is backed up internally using the HSM Master Key (HRK) – see command SK for details.

Authorization: The HSM must be in the secure state to run this command.

Inputs:

- Certificate fields (Country, State, Locality, Org Name, Org Unit Name, Common Name, E-mail Address).
- Key Type (RSA, ECDSA)
- Filename when saving to USB memory stick

Outputs:

- Prompts, as above
- Key generation message
- Prompt to save to USB memory stick
- Certificate Signing Request

Errors:

- File exists – replace?

Notes:

- The HRK must be installed (using the SK console command) prior to using this command.
- The exported file will automatically have the extension ".CSR".
- The size of RSA keys used is 2048-bits.
- The size of ECDSA keys used is either 256-bits, 384-bits or 521-bits (user selectable).
- The client must use the same RSA/ECDSA key type as is included in the HSM's CSR.
- A maximum certificate chain length of 6 is supported.
- The required format for the USB memory stick is FAT32. The Operating System used in the payShield 10K supports most types of USB memory stick, 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.

Example 1: *This example demonstrates the use of the **SG** console command to generate a 521-bit ECDSA public/private key pair and output a certificate signing request.*

```
Secure> SG <Return>
Please enter the Subject Information for the Certificate Request:

   Country Name (2 letter code) []: UK <Return>
   State or Province Name (full name) []: Greater London <Return>
   Locality Name (eg, city) []: London <Return>
   Organization Name (eg, company) []: Bank XYZ <Return>
   Organizational Unit Name (eg, section) []: Operations <Return>
   Common Name (e.g. server FQDN or YOUR name) []: HSM-0001
<Return>
   Email Address []: bill@bankxyz.com <Return>

Select key type:
  1 - RSA
  2 - ECDSA P-256
  3 - ECDSA P-384
  4 - ECDSA P-521
Type [4]: 4 <Return>

Generating key pair ......................+++
.......+++
DONE

Do you wish to save to a file [Y/N]: Y <Return>
Enter filename: HSM-0001 <Return>
-----BEGIN CERTIFICATE REQUEST-----
MIIC2TCCAcECAQAwgZMxCzAJBgNVBAYTAlVLMRcwFQYDVQQIEw5HcmVhdGVyIExv
bmRvbjEPMA0GA1UEBxMGTG9uZG9uMREwDwYDVQQKEwhCYW5rIFhZWjETMBEGA1UE
CxMKT3BlcmF0aW9uczERMA8GA1UEAxMISFNNLTAwMDIxHzAdBgkqhkiG9w0BCQEW
EGJpbGxAYmFua3h5ei5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQC+JhIisca5k7l5YIRNcDcq/QMb3jHzhQIbME4O9zDhTtmINFM7YrvZ6N2Sy1TU
za1cPf9JKR2X5D3ukaICtkTwxArj1WRnU2UnINTYeO0RWeBaouxO4ijSvzx5mCCg
RtcSQDK748+0xgWlZezkKkv+akOh4vYPdiOKx47wiS7UAENBaQI14C5cbnj6JMLe
f3hmzQzzu3vACAIDbuQXZ5A7w7ecGLSLahjEyx1H7PXpLnul2lPRlBcemVdqHi8f
dfXTAKE1RrKSrvU22sOn6uQLGFRTseIuC4tFvtZNJRHAtqCYpabV4vrBmNQDaw8W
p2FFu+e71ybqsLY0R5xt7ZABAgMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEAvVzS
iy5gJkAjUdqaBjr5MUoAXvk15fEg6gO+SV39X3mSsQklQdoHwFSNgOUWYHkTKPvN
vZnCxMlUK2nBhlu2Xz44yC/U7+E7FsaQz2nXrNx/gF3SY/a/ODA+Y9iSERIpwRCM
9CKapYONeBHqK/NIcgTOZ3SMsC9JXsvtxPyQ7vmbu4a/JpMantWfcLCA+z6i+S+H
WavGnPVGt9ERD5Cij7B6qSbbrkn+xoJARIGsXhbVQmdSxR8I8HUAQDYV+2VJo3bA
ct9ubVjaw2SSiQZp9xB7BOJjk/NQrTk5gG3BkDI/Ukp9A9s7YoW1oMY8YdIg/YRo
Y+LI5trvXN73V2X0Ow==
-----END CERTIFICATE REQUEST-----


Secure>
```

Example 2: *This example demonstrates the use of the* ***SG*** *console command to generate a 2048-bit RSA public/private key pair and output a certificate signing request.*

```
Secure> SG <Return>
Please enter the Subject Information for the Certificate Request:

   Country Name (2 letter code) []: UK <Return>
   State or Province Name (full name) []: Greater London <Return>
   Locality Name (eg, city) []: London <Return>
   Organization Name (eg, company) []: Bank XYZ <Return>
   Organizational Unit Name (eg, section) []: Operations <Return>
   Common Name (e.g. server FQDN or YOUR name) []: HSM-0002
<Return>
   Email Address []: bill@bankxyz.com <Return>

Select key type:
  1 - RSA
  2 - ECDSA P-256
  3 - ECDSA P-384
  4 - ECDSA P-521
Type [4]: 1 <Return>

Generating key pair ......................+++
.......+++
DONE

Do you wish to save to a file [Y/N]: Y <Return>
Enter filename: HSM-0002 <Return>
-----BEGIN CERTIFICATE REQUEST-----
MIIC2TCCAcECAQAwgZMxCzAJBgNVBAYTAlVLMRcwFQYDVQQIEw5HcmVhdGVyIExv
bmRvbjEPMA0GA1UEBxMGTG9uZG9uMREwDwYDVQQKEwhCYW5rIFhZWjETMBEGA1UE
CxMKT3BlcmF0aW9uczERMA8GA1UEAxMISFNNLTAwMDIxHzAdBgkqhkiG9w0BCQEW
EGJpbGxAYmFua3h5ei5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQDBJAjJVtpE2Covk13BpZCACN6hUoQeLRv62+M3Lioa/ckvrIDaFxRTmlBGAof/
nZR3uRXSRz5oo3MX+fG4QXuLCGujFPHUfdnJRFIGnxoxkrrXn5OyxtokLwdE3HrK
VgKeUPQvDluZVXCbFJ1rGGaBk6bRQCfb7hBI7gcba6NfLIPms/bXYgy5hKUbkf+N
rMGtKAHz70E7BRMyY95GFo6nDne579rUi8RDxC4vqIJgkaXbuv4evYxlliTsQ69O
wr0iRSygYHSYzA8TVcwJ1pNTO1Jeg2xJ8r4axs0r5IKxxpD2PDAv4DdyQ0TsZkTB
QfSxPnlD4sTeQW5s42Y0B02ZAgMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEAJqPX
alHvtQKsfxgzTn2nWiw/v/9v8Qs11MIRJ5/Y3x+fdRSSK55uwPmRIRlCYdM0xQ4C
tSW3jWUiB1P0a3XxC5O4cWfbXJSxWkoSiN6V5gZrCI9W1z05xAuJZtjdVcFbUvVI
pPw3LXXS2CxAsAbgtz3QG+MIdyiicE5vUN2kKxhhZaC8Ev3tpy2Uue8XGy1sDybu
8qx5I5tMUSAsYx4M956gJEL0Mt9k8phIhsbKz5IKDDEwuyurJlYoOqkVVZeuBKZu
YKJKdOtwzzuUesEcGQfbAleBR0ntezm0irWJRaCXEyg0e5DF0FfWGIE08ojx4dvh
w3mX71ZX4RGchVEsYQ==
-----END CERTIFICATE REQUEST-----


Secure>
```

Import Certificate (SI)

Variant ☑		Key Block ☑
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **SI**

Function: To import a certificate for storage inside the HSM for use with secure host communications.
The certificate may be one of the following:

- HSM certificate
- Client certificate
- Sub-CA certificate (for either HSM or client)
- Root-CA certificate (for either HSM or client)

Authorization: The HSM must be in the secure state to run this command.

Inputs:

- File selection
- Prompt for import of additional certificates

Outputs:

- Prompts, as above
- Filenames of certificates on USB memory stick
- Summary of imported certificate (Issued to/by, Validity, ID)
- Chain of Trust statement (for an HSM certificate)

Notes:

- The HSM's public/private key pair must be installed (using the SG console command) prior to using this command.
- The file(s) to be imported must have the extension ".CRT".
- A maximum certificate chain length of 6 is supported.
- The required format for the USB memory stick is FAT32. The Operating System used in the payShield 10K supports most types of USB memory stick, 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.

Example 1: *This example demonstrates the use of the **SI** console command to import the root CA certificate (that signed the HSM's certificate) into the HSM.*

```
Secure> SI <Return>

Select File
   1 – HSM-0001.crt
   2 – BankXYZRootCA.crt
   3 - Client.crt
   4 - ClientRootCA.crt
File: 2 <Return>

Imported Trusted CA Certificate
         Issued to: Bank XYZ, Issued by: Bank XYZ
         Validity : May 9 10:59:22 2013 GMT to May 7 10:59:22
2023 GMT
         Unique ID: 9C8FC713FAA31010 - AC03FAD5 (Root)

Do you wish to import another certificate? N <Return>

Secure>
```

Example 2:

This example demonstrates the use of the ***SI*** *console command to import the HSM's (now signed) certificate back into the HSM.*
(Note that the root CA certificate has already been installed (see Example 1), and so the HSM indicates that the "Chain of Trust" is complete.

```
Secure> SI <Return>

Select File
   1 – HSM-0001.crt
   2 - BankXYZRootCA.crt
   3 - Client.crt
   4 - ClientRootCA.crt
File: 1 <Return>

Imported CA-signed HSM Certificate
         Issued to: HSM-0001, Issued by: Bank XYZ
         Validity : May 21 15:05:51 2013 GMT to May 21 15:05:51
2014 GMT
         Unique ID: 2050 - AC03FAD5

Chain of Trust validated
         Bank XYZ (Root)

Do you wish to import another certificate? N <Return>

Secure>
```

Export HSM Certificate's Chain of Trust (SE)

Variant ☑		Key Block ☑
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **SE**

Function: To export the HSM certificate's chain of trust (i.e. the chain of certificates required to authenticate the HSM's certificate, up to and including the root CA certificate).

Authorization: The HSM must be in the secure state to run this command.

Inputs:

- Filename when saving to USB memory stick

Outputs:

- Prompts, as above
- Prompt to save to USB memory stick
- Certificate Chain of Trust is displayed at the console, and (if requested) saved to the USB memory stick

Errors:

- File exists – replace?

Notes:

- The HSM's public/private key pair must be installed (using the SG console command) prior to using this command.
- The exported file will automatically have the extension ".CRT".
- A maximum certificate chain length of 6 is supported.
- The required format for the USB memory stick is FAT32. The Operating System used in the payShield 10K supports most types of USB memory stick, 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.

Example 1: *This example demonstrates the use of the **SE** console command to export the HSM certificate's chain of trust (in this case, just the root CA certificate) to a USB memory stick.*

```
Secure> SE <Return>

Do you wish to save to a file [Y/N]: Y <Return>
Enter filename: BankXYZRootCA <Return>

Bank XYZ

-----BEGIN CERTIFICATE-----
MIID+TCCAuGgAwIBAgIJAJyPxxP6oxAQMA0GCSqGSIb3DQEBBQUAMIGyMQswCQYD
VQQGEwJVSzEYMBYGA1UECBMPQnVja2luZ2hhbXNoaXJlMRUwEwYDVQQHEwxMb25n
IENyZW5kb24xDzANBgNVBAoTBlRoYWxlczEMMAoGA1UECxMDUE1HMR4wHAYDVQQD
ExVwYXlTaGllbGQgQ2VydGlmaWNhdGUxMzAxBgkqhkiG9w0BCQEWJGphbWVzLnRv
cmp1c3NlbkB0aGFsZXMtZXNlY3VyaXR5LmNvbTAeFw0xMzA1MDkxMDU5MjJaFw0y
MzA1MDcxMDU5MjJaMIGyMQswCQYDVQQGEwJVSzEYMBYGA1UECBMPQnVja2luZ2hh
bXNoaXJlMRUwEwYDVQQHEwxMb25nIENyZW5kb24xDzANBgNVBAoTBlRoYWxlczEM
MAoGA1UECxMDUE1HMR4wHAYDVQQDExVwYXlTaGllbGQgQ2VydGlmaWNhdGUxMzAx
BgkqhkiG9w0BCQEWJGphbWVzLnRvcmp1c3NlbkB0aGFsZXMtZXNlY3VyaXR5LmNv
bTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANTFR+dFeafMZsMwgeOK
vWxjmaUOP6z5mK+qeD4wYvNP5cv1GVqKoMFTNkJL+jeBSyo39IR0T4AoalroUb6F
yi76nmv0VVqFgPWIS92bRBozGp8dZU09aJQGCuOIjEvKuUtddWrpp0ClFEnTXXsx
LpfjTal5vSl+D9lazkMiFxdi7OUQyf6CiVuoch7bq0A4nmcjSlPyE/b3FpJn6zul
S+/DvRo4N4wJBHkZftAyPHZUYaV84perRG4CRbirFUfpRH1kVC+P6Gal/KMKWlzE
kKJOIxZqtaU973/AD4CV2QZtMurFC9m9p84uOW2SinMeKEdolVTFgVo+h3KjFHM/
yVsCAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAoHEN
1QyqWSTXkhtAnu+F3gy/Qs/wYLszaYYlBUSQasjN866SzRC/jVtYT6UYabvOke5B
9Z4KNsICkRtmgdYpic0kjK40RjUdw4QZu4jC+EM4eY8HTa7fSaH1nxrkPAEUwNKZ
o3Re+3jQeIx6gi5rnLf/FZ1cEP1fySh0hzuSo2xSIY/hwUWhlZJYZKBu3wzfHG1d
GB7D4xU4jUTvkKJQDuCHUdSrf+cMstN9dkrhYNNw49L9tYrD0ZzlPM3rVXD28uAL
Wt+CPOtsjIixNRl8vZmEVJDWJaRibCcfrTeDBs4O3hmAgx/Mdv5FX/NSjhZZO15m
X4FkYiQv2CJb7J/vAw==
-----END CERTIFICATE-----

Secure>
```

View Installed Certificate(s) (SV)

Variant ☑		Key Block ☑
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **SV**

Function: To view the list of currently installed certificates (for use with secure host communications). Individual certificates can be displayed in full.

Authorization: The HSM can be in any state to run this command.

Inputs:

- Certificate to be displayed in full.

Outputs:

- The HSM's public/private key pair must be installed (using the SG console command) prior to using this command.
- Prompts, as above
- List of currently installed certificates.
- Status of HSM's private key – installed or not installed
- HSM Certificate installed – maximum of 1 certificate
- Client Certificate(s) installed – maximum of 10 certificates
- CA Certificate(s) installed – maximum of 10 certificates
- Chain of trust validity – for the HSM's certificate chain
- Contents of selected certificate.
- A maximum certificate chain length of 6 is supported.

Example 1: *This example demonstrates the use of the **SV** console command to view the list of currently installed certificates, and to display the contents of the HSM's certificate.*

```
Secure> SV <Return>

HSM Private Key installed: Yes

HSM Certificate installed:
     1 - Issued to: HSM-0002, Issued by: Bank XYZ
         Validity : May 21 15:05:51 2013 GMT to May 21 15:05:51
2014 GMT
         Unique ID: 2050 - AC03FAD5

Client certificate(s) installed:
     2 - Issued to: APP-0001, Issued by: Applications
         Validity : May  7 09:37:18 2013 GMT to May  7 09:37:18
2014 GMT
         Unique ID: 2016 - D221289A

CA Certificate(s) installed:
     3 - Issued to: Applications, Issued by: Applications
         Validity : May  7 09:24:10 2013 GMT to May  5 09:24:10
2023 GMT
         Unique ID: C14FF9DE78FB441A - D221289A (Root)

     4 - Issued to: Bank XYZ, Issued by: Bank XYZ
         Validity : May  9 10:59:22 2013 GMT to May  7 10:59:22
2023 GMT
         Unique ID: 9C8FC713FAA31010 - AC03FAD5 (Root)

Chain of Trust validated:
         Bank XYZ (Root)

Select an item to view: 1 <Return>

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8273 (0x2051)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=UK, ST=Greater London, L=London, O=Bank XYZ,
OU=RootCA, CN=Bank XYZ/emailAddress=root@bankxyz.com
        Validity
            Not Before: May 21 15:05:51 2013 GMT
            Not After : May 21 15:05:51 2014 GMT
        Subject: C=UK, ST=Greater London, O=Bank XYZ,
OU=Operations, CN=HSM-0002/emailAddress=bill@bankxyz.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:aa:31:e6:90:46:fe:e9:26:8b:93:39:5a:8c:be:
                    …
                    3d:39:2b:d7:06:47:04:6a:54:d2:12:4e:ac:9a:a3:
                    5b:49
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key
Encipherment
    Signature Algorithm: sha1WithRSAEncryption
         b8:e9:e9:8f:2e:f9:50:93:a1:8b:8d:0b:e5:fd:ef:6f:6c:05:
         …
         59:0d:df:85:b7:48:c6:02:d9:16:f9:80:e5:c9:c2:69:7f:06:
         2b:ba:18:9f

Do you wish to view another certificate? N <Return>

Online>
```

Delete Installed Certificate(s) (SD)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **SD**

Function: To delete a currently installed certificate (for use with secure host communications).

Authorization: The HSM must be in the secure state to run this command.

Inputs:

- Certificate to be deleted.

Outputs:

- Prompts, as above
- List of currently installed certificates.
- Status of HSM's private key – installed or not installed
- HSM Certificate installed – maximum of 1 certificate
- Client Certificate(s) installed – maximum of 10 certificates
- CA Certificate(s) installed – maximum of 10 certificates
- Chain of trust validity – for the HSM's certificate chain
- Prompt to delete another certificate

Example 1: *This example demonstrates the use of the* ***SD*** *console command to remove a client certificate from the HSM.*

```
Secure> SD <Return>
HSM Private Key installed: Yes

HSM Certificate installed:
     1 - Issued to: HSM-0002, Issued by: Bank XYZ
         Validity : May 21 15:05:51 2013 GMT to May 21
15:05:51 2014 GMT
         Unique ID: 2050 - AC03FAD5

Client certificate(s) installed:
     2 - Issued to: APP-0001, Issued by: Applications
         Validity : May  7 09:37:18 2013 GMT to May  7
09:37:18 2014 GMT
         Unique ID: 2016 - D221289A

CA Certificate(s) installed:
     3 - Issued to: Applications, Issued by: Applications
         Validity : May  7 09:24:10 2013 GMT to May  5
09:24:10 2023 GMT
         Unique ID: C14FF9DE78FB441A - D221289A (Root)

     4 - Issued to: Bank XYZ, Issued by: Bank XYZ
         Validity : May  9 10:59:22 2013 GMT to May  7
10:59:22 2023 GMT
         Unique ID: 9C8FC713FAA31010 - AC03FAD5 (Root)

Chain of Trust validated:
         Bank XYZ (Root)

     5 – HSM Private Key

Select an item to delete (6 for ALL): 2 <Return>
Do you wish to delete another certificate? N <Return>
Secure>
```

Generate HRK (SK)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☒</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **SK**

Function: To generate a new HSM Recovery Key (HRK). Once installed, the HRK will be used to back-up secret key material inside the HSM into persistent memory (a process known as key synchronization).
The following secret key material is backed-up in this process:

- Secure Host Communications key material:
  - HSM's private key
- Remote Management key material:
  - HSM's private key
  - HSM's public key certificate
  - CA public key certificate

Authorization: The HSM must be in the secure state to run this command.

Inputs:

- Passphrases 1 & 2 (each entered twice for verification).

Outputs:

- Prompts, as above.
- Passphrase rules.
- Creating HRK message.
- Key synchronization message.

Notes:

- The HRK replaces the RMK (used in previous versions of software).

Example 1: *This example demonstrates the use of the* ***SK*** *console command to generate an HRK.*

```
Secure> SK <Return>

**** NOTE ****
Passphrase rules as follows:
1 - Must be between 8 and 30 characters long.
2 - Can contain spaces
3 - Must be comprised of (at a minimum):
   2 digits
   2 uppercase characters
   2 lowercase characters
   2 symbols (e.g. !/?.#:')

   Enter administrator 1 passphrase: ********************
Re-enter administrator 1 passphrase: ********************

   Enter administrator 2 passphrase: **************
Re-enter administrator 2 passphrase: **************

Creating HRK. Please, wait ... DONE

HRK generated successfully

Key synchronization complete
Secure>
```

Change HRK Passphrase (SP)

<table>
<tr><td colspan="3">Variant ☑</td><td colspan="3">Key Block ☑</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☒</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **SP**

Function: To change one of the passphrases associated with the HRK.

Authorization: The HSM must be in the secure state to run this command.

Inputs:

- Existing passphrase 1 or 2.
- New passphrase 1 or 2 (entered twice for verification).

Outputs:

- Prompts, as above.
- Passphrase rules.
- Creating HRK message.
- Key synchronization message.

Notes:

- The HRK replaces the RMK (used in previous versions of software).

Example 1: *This example demonstrates the use of the **SP** console command change administrator #1's HRK passphrase.*

```
Secure> SP <Return>

**** NOTE ****
Passphrase rules as follows:
1 - Must be between 8 and 30 characters long.
2 - Can contain spaces
3 - Must be comprised of (at a minimum):
   2 digits
   2 uppercase characters
   2 lowercase characters
   2 symbols (e.g. !/?.#:')
4 - Cannot use the same passphrase that was used within
the past 10 previous attempts

Select administrator password to change [1,2]: 1
   Enter administrator 1 current passphrase:
********************
   Enter administrator 1 new passphrase: ************
Re-enter administrator 1 new passphrase: ************


Changing passphrases. Please, wait ... DONE

HRK generated successfully

Secure>
```

Restore HRK (SL)

Variant ☑	Key Block ☑	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **SL**

Function: To restore the HRK (and also the secret key material backed-up by the HRK) in the event of erasure of tamper protected memory.

Authorization: The HSM must be in the secure state to run this command.

Inputs:

- Passphrases 1 & 2.

Outputs:

- Prompts, as above.
- Restoring HRK message.
- Key synchronization message.

Errors:

- HRK already loaded.

Notes:

- The HRK replaces the RMK (used in previous versions of software).

Example 1: *This example demonstrates the use of the **SL** console command to generate an HRK.*

```
Secure> SL <Return>

Enter administrator 1 passphrase: ********************
Enter administrator 2 passphrase: **************

Recovering HRK. Please, wait ... DONE

HRK recovered successfully

Key synchronization complete

Secure>
```

KMD Support Commands

This section describes the set of console commands that facilitate the operation of the Thales Key Management. Please note the Key Management Device (KMD) is now end of sale and has been replaced by the Trusted Management Device (TMD) – see Section 1.11 earlier in this document for further information.

This section describes the set of console commands that facilitate the operation of the Thales Key Management Device (KMD) in a PCI PIN compliant manner.

Command	Page
Generate KTK Components (KM)	**443**
Install KTK (KN)	**444**
View KTK Table (KT)	**445**
Import Key encrypted under KTK (KK)	**446**
Delete KTK (KD)	**447**

Generate KTK Components (KM)

<table>
<tr><td colspan="3">Variant ☐</td><td colspan="3">Key Block ☐</td></tr>
<tr><td colspan="2">Online ☒</td><td colspan="2">Offline ☒</td><td colspan="2">Secure ☑</td></tr>
<tr><td colspan="6">Authorization: <b>Not required</b></td></tr>
</table>

Command: **KM**

Function: To generate the components of a KMD Transport Key (KTK), and store the components on smartcards.

Authorization: None

Inputs:

- Number of components to generate
- Prompt for smartcards & PINs to be entered

Outputs:

- Check value of smartcards
- Check value of new KTK

Example 1: *This example demonstrates the use of the* ***KM*** *console command to generate two KTK components on smartcards.*

```
Secure> KM <Return>

Enter number of components [2-3]: 2 <Return>
Insert blank card and enter PIN: ****** <Return>
    Writing keys...
    Checking keys...
Device write complete, check: ZZZZZZ

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

    1 copies made
Insert blank card and enter PIN: ****** <Return>
    Writing keys...
    Checking keys...
Device write complete, check: ZZZZZZ

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

    1 copies made

KTK Check Value: ZZZZZZ

Secure>
```

Install KTK (KN)

Variant ☐	Key Block ☐	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **KN**

Function: To install a KMD Transport Key (KTK) into the HSM.

Authorization: None

Inputs:

- KTK Identifier: 2 numeric digits
- Number of components to use
- Prompt for smartcards & PINs to be entered

Outputs:

- Check value of smartcards
- Check value of new KTK

Example 1: *This example demonstrates the use of the **KN** console command to install a KTK in KTK Id 01, using two smartcards.*

```
Secure> KN <Return>
Enter KTK id [00-19]: 01 <Return>
Enter comments: KTK for KMD in secure room <Return>
KTK in selected location must be erased before
proceeding.
Erase KTK? [Y/N]: Y <Return>

Load KTK in components
Insert card and enter PIN: ****** <Return>
Check: ZZZZZZ
Load more components? [Y/N]: Y <Return>

Insert card and enter PIN: ****** <Return>
Check: ZZZZZZ
Load more components? [Y/N]: N <Return>

KTK check: ZZZZZZ
KTK id: 01
KTK key scheme: Variant
KTK algorithm: AES-256
Comments: KTK for KMD in secure room

Confirm details? [Y/N]: Y <Return>

Secure>
```

View KTK Table (KT)

Variant □	Key Block □	
Online ☑	Offline ☑	Secure ☑
Authorization: **Not required**		

Command: **KT**

Function: To display the KTK table.

Authorization: None

Inputs:

- None

Outputs:

- List of installed KTKs

Example 1: *This example demonstrates the use of the **KT** console command to display the list of all KTKs currently installed in the HSM.*

```
Online> KT <Return>

KTK table:
ID Scheme   Algorithm   Check   Comments
01 Variant  3DES(2key)  292489  KTK for KMD in secure
room
03 Variant  3DES(2key)  549235  KTK for 2nd KMD

Online>
```

Import Key encrypted under KTK (KK)

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

Command: **KK**

Function: To translate a key from encryption under a KTK to encryption under an LMK.

Authorization: The HSM must either be in the Authorized State, or the activity **command.kk.console** must be authorized.

Inputs:

- LMK Identifier
- Key Type Code
- Key Scheme (LMK)
- KTK Identifier
- Key encrypted under KTK

Outputs:

- Key encrypted under LMK

Example 1: *This example demonstrates the use of the **KK** console command to import a double-length DES ZMK (key type 000) from encryption under KTK Id 01 to encryption under LMK Id 02.*

```
Online-AUTH> KK <Return>

Enter LMK id: 02 <Return>
Enter Key type: 000 <Return>
Enter Key Scheme (LMK): U <Return>

Enter KTK id: 01 <Return>
Enter key: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
<Return>

LMK encrypted key: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY
YYYY
Key check value: ZZZZZZ

Online-AUTH>
```

Delete KTK (KD)

Variant ☐	Key Block ☐	
Online ☒	Offline ☒	Secure ☑
Authorization: **Not required**		

Command: **KD**

Function: To delete a selected KTK from the HSM.

Authorization: None

Inputs:

- KTK Identifier

Outputs:

- Display of relevant entry from KTK table.

Example 1: *This example demonstrates the use of the **KD** console command to delete a previously installed KTK (KTK Id 01) from the HSM.*

```
Secure> KD <Return>
Enter KTK id: 01 <Return>

KTK table entry:
ID Scheme   Algorithm   Check   Comments
01 Variant  3DES(2key)  292489  KTK for KMD in secure
room

Confirm KTK deletion [Y/N]: Y <Return>
KTK deleted from main memory

Secure>
```

Error Responses Excluded from Audit Log

If the option to Audit Error Responses to Host Commands is selected using AUDITOPTIONS, those errors which may require attention by the HSM Administrators or Security Officers are logged. The following non-00 error responses are not included in the Audit Log:

	Not Audited if error response is:		
Cmnd	01	02	43
A6	X		
BC	X		
BE	X		
BK		X	
BY	X		
CG	X		
CK	X	X	
CM	X		
CO	X		
CQ	X		
CU	X		
DA	X	X	
DC	X		
DE		X	
DU	X	X	
EA	X	X	
EC	X		
EE		X	
EG	X		
EI			X
F0	X		
F2	X		
FA	X		
FU	X		
G2	X		
G4	X		
GO	X		
GQ	X		
GS	X		
GU	X		
J0			X
K2	X		
KE			X
KO			X
P0	X		
PG	X		
PY	X		
QQ	X		
QS	X		
QU	X		
QW	X		
XM	X		
XK	X		
ZU	X		

Appendix B - Configuring Ports Using the Console

This chapter describes how to physically configure the payShield HSM to work with the Host system via console commands.

Note: Host commands are disabled by default.

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

When entering sensitive (clear text) data, use the inhibit echo back facility to ensure that the HSM does not echo the data to the console screen. This is set at configuration using the CS (Configure Security) command.

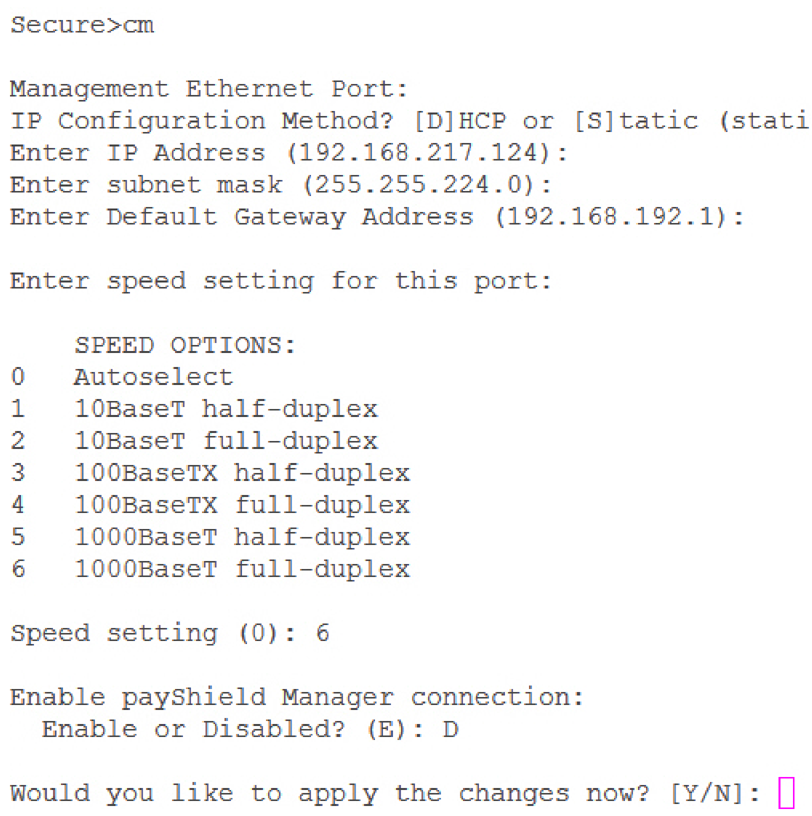
Instead of displaying the data, the HSM displays a star for each character entered.

Note: New values take effect immediately after the command has completed. To exit out of any command simultaneously press: **<Control> C**. The system responds with: **Terminated**.

B.1 Configure the Management Port

The Management port is an Ethernet port that is used only for managing the HSM. It cannot be used to process host commands.

An example of the CM command follows.



```
Secure>cm

Management Ethernet Port:
IP Configuration Method? [D]HCP or [S]tatic (static):
Enter IP Address (192.168.217.124):
Enter subnet mask (255.255.224.0):
Enter Default Gateway Address (192.168.192.1):

Enter speed setting for this port:

    SPEED OPTIONS:
0   Autoselect
1   10BaseT half-duplex
2   10BaseT full-duplex
3   100BaseTX half-duplex
4   100BaseTX full-duplex
5   1000BaseT half-duplex
6   1000BaseT full-duplex

Speed setting (0): 6

Enable payShield Manager connection:
  Enable or Disabled? (E): D

Would you like to apply the changes now? [Y/N]:
```

Where a firewall is used to protect the network link to the Management port, the following ports should be opened as appropriate:

Table 7 Port settings with Firewall

Port	Protocol	Purpose
20	TCP	FTP (for software and license updates)
21	TCP	FTP (for software and license updates)
161	UDP	SNMP Requests - Utilization and Health Check data
162	UDP	SNMP traps
5002	UDP	sysid
5003	UDP	Software update management
80 443	TCP	payShield Manager

It is recommended that the Management Ethernet port and Host Ethernet port(s) have independent IP subnets.

B.2 Configure the Printer Port

The payShield 10K is compatible with several types of printers:

- a serial printer (connected via a USB-to-serial converter cable),
- a parallel printer (connected via a USB-to-parallel converter cable),
- or a native-USB printer.

Configuring the port is accomplished via entering the console command CP.

Note: Follow this link for additional instruction: Appendix , “Console Commands”

B.3 Configure the Host Ports

The payShield HSM Host interfaces can be configured using the Console to emulate a number of types of data communications equipment and control equipment. At the end of the configuration, the user is given the option to save the host interface settings to a smart card.

B.3.1 Configuring the Software

Prerequisites:

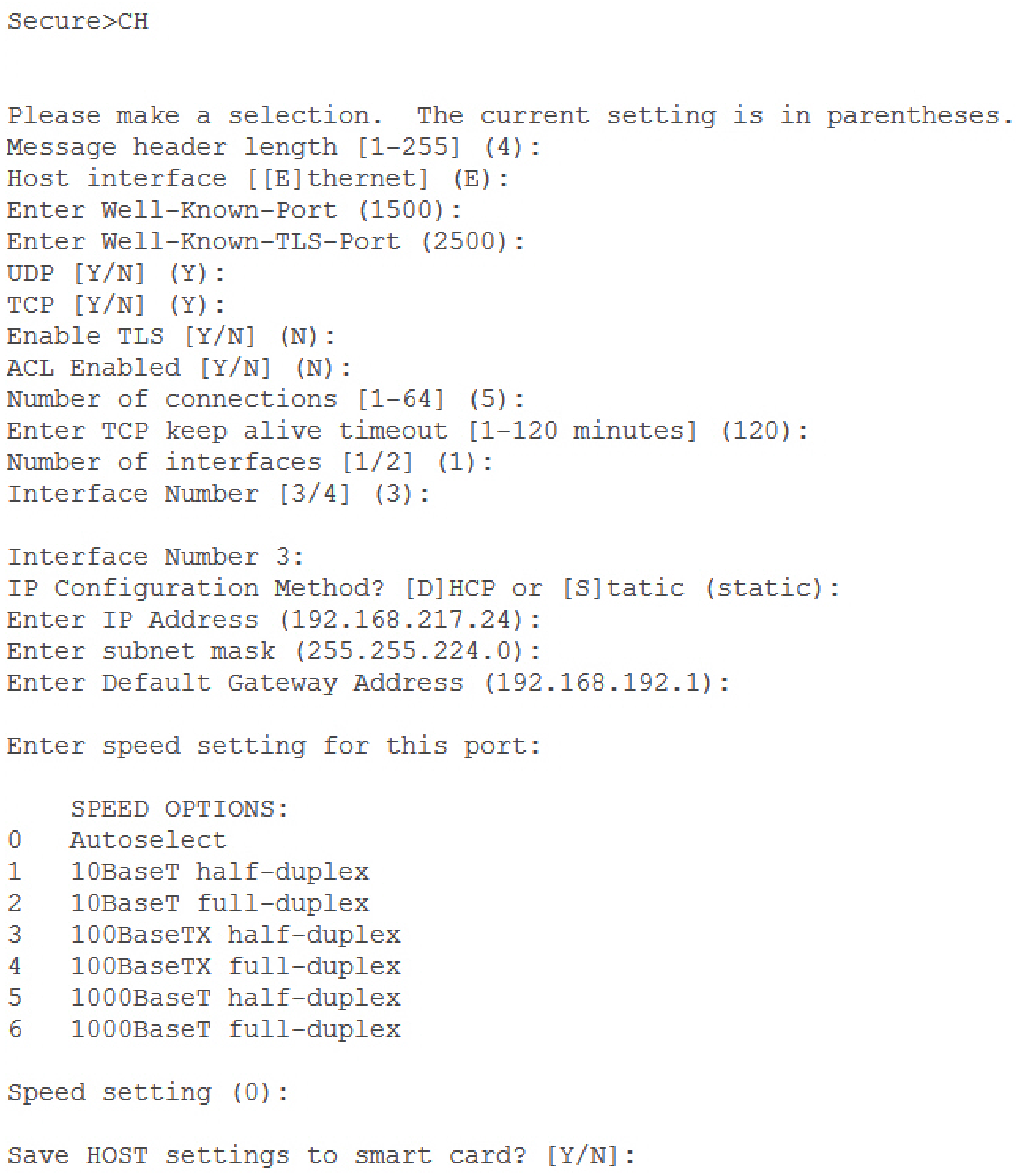
- The HSM is in either the secure state or the offline state
- Power applied
- Console terminal connected

Host ports are configured via the console command CH.

Note: Follow this link for additional instruction: Appendix , “Console Commands”

For quick reference purposes, see example below.

Note: In this example, the HSM is in the Secure state.



```
Secure>CH


Please make a selection.  The current setting is in parentheses.
Message header length [1-255] (4):
Host interface [[E]thernet] (E):
Enter Well-Known-Port (1500):
Enter Well-Known-TLS-Port (2500):
UDP [Y/N] (Y):
TCP [Y/N] (Y):
Enable TLS [Y/N] (N):
ACL Enabled [Y/N] (N):
Number of connections [1-64] (5):
Enter TCP keep alive timeout [1-120 minutes] (120):
Number of interfaces [1/2] (1):
Interface Number [3/4] (3):

Interface Number 3:
IP Configuration Method? [D]HCP or [S]tatic (static):
Enter IP Address (192.168.217.24):
Enter subnet mask (255.255.224.0):
Enter Default Gateway Address (192.168.192.1):

Enter speed setting for this port:

    SPEED OPTIONS:
0   Autoselect
1   10BaseT half-duplex
2   10BaseT full-duplex
3   100BaseTX half-duplex
4   100BaseTX full-duplex
5   1000BaseT half-duplex
6   1000BaseT full-duplex

Speed setting (0):

Save HOST settings to smart card? [Y/N]:
```

B.3.1.1 Message Header Length

Each transaction to the HSM begins with a string of characters (header) which the Host can use to identify the transaction (or for any other purpose). The HSM returns the string unchanged to the Host in the response message. The length of the header can be set to any value between 1 and 255; the default value is 4.

B.3.1.2 Ethernet Communications

The payShield Host port provides two auto-sensing Ethernet interfaces, which support 10 base-T, 100 base-TX or 1000 base-T.

The payShield provides network resiliency by supporting two independent network paths between the Host computer and HSM. In order to take advantage of this feature, the two HSM Host interfaces must be connected to two independent interfaces at the Host computer.

B.3.1.3 Software Parameters

There are a number of prompts for configuring the software:

- The message header length
- The availability of a UDP port
- The availability and number of TCP ports. The number of TCP/IP sockets available has a maximum of 64.
- The Keep-Alive timer, which enables TCP to periodically check whether the other end of a connection is still open. This enables the HSM to free resources by closing any unused connections.
- The Well-Known-Port address, which is the published TCP port address of the HSM, in the range 0000010 to 6553510 representing an address in the range 000016 to FFFF16.
- The IP address for each of the host ports, i.e. the Internet Protocol addresses of the unit's host ports in the system. The addresses are four decimal numbers, each not exceeding 255.
- The subnet mask for each host port, used to define the network class. This is four decimal numbers, each not exceeding 255. It is recommended that the Ethernet ports on the HSM are on different subnets from each other.
- The default gateway for each host port, used to define the IP address to which off-subnet traffic is to be sent to for onward routing. This is four decimal numbers, each not exceeding 255.

Note: The payShield HSM automatically detects whether an incoming command message uses ASCII or EBCDIC characters, and processes the command accordingly, returning the result in the same format.

To query the current configuration, use command **QH**. Example follows:

Note: In this example, the unit is in the Offline state.

```
Offline>QH


Message header length: 04
Protocol: Ethernet
Well-Known-Port: 01500
Transport: UDP and TCP, 64 connections
TCP Keep_Alive value (minutes): 120 minutes
Number of interfaces: (2)

Interface Number: 1
IP address: 192.168.200.036
Subnet mask: 255.255.255.000
Default Gateway: 192.168.200.1
Port speed:  Ethernet autoClick (1000baseT full-duplex)

Interface Number: 2
IP address: 192.168.202.110
Subnet mask: 255.255.255.000
Default Gateway: 192.168.202.1
Port speed:  Ethernet autoClick (1000baseT full-duplex)


Offline>
```

Where a firewall is used to protect the network link to the host port, the following ports should be opened as appropriate:

Table 8 Port Settings

Port	Protocol	Purpose
161	UDP	SNMP Requests - Utilization and Health Check data
162	UDP	SNMP Traps.
xxxx	TCP/UDP	Well-known port for command traffic between host and payShield, as defined in host port parameters. Default is 1500. Use of this port results in the default LMK being used unless the command explicitly identifies another LMK.
xxxx + n	TCP/UDP	Well-known port for command traffic between host and payShield where LMK n-1 is to be used. For example, if the default well-known port has been defined as 1500, then 1501 is used if LMK 0 is required for the command, 1502 is used if LMK 1 is required for the command, and so on. An explicit identification of the LMK in the command overrides the LMK implied by the port number.
9100	UDP	Postscript printing. (Only applicable to some customized software versions.)

It is recommended that the Management Ethernet port and Host Ethernet ports are all on different IP subnets.

Appendix C - Commission payShield Manager using Console Commands

This chapter describes how to commission a payShield 10K using console commands.

payShield Manager for payShield 10K is usually commissioned remotely. However if for any reason the payShield 10K is no longer warranted, the Console can be used to set up payShield Manager as described in this section.

C.1 Background information

The payShield relies on a trust model with 2 parallel key hierarchies consisting of key material and signed certificates installed at the Thales factory (the Pre-placed Trust) and key material and signed certificates locally or remotely installed by the customer (i.e., the Customer Trust Authority or CTA).

Key management material on an HSM can be in one of two states:

- Warranted
  - The payShield only has the Pre-placed Trust. This is the factory default state. A unit will return to this state upon tamper.
- Commissioned
  - The payShield has Customer Trust (i.e., the customer has placed trust elements on the HSM).

The Pre-placed Trust is only used to facilitate the secure, authenticated loading of Customer Trust in a remote environment. Once Customer Trust is installed in an HSM, it is considered Commissioned and management operations can be used.

Follow the steps in the following checklist to ready the payShield for use.

Table 9 Installation Checklist

Step	Tasks
1.	Secure the HSM
2.	Generate a Customer Trust Authority
3.	Create the HRK passphrases
4.	Commission the HSM
5.	Commission Smart Cards
6.	Migrate LMK Cards to become RLMK Cards

C.2 Prerequisites

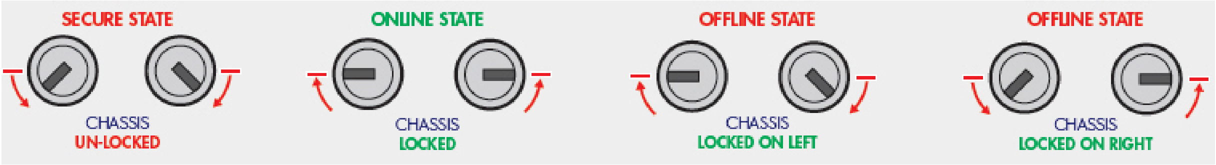
- The Remote payShield Manager license (i.e., PS10-LIC-RMGT) is installed.
- A payShield HSM is connected via the Management Port to a secure WAN.
- You are using DHCP to connect and you know the IP address of the HSM.
- A laptop/desktop PC with access to an Internet browser, e.g., Chrome, Internet Explorer, Firefox.
- A sufficient number (to meet the requirements established in your organization's security policies) of payShield Manager smart cards formatted for LMK type cards.
- The trusted officers, that will hold the shares in the Customer Trust Authority, are present.

C.3 Procedure

All commands are entered via the console terminal.

C.3.1 Secure the HSM

1. Place the HSM in the Secure state.
   - Place the keys in the locks located on the front of the unit.
   - Turn the keys to the locked position.



C.3.2 Generate a Customer Trust Authority

The XI console command generates the Customer Trust Authority. The shares are then stored on the smart cards.

Note: The presence of the trusted officers is required.

1. Place the HSM in the Secure state.
   - Place the keys in the locks located on the front of the unit.
   - Turn the keys to the locked position.
2. At the prompt, enter **XI** and press **ENTER**.

```
Secure> XI <ENTER>
```

Follow the prompts and enter appropriately.

```
Secure> XI <Return>
Please enter the certificate Subject information:
Country Name (2 letter code) [US]: US <Return>
State or Province Name (full name) []: Florida <Return>
Locality Name (eg, city) []: Plantation <Return>
Organization Name (eg, company) []: Thales <Return>
Organizational Unit Name (eg, section) []: Production <Return>
Common Name (e.g. server FQDN or YOUR name) [CTA]: CTA <Return>
Email Address []: info@thalesesec.com <Return>
Enter number of Customer Trust Authority private key shares [3-9]: 3
<Return>
Enter number of shares to recover the Customer Trust Authority private
key [3-3]: 3 <Return>
Issued to: CTA, Issued by: CTA
Validity : Jan 9 10:28:49 2015 GMT to Jan 3 10:28:49 2040 GMT
Unique ID: EE3CB7CE8343B464CC04278188CF7EB3 - 3DE05514 (Root)
Insert payShield Manager Smart Card 1 of 3 and press ENTER: <Return>
Enter new PIN for smart card: ****** <Return>
Re-enter new PIN: ****** <Return>
Working....
CTA share written to smart card.
Insert payShield Manager Smart Card 2 of 3 and press ENTER: <Return>
Enter new PIN for smart card: ****** <Return>
Re-enter new PIN: ****** <Return>
Working....
CTA share written to smart card.
Insert payShield Manager Smart Card 3 of 3 and press ENTER: <Return>
Enter new PIN for smart card: ****** <Return>
Re-enter new PIN: ****** <Return>
Working....
CTA share written to smart card.
Successfully generated a Customer Trust Authority
Secure>
```

Notes:

- The Country, State, Locality, Organization, Common Name, and Email parameter values are those that are included in the X.509 certificate corresponding to the CTA. The Common Name is the only required parameter and it should concisely describe the security domain.
- Enter the number of Customer Trust Authority private key shares you wish to create.

  This is the number of smart cards onto which the CTA shares will be distributed.

  Valid values are: 3-9.
- Enter the number of shares to recover the Customer Trust Authority private key.

  This is the number of smart cards holding CTA shares that must be present in order to reassemble a CTA to perform various operations (including commissioning a payShield).

  The minimum value is: 3.

The payShield will display information regarding the Customer Trust Authority that was just created and prompt you to store the CTA components onto smart cards.

```
Issued to: Group1, Issued by: Group1
Validity : Apr  9 07:02:16 2015 GMT to Apr  2 07:02:16 2040 GMT
Unique ID: B07EA9A049325E02BF84B48A3644CCC3 - 702788CA (Root)
Insert payShield Manager Smart Card 1 of 3 and press ENTER:
```

- Follow the on-screen directions:
  - One by one, place a smart card into the integrated reader of the HSM.
  - Each officer should create a PIN and the HSM will write a share of the CTA to the smart card.

  Note: If the smart cards were previously commissioned, it will prompt you for the current PIN.

Upon completion, the following message displays:

```
Successfully generated a Customer Trust Authority
```

C.3.3 Create the HRK passphrases

The SK console command generates a new HSM Recovery Key (HRK). Once installed, the HRK is used to back-up secret key material inside the HSM into persistent memory. This back-up process is known as “key synchronization”.

This process backs up the following secret key material:

- Secure Host Communications key material:
  - HSM’s private key
- Remote Management key material:
  - HSM’s private key
  - HSM’s public key certificate

- CA public key certificate

The HMK is used to encrypt the HSM's private key. The HSM uses the HSM's private key when establishing the TLS/SSL session.

1. At the prompt, enter **SK** and press **ENTER**.

```
Secure> SK <ENTER>
```

Example:

```
Secure> SK <Return>
**** NOTE ****
Passphrase rules as follows:
1 - Must be between 8 and 30 characters long.
2 - Can contain spaces
3 - Must be comprised of (at a minimum):
2 digits
2 uppercase characters
2 lowercase characters
2 symbols (e.g. !/?.#:')
Enter administrator 1 passphrase: ********************
Re-enter administrator 1 passphrase: ********************
Enter administrator 2 passphrase: **************
Re-enter administrator 2 passphrase: **************
Creating HRK. Please, wait ... DONE
Successfully generated an HRK
Secure>
```

Notes:

- When prompted, create two passphrases.

  Passphrases require the following:

  - At least 2 upper case characters (e.g., AA)
  - At least 2 lower case characters (e.g., aa)
  - At least 2 numbers (e.g., 11)
  - At least 2 special characters (e.g., !!)

  You will enter both passphrases twice. Upon completion, the unit will set the HMK passphrase.

  The first time the unit is turned on, the HRK is generated with default passphrases. The passphrase can be the same among one or more payShields based upon your organization's security policy.

C.3.4 Commission the HSM

The XH console command commissions the factory warranted HSM.

Note: The presence of two trusted officers is required along with the following:

- The Customer Trust Authority smart cards (i.e., the CTA cards that you just created)

- Two payShield Manager smart cards (different than the CTA shares)

Note: These smart cards will be used as the Left and Right RACCs that replace both the physical keys on the front panel and the trusted officers. The cards can be key RACCs used for other HSMs in the same security domain.

The same Left and/or Right RACCs can be used in several payShields.

Note: Trust equates to access. You need the CTA cards to obtain access and then you use the other cards to change the lock state of the HSM.

1. At the prompt, enter **XH** and press **ENTER**.

   ```
   Secure> XH <ENTER>
   ```

   One by one, insert and assign a PIN for each smart card.

   The HSM creates the CTA private key.

Example:

```
Secure> XH <Return>
Please have all Customer Trust Authority (CTA) payShield Manager smart
cards available
Insert first CTA payShield Manager Smart Card and press ENTER: <Return>
Enter PIN: ****** <Return>
Insert CTA payShield Manager Smart Card 2 of 3 and press ENTER: <Return>
Enter PIN: ****** <Return>
Insert CTA payShield Manager Smart Card 3 of 3 and press ENTER: <Return>
Enter PIN: ****** <Return>
Starting the commissioning of the HSM process...
Please insert left key card and press ENTER: <Return>
Enter PIN: ****** <Return>
Please insert right key card and press ENTER: <Return>
Enter PIN: ****** <Return>
Successfully commissioned HSM
Secure>
```

Notes:

- Insert the left smart card and press **ENTER**.

  This card becomes the left RACC.

- Insert the right smart card and press **ENTER**.

  This card becomes the right RACC.

  These are used to access the payShield after completing the commissioning procedure. These also replace the physical keys that put the payShield into the **Offline** or **Secure** state.
  If the smart card has been previously commissioned with a different CTA (security domain), the system will query for confirmation prior to proceeding to erase and reprogram with the current CTA.

  Upon completion, the following message displays:

  ```
  Successfully commissioned HSM.
  ```

  payShield Manager can now provide remote access to the HSM.

C.3.5 Commission Smart Cards

Note: All cards used remotely must be commissioned prior to use. This includes the following:

- RLMK cards
- Authorizing Officer cards
- Restricted cards
- Administrator cards (both Right and Left cards)

1. From the payShield Manager landing page, Click **Login**.
2. Follow this link to continue: Section 8.9.2.1, “Commission a Smart Card”, on page 147.

   Note: A link is provided to return you to the section below.

C.3.6 Migrate LMK Cards to become RLMK Cards

The XT console command transfers an existing HSM LMK stored on legacy Thales smart cards to payShield Manager RLMK cards for use through the payShield Manager.

In order to transfer a Variant LMK you will be required to fully reassemble the LMK (bring all the components together). Then, the fully formed Variant LMK is split among shares onto the pre-commissioned payShield Manager RLMK cards.

For Key Block LMKs, they are not stored as components on non-payShield Manager smart cards, but as shares. However, you must bring a quorum of share holders together, reconstitute the LMK, and then split it among shares onto the pre-commissioned payShield Manager RLMK cards.

1. At the prompt, enter **XT** and press **ENTER**.

   Follow the prompts and enter appropriately.

Example:

```
Secure> XT <Return>
Please have all the local LMK components and enough commissioned RACCs
to receive the LMK ready.
Insert card and press ENTER: <Return>
Enter PIN: ***** <Return>
Check: 268604
Load more components? [Y/N]: N <Return>
LMK Check: 268604
LMK key scheme: Variant
LMK algorithm: 3DES(2key)
LMK status: Test
Is this the LMK you wish to transfer? [Y/N]: Y <Return>
Enter the number of shares to split the LMK into: [2-9]: 2 <Return>
The number of shares required to reconstitute the LMK is fixed for
variants: 2 <Return>
Insert a commissioned card 1 of 2 and press ENTER: <Return>
Enter PIN: ****** <Return>
Card Check: E0CBF4
LMK share written to smart card.
Insert a commissioned card 2 of 2 and press ENTER: <Return>
Enter PIN: ****** <Return>
Card Check: E0CBF4
LMK share written to smart card.
Want to test the reassembly of the LMK? Y <Return>
Please have all the RLMK shares ready
Insert RLMK card and press ENTER: <Return>
Enter PIN: ****** <Return>
```

Appendix D - 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

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <