payShield 9000 Security Policy

Product Version Details:

Hardware Versions:

Part Name	Hardware Version
payShield 9000 (Single PSU)	1600A466.01.X.X.X.X.X.X, 1600A466.04.X.X.X.X.X.X, 1600A466.05.X.X.X.X.X.X
payShield 9000 (Dual PSUs)	1600B466.01.X.X.X.X.X.X, 1600B466.04.X.X.X.X.X.X, 1600B466.05.X.X.X.X.X.X
payShield 9000 with FICON support (Dual PSUs)	1600D466.04.X.X.X.X.X.X, 1600D466.05.X.X.X.X.X.X

Firmware Versions:

Part Name	Firmware Version
Version 1.2a (no FICON support)	1317-1900
Version 2.1c	1346-1905
Version 2.3c	1346-1914

Thales e-Security
Meadow View House
Crendon Industrial Estate
Long Crendon
AYLESBURY
HP18 9EQ
United Kingdom

Tel: +44 (0)1844 201800
Fax: +44 (0)1844 208550

PCI HSM Non-proprietary Security Policy

Contents

Figures

Tables

1. Abbreviations

CA	Certificate Authority
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standard
FIPS 140-2	FIPS PUB 140-2 (Ref: FIPS 140-2)
HSM	Hardware Security Module
PCB	Printed Circuit Board
TSPP	Thales Secure Processing Platform

2. Reference documents

1 Payment Card Industry (PCI) Hardware Security Module (HSM) Security Requirements Version 1.0

2 Payment Card Industry (PCI) Hardware Security Module (HSM) Derived Test Requirements Version 1.0

3 Payment Card Industry (PCI) Hardware Security Module (HSM) Evaluation Vendor Questionnaire Version 1.0

4 ASEC0942 TSPP Security Policy

5 1270A350 payShield 9000 Security Operations Manual

6 1270A544 payShield 9000 Console Reference Manual

7 1270A546 payShield 9000 Host Command Reference Manual

8 1270A543 payShield 9000 Installation Manual

9 1270A536 payShield 9000 Local HSM Manager – User's Guide

10 1270A529 Remote HSM Manager – User's Guide

3. Introduction

The payShield 9000 is a Thales e-Security (Thales) Hardware Security Module (HSM) designed to secure card payment and issuance systems. This secure module has a 2U high chassis designed for rack mounting in a secure datacentre. A variety of physical and logical security protection mechanisms are incorporated into the payShield 9000 including but not limited to, e.g.: tamper evident labels, tamper resistant switches, rack-mounting locks, secure separation between logical interfaces and NIST-approved cryptographic algorithms, modes and key sizes.

This document aims to provide an overarching summary for security-related information pertaining to the payShield 9000. It will specify the underlying techniques designed to provide security within the product; and it then proceeds to describe how the various management interfaces implement those techniques.

Figure 1 payShield 9000

Protected within the payShield 9000 is a TSPP module which is a FIPS 140-2 Level 3 approved multi-chip embedded cryptographic module.

The TSPP module protects the security sensitive circuitry on its printed circuit board (PCB). The TSPP stores all the unit's critical security parameters (CSPs) as well as performing all of its cryptographic operations; and it also controls and protects the firmware that runs on the payShield 9000. For further information on the TSPP security functions refer to the TSPP security policy [ref. 4].

Circuitry outside the TSPP performs no sensitive operations, and mainly consists of power supplies and interfacing electronics.

4. HSM Management Interfaces

The payShield 9000 can be managed via three different interfacing devices: the Console, the Local HSM Manager, or the Remote HSM Manager (dependent on the license installed).

4.1 Console Interface

The Console interface enables the payShield 9000 to be managed locally via a terminal directly connected to the HSM using a serial interface. The serial data cable connects to the HSM via a serial-to-USB adapter. The interface was originally designed to be operated via a dumb terminal. However old-style dumb terminals are increasingly scarce, and users are transitioning to newer, intelligent terminals – with their greater potential for introducing security vulnerabilities. This drove the introduction of the Local and Remote HSM Managers to protect against these vulnerabilities whilst utilising the newer technologies available and to provide a modern user interface.

Despite the local nature and direct connection of the Console interface the user should ensure that they are communicating with the intended HSM and that they are protected against man-in-the-middle attacks. For information on the procedural security required refer to the payShield 9000 Security Operations Manual [5].

4.2 Local HSM Manager Interface

The Local HSM Manager enables the payShield 9000 to be managed locally via a PC directly connected to the HSM using an Ethernet interface; and it utilizes a user-friendly menu-driven interface.

To guard against vulnerabilities that could be encountered when connecting to the payShield 9000 from a potentially insecure environment, the Local HSM Manager operates within an immutable, functionality-restricted Linux boot environment provided on a self-booting CD. This enables the Local HSM Manager to run without ever having to access the PC's internal hard disks.

The security of the connection between the payShield 9000 and the PC is based upon a pre-placed secret for authentication, plus a secret cryptographic key – derived uniquely per connection using random data produced by the payShield 9000. The pre-placed secret (i.e. a password) is configured within the payShield 9000 using a command via the Console interface; and this password is then required to connect to the HSM via the Local HSM Manager.

Despite the local nature and direct connection of the Local HSM Manager interface the user should ensure that they are communicating with the intended HSM, and that they are protected against man-in-the-middle attacks. For information on the procedural security required refer to the payShield 9000 Security Operations Manual [5].

4.3 Remote HSM Manager Interface

The Remote HSM Manager enables the payShield 9000 to be managed remotely via a PC and a

set of three smartcard readers (used to replicate the smartcard reader and physical locks on the payShield 9000), and connected to the HSM using an Ethernet interface. The Remote HSM Manager builds upon the Local HSM Manager but provides the extra protection required to operate securely over a distributed network.

When installing the Remote HSM Manager a CA must be established as a Security Domain. A Security Domain is made up of:

- Any number of HSMs (any combination of HSM 8000s or payShield 9000s).
- Administrators, working via the Remote Manager software; each of whom has their own administrator smartcard.
- Operators, working via the Remote Manager software; each of whom has their own operator smartcard.

A CA cardset must be created. This CA forms the basis of authenticated communication between the Remote HSM Manager and the HSM(s). The CA cardset can be created using an HSM in its Secure operating mode. Each CA card protects an RSA private key with a modulus length between 1024 bits and the recommended 2048bits. The CA cardset's RSA public key is embedded within a self-signed certificate. The hash algorithm used by the cardset is determined by the policy defined in the CA at creation time – either SHA-1 or the recommended SHA-256.

The CA cardset is a group of PIN protected smartcards; and a share of the private key is stored on each card via a (k, n)-threshold scheme. A threshold scheme (also known as a "secret sharing scheme") is a mechanism that allows a "secret" to be broken into "shares", so that the secret can be recovered provided a defined number of shares are available, yet no information about the secret can be obtained if fewer than the required number of shares are presented. In the case of the Remote HSM Manager the CA private key is broken into n shares, and can be recovered provided k shares are presented. The only restrictions on the values of the parameters 'k' and 'n' that are enforced by the payShield 9000 are that $3 \leq k \leq n \leq 9$. The people responsible for the CA private key shares are called "shareholders".

Each entity within the Security Domain (HSMs and smartcards) must possess an RSA key pair, the size of which is determined by policies defined when the CA was created. The public key is held in the form of a certificate signed by the CA's private key. The hash algorithm used is as defined by the CA policies. The CA public key, in the form of its self-signed certificate, is also loaded into each HSM and smartcard. These certificates enable the HSMs and smartcards that form the Security Domain to identify and authenticate themselves to one another.

Another concept introduced by the Remote HSM Manager, that is built upon the Security Domain but with greater granularity, is the Security Group. The Security Group controls which Administrators and Operators can access an individual HSM within the Security Domain. To initialise a Security Group, one 'left' and one 'right' administrator smartcard holder must simultaneously present their cards to the HSM. The smartcards and HSM authenticate one another's certificates, and exchange identification information. From this point onwards these administrators control access to that particular HSM in the following manner:

- 'Right' administrators can only be added by another 'right' administrator.
- 'Left' administrators can only be added by another 'left' administrator.
- Operator smartcards can be added by either type of administrator.

5. Ports and Interfaces

The payShield 9000 has a variety of different physical ports which can be seen in Table 5-1*Table 5-1*.

There are two variants of the payShield 9000. One variant comes with dual power supplies, to enhance resiliency (1600B467), and the other variant comes with a single power supply (1600A467).

Table 5-1 Ports and Interfaces Description

Physical Port	Qty	Logical interface definition	Technical Specification
USB	6	Data input Data output Status output Control input	Can be used to connect the HSM to a standard console terminal via a USB-to-9 pin lead. An asynchronous serial connection to the host computer can also be connected via a USB-to-9 pin lead. Can also be used to connect to a printer.
Smartcard	1 or 4	Data input Data output	ISO card compliant smartcard reader with automatic card ejection on the payShield 9000 front panel.
Ethernet	4	Data input Data output Status output Control input	RJ45 sockets comprising: one management port, two host ports and one auxiliary port. Note: the auxiliary Ethernet port is not currently in use.
Power	1 or 2	Power	Single or dual IEC style power sockets and 20nm fuse holders. Each power unit requires 100/240 Volts AC.

5.1 Front Panel LEDs

The payShield 9000 has eight LEDs on its front panel.

Table 5-2 identifies the purpose of each LED.

Table 5-2 LED Function

LED	Single PSU Description	Dual PSU Description
Power LED	Indicates the condition of the power supply. • An unlit LED indicates that power is not being supplied. • A solid green LED indicates that the power is being supplied.	Indicates the condition of the power supply. • An unlit LED indicates that power is not being supplied through either socket. • A solid red LED indicates power is only being supplied through the upper socket. • A solid yellow LED indicates power is only being supplied through the lower socket. • A solid green LED indicates that power is being supplied through both sockets.
Error LED	Indicates the condition of the error log: • An unlit LED indicates there are no errors recorded in the error log. • A flashing LED indicates a new error has occurred since the error log was last checked. • A solid LED indicates that the error log contains errors which have been investigated.	
LMK LED	Indicates whether an LMK is installed in the HSM: • An unlit LED indicates no LMKs are installed. • A solid green LED indicates one or more LMKs are installed.	
Alarm LED	Indicates when a security mechanism has triggered the HSM to enter an alarmed state. This triggers the erasure of all the secret data stored within the HSM. • An unlit LED indicates no tamper condition exists. • A solid LED indicates a security compromise has occurred and the HSM is in an alarmed state.	
Host 1 LED	Indicates communication between with the HSM via the Host 1 port. • An unlit LED indicates no data is being received from the host. • A flashing LED indicates small amounts of data are being received. • A solid LED indicates large amounts of data are being received.	
Host 2 LED	Indicates communication between with the HSM via the Host 2 port. • An unlit LED indicates no data is being received from the host. • A flashing LED indicates small amounts of data are being received. • A solid LED indicates large amounts of data are being received.	
Management LED	Indicates communication between with the HSM via the Management port. • An unlit LED indicates no data is being received from the management PC. • A flashing LED indicates small amounts of data are being received. • A solid LED indicates large amounts of data are being received.	
Test LED	Not currently in use.	

5.2 Other Security-Relevant Information

The payShield 9000 has sensors that can monitor: physical intrusion, movement, temperature and voltage via its embedded TSPP cryptographic module. For further information on the TSPP security functions refer to the TSPP security policy [ref. 4].

The Reset button on the front panel of the payShield 9000 is used to trigger a reboot of the module when pressed for two seconds. The button is recessed to prevent accidental use.

The Erase button on the back panel of the payShield 9000 deletes the CSPs that reside in the embedded TSPP module; regardless of the power and operational state of the payShield 9000. The push-button itself is recessed behind the panel to prevent accidental erasures, and requires a thin probe to operate.

6. Identification and Authentication Policy

Every payShield 9000 has a fixed, unique serial number that is stored persistently within the device and is accessible via each of the payShield 9000 management interfaces. This serial number is also identifiable on the payShield 9000's hardware, on printed labels on the front and back panels of the chassis and also printed onto the tabs supplied with the physical keys associated with that module. These means of identification enable users to verify that the hardware inside the payShield 9000 is correctly aligned with the physical chassis and keys. For further information on the required inspection procedures refer to *Section 9* of this document.

The payShield 9000 chassis uses serialised, holographic labels to provide authenticated evidence of the unit's continuous physical integrity. For more information about the protection offered by the tamper evident labels see *Section 8.3* of this document.

The firmware that runs on the payShield 9000 is contained and controlled by the TSPP. For information on the security mechanisms in place to protect the firmware refer to the TSPP Security Policy [ref. 4].

For further details on the protection provided by each of the individual management interfaces refer to *Section 4* of this document.

7. Access Control Policy

The Access Control Policy enforced in the payShield 9000 depends on a number of factors which are described below. For further information on the mechanisms below refer to the payShield 9000 Security Operation Manual [ref. 5].

7.1 Locks and Security State

The payShield 9000 has two dual purpose cam locks on the front panel. These locks provide physical security by requiring independent keys which secure the module in a rack, i.e. under the principal of dual control. These locks also provide logical security to the payShield 9000 by controlling the security state of the module as seen in *Table 7-1* below.

Table 7-1 State and Required Lock Positions

State	Left Hand Lock	Right Hand Lock
Online	Locked	Locked
Offline	Locked	Unlocked
Offline	Unlocked	Locked
Secure	Unlocked	Unlocked

The three security states govern access to the security sensitive functions of the payShield 9000:

- Online state is the normal operating mode of the module and provides the most restrictive access to security sensitive functions.
- Offline state requires at least one physical key holder to be present, and allows access to some security sensitive functions.
- Secure state requires both physical key holders to be present and allows access to the most security sensitive functions within the module. It also facilitates unlocking the unit to remove it from a rack.

The Remote HSM Manager models the unit's physical keys with two Administrator smartcards. However, the Remote HSM Manager cannot connect to an HSM if either physical lock is in the unlocked position; i.e. the payShield 9000 must be fully locked and in the Online state. State changes within the Remote HSM Manager are triggered using the 'State' menu options; the options available are determined based on the current state and the required configurations for the physical locks and smartcard readers;

Table 7-2 highlights these configurations. For further information on state transitions within the Remote HSM Manager refer to the Remote HSM Manager User's Guide [10].

Table 7-2 Remote HSM Manager States

State	Smartcard Reader #1	Smartcard Reader #2
Online or Offline	Administrator smartcard inserted	Empty
Online or Offline	Empty	Administrator smartcard inserted
Online, Offline or Secure	Administrator smartcard inserted	Administrator smartcard inserted

7.2 Roles

The payShield 9000 supports Guest, Operator and Security Officer roles. The types of role and the associated authentication required are given in *Table 7-3* below.

Table 7-3 Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Guest	Unauthenticated	N/a
Operator	Identity based	Smartcard & PIN
Security Officer	Identity based	Smartcard & PIN (x2)

To authenticate to the Operator or Security Officer roles the user must present one or two Local Master Key (LMK) Authorizing Officer smartcards respectively. Once in an authenticated role the user receives escalated privileges specific to the LMK that the smartcards authorize. Thus the Operator and Security Officer roles are only available once at least one LMK has been installed within the payShield 9000.

The associated activities allowed within each role are shown below in *Table 7-4*.

Table 7-4 Role Activities

Role	Without LMK(s) Installed	With LMK(s) Installed
Guest	Fundamental configuration including initial security settings.	Read-only operations such as viewing the configuration and error logs.
Operator	N/a	In addition to Guest activities Operators may also perform key management functions and various diagnostic commands.
Security Officer	N/a	In addition to Operator activities Security Officers may also perform the most sensitive functions.

7.3 Authorization

Sensitive commands within the payShield 9000 require authorization before they can be executed. There are two supported methods of authorizing the HSM:

- Single authorized state involves authorizing all authorizable commands on a per LMK basis with the appropriate Authorizing Officer smartcards.

- Multiple authorized activities allow authorizable commands to be controlled with a finer degree of granularity. This functionality enables the user to select which commands are authorized and requires activities be authorised on a per LMK basis with the appropriate Authorizing Officer smartcards.

When a sensitive command(s) are authorized the user specifies how long the sensitive command(s) remain authorized for. Console commands may be authorized for up to 12 hours, host commands may be authorized indefinitely.

For a complete list of the authorizable activities within the payShield 9000 refer to the payShield 9000 Console Reference Manual [ref. 6].

7.4 Protection of Cryptographic Keys and Other CSPs

The payShield 9000 contains a TSPP cryptographic module within its metal enclosure. The TSPP module contains a protected battery-backed non-volatile memory that is the only place being used to store its non-volatile secret data.

The TSPP stores most of its cryptographic keys and other CSPs only in volatile memory. This memory is erased in response to detected tampering.

For further information on the cryptographic keys and CSPs stored within the TSPP refer to the TSPP security policy [ref. 4].

8. Physical Security Policy

The physical security of the payShield 9000 utilizes a layered defence approach which relies upon the combination of several separate components. The physical security mechanisms provided within the payShield 9000 are outlined in this section.

8.1 Physical Enclosure

The payShield 9000 has a strong steel case; and has no transparent surfaces or windows. The module also has baffles and internal covers that protect and shield components that handle sensitive information from view outside the HSM via ventilation holes. The locks on the front panel provide a mechanism for securely storing the module in a rack. The front panel itself has been designed to be difficult to remove without leaving evidence of the attack. Non-tamper evident labels on the casing are transparent to prevent an attacker hiding any tamper evidence underneath the label.

8.2 Tamper Detection & Response Switches

The payShield 9000 has a sealed top panel that is restricted to vendor-only access. Removing this top panel will provide access to the PCB, TSPP module covers, batteries and other internal components. As a result of this the panel is protected by two micro-switches which detect panel removal and upon detection trigger a tamper response mechanism.

The switches are positioned on opposite sides of the casing to decrease the probability of an attacker being able to gain access to both switches and disable the tamper detection circuit. When the top panel is secured in place it will depress the two switches into their normal operating positions. The switches are connected to the TSPP which monitors their state to check for any signs of tampering. Upon the detection of a tamper the TSPP triggers the erasure of all the secret data within the module.

8.3 Tamper Evident Labels

The payShield 9000 chassis uses serialised, holographic labels to provide tamper detection. The labels are serialized to aid the customer when inspecting the unit; the vendor maintains a record of the association between seals and modules. As shown in *Figure 2*, the left-hand end of the custom-designed label has a holographic background image to prevent them from being easily duplicated. If there is an attempt to peel the label from the metal cover, the surface will discolour; and, in the darkening colour, the word “VOID” will appear and will remain visible even if the label is pressed back to the surface of the cover. Any significant damage to a label may indicate attempts at tampering with the module.

Figure 2 Close-up of Thales Tamper Evident Label

The labels are self-adhesive, and their adhesive is fully cured and effective before the completed modules leave the manufacturing facility. The labels are designed and intended to stay in place and intact for the entire life of the module.

The labels are placed where the removable top metal cover meets the sides of the chassis, with one label on every side except the front, giving a total of three labels. The positioning of the labels would require that all three labels be removed to allow authorized access beneath the top cover e.g. for repair; and at least one label would need to be damaged or removed to enable sufficient access to the internals of the module. It should be noted that gaining access to the internals of the payShield 9000 does not provide access to the cryptographic keys and security-sensitive areas because they are protected by the TSPP module.

A further tamper evident label is used to protect the contents of the cardboard box used to ship the physical keys and smartcards associated with a payShield 9000.

8.4 TSPP Physical Security

The TSPP module embedded within the payShield 9000 contains a tamper-detection and response system of its own, used to protect the cryptographic keys and security-sensitive components housed within it. This system includes a tamper responsive metal enclosure, serpentine tracks to detect intrusion, a motion sensor and environmental failure protection to monitor temperature and voltage. For detailed information on this system refer to the TSPP Security Policy [ref. 4]. If the TSPP detects a tamper it triggers the erasure of its secure memory – deleting the secret data secured by the module.

9. Maintenance

The following section provides a description of the required payShield 9000 maintenance tasks. Detailed information pertaining to the required maintenance can found in the payShield 9000 Security Operations Manual [ref. 5]; to ensure the security of the module the procedures contained within this document should be adhered to.

9.1 Initial Inspection

Upon initial receipt of the module from the vendor or any time the HSM has travelled outside of the HSM Secure Area it is recommended that the Initial Inspection Procedure is performed. This inspection procedure aims to ensure the integrity and authenticity of the module upon delivery. It also tries to ensure that any unanticipated discrepancies related to the packaging can be attributed to a reliable source (e.g. as a result of a customs inspection).

9.2 Routine Inspection

The Routine Inspection Procedure should be carried out after any unauthorised entry to the HSM Secure Area and periodically every three months. It should also be performed whenever the Initial Inspection Procedure is performed. This inspection procedure aims to ensure that the module has not been tampered with in any way. This is achieved by checking the physical condition of the unit, that the operating state of the HSM matches its anticipated state, that there are no unexplained errors being reported, that the diagnostics complete successfully, and that the firmware versions match the expected versions.

9.3 Log Maintenance

The payShield 9000 has both an error log and audit log. The error log stores fault information for use by Thales e-Security support personnel. The audit log records state changes in the module and can be configured to record the execution of almost any console or host command.

The payShield 9000 has a finite amount of memory at its disposal, and as a result both logs store a limited number of records. The audit log has as much larger capacity than the error log because under normal operation it will be used more frequently. Once either log has reached its limit it will wrap around and proceed to overwrite the oldest records. To avoid the potential loss of log records due to the wrapping functionality Operators are recommended to routinely monitor the state of the logs as specified in the payShield 9000 Security Operations Manual [ref. 5]. This situation can be easily avoided by either clearing or archiving the logs on a regular basis.

9.4 Operational Limits

The payShield 9000 must operate in a controlled environment that provides conditions within the ranges specified in *Table 9-1*.

Table 9-1 Environmental Limits

Factor	Range
Operating Temperature	0 to 40°C
Humidity	10 to 90% (non-condensing)