THALES

cpl.thalesgroup.com

payShield 9000 v3.5

Installation Manual

1270A543-038

26 July 2021

Contents

End User License Agreement

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

https://cpl.thalesgroup.com/legal

Revision Status

Document No.	Manual Set	Software Version	Release Date
1270A543-038	Issue 38	payShield 9000 v3.5	July 2120

References

The following documents are referenced in this document:

1	payShield 9000 Console Reference Manual Document Number: 1270A544
2	payShield 9000 Host Command Reference Manual Document Number: 1270A546
3	PKCS#1: RSA Encryption Standard - Version 1.5 – Revised November 1993 (www.rsalabs.com)
4	PKCS#1: RSA Cryptography Standard – Version 2.0 – October 1998 (www.rsalabs.com)
5	Visa Integrated Circuit Card Specification, Version 1.4.0 – April 2001, plus August 2002 Corrections (www.visa.com)
6	MasterCard M/Chip 4 Cryptography and Key Management v4.0 – May 2002 (www.mastercardinternational.com/)
7	ASC X9 TR-31, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms, 2005.
8	Global Interoperable Secure Key Exchange Key Block Specification, version 2.3, written by ACI Worldwide, HP Atalla, Diebold, Thales e-Security and VeriFone Inc. 2002.

Chapter 1 – Introduction

General

The payShield 9000 hardware security module (HSM) provides cryptographic functions to support network and point-to-point data security. Acting as a peripheral to a Host computer, the HSM provides the cryptographic facilities required to implement key management, message authentication and Personal Identification Number (PIN) encryption in real time online environments. The payShield 9000 HSM is made physically secure by locks, electronic switches and tamper-detection circuits.

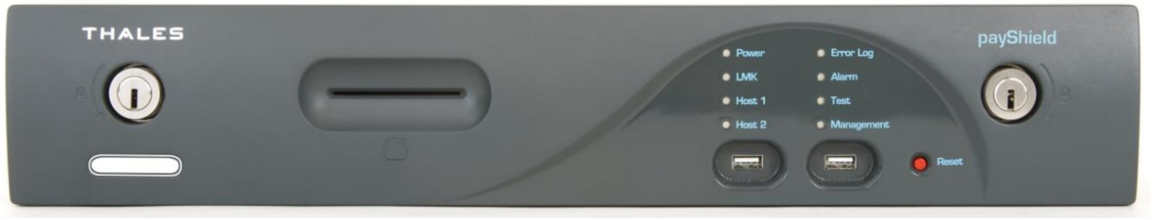


Figure 1 - payShield 9000: Front view

The payShield 9000 HSM supports a number of standard functions and can be customized to perform client-specific cryptographic functions. Standard functions include:

- Verifying and generating Personal Identification Numbers (PINs) such as those used with bank accounts and credit cards.
- Generating encrypted card values such as Card Verification Values (CVVs) for the plastic card industry.
- PIN solicitation, to obtain a new PIN from a card holder (against a reference number).
- 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.

A payShield 9000 system consists of a single stand-alone unit or a number of units mounted in a standard 19-inch cabinet. The payShield 9000 HSM can also be used to complement other HSMs in a standard 5-unit cabinet. A typical 5-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.

The payShield 9000 HSM is normally online to the Host and does not require operator monitoring or intervention. The HSM performs cryptographic processing in response to 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. The HSM processes the command messages and generates response messages, which also contain a variable number of fields (depending on the message type). Some commands, mainly involving plain text data, are entered by the user via the associated HSM console.

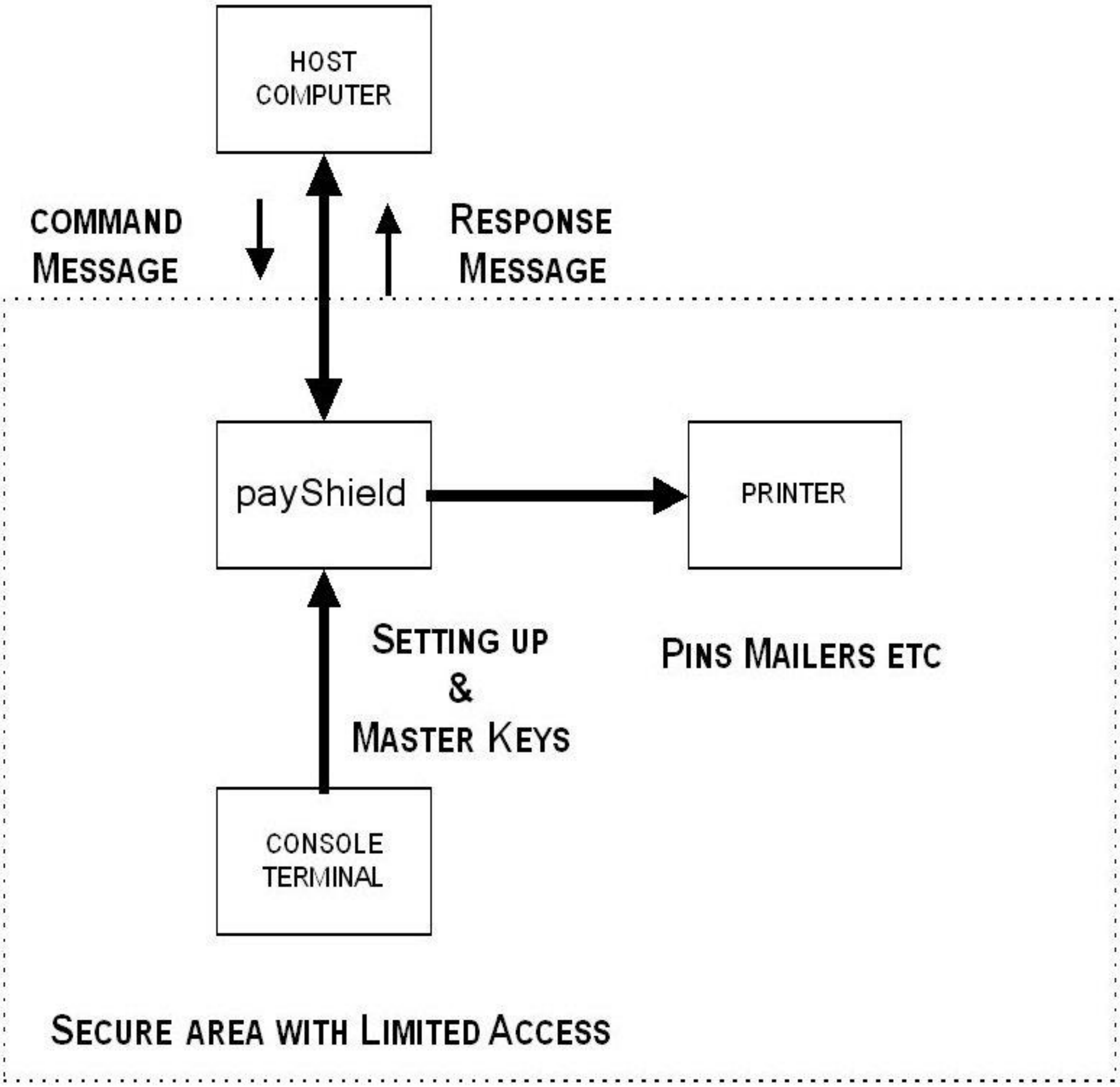


Figure 2 - payShield 9000 HSM in a typical system

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

Note that the console terminal, printer, cables or transceiver are not supplied with the HSM.

PCI HSM Certification and Compliance

Information about PCI HSM certification of the payShield 9000 can be found in Chapter 10 of the *payShield 9000 General Information Manual*.

About this Manual

This manual contains instructions for installing, connecting and configuring a payShield 9000 HSM. For other payShield 9000 information, see the following manuals:

- *payShield 9000 Security Operations Manual*
- *payShield 9000 Console Reference Manual*
- *payShield 9000 Host Programmer's Manual*
- *payShield 9000 Host Command Reference Manual*

Physical Description

See Chapter 2 of the *payShield 9000 General Information Manual* for a description of the payShield 9000.

Electrical Requirements

All electrical connections are made at the rear panel of the payShield 9000 HSM. Units are independent and each HSM in a cabinet requires power (100/240 volts) and connection to a Host port. If the Host computer runs from an uninterruptible power supply, connect the HSM(s) to the same supply.

A chassis earthing point is fitted to provide a good electrical connection, via a substantial braid, to a low impedance building earth, which is required for compliance with EMC regulations.

Host Interfaces

The HSM receives command messages via the Host interface. A message contains all the data required by the HSM to perform a cryptographic operation. The HSM processes the data, and generates a response message which it sends to the Host. If the HSM identifies errors in the received data, it sends an error code.

The HSM can be configured from the Console or via payShield Manager to provide either asynchronous serial or TCP/IP host connections.

Asynchronous Host Port

The payShield 9000 HSM can communicate with a host computer via an asynchronous serial connection by employing a USB-to-serial converter cable available from Thales. If it is not needed, the USB-to-Serial converter provided with the payShield 9000 for attachment of a Console can be used for asynchronous Host connection. (***Note**: you should not use any other USB-to-Serial converter cables – these converters are intelligent devices incorporating microprocessors, and the payShield 9000 software includes drivers only for the converter supplied by Thales.*)

The USB-to-Serial converter cable supplied with the payShield 9000 is 1.85 metres long and offers a 9-pin female serial connector. Although only Thales USB-Serial adapters may be used, standard off-the-shelf gender converters, connector adaptors (e.g. 9-pin to 25-pin), and extension leads available from PC shops, etc., can be used to provide flexibility of attachment (subject to limitations imposed by the serial communication standards).

The USB cable end should be inserted into one of the 4 USB ports on the rear panel of the HSM – see the comments on USB port hierarchy in the later section on Connecting to the Console Terminal. The serial cable end should be connected to the host computer. The console (CH command) or payShield Manager can then be used to select the appropriate configuration for the port.

Standard Asynchronous Emulation

Standard asynchronous emulation is half duplex, i.e. the Host must receive the response from the HSM before sending another command. There is no inherent flow control and the HSM returns its response as soon as it has finished processing a command. Typical processing times for PIN translations and verifications are 10 to 70 milliseconds (depending on the performance of the HSM). If the Host is logically half duplex and cannot receive such a quick response, a preset delay of 1 to 255 milliseconds can be inserted before the HSM sends the response.

Each command message to the HSM starts with STX (hexadecimal 02) and ends with ETX (hexadecimal 03). The response to the Host is also bracketed with the STX/ETX pair. These characters are the only data link control codes recognized, and any data between an ETX and the next STX is discarded. The HSM can be programmed to replace the ETX in its response with a one or two character string selected by the user, but the data from the Host is always terminated by ETX.

The data in the Host commands and the HSM responses is always ASCII/EBCDIC character data. Raw binary data is never sent; keys and PIN blocks are converted to their hexadecimal character representations (0-9, A-F) for transmission.

Transparent Asynchronous Emulation

In order to send binary data, the HSM can be configured for transparent asynchronous communications, in which it sends STX then the count (number of bytes), the data, a redundancy check character and ETX. The receiving unit verifies the redundancy check (which is over just the data), and confirms the number of bytes before accepting the data.

Ethernet Host Ports

There are two host Ethernet RJ45 ports on the rear panel: each has its own IP address and both ports may be used simultaneously for host communications. The host Ethernet interfaces use the TCP/IP and UDP protocols for 10/100/1000Mbps transmission over standard Cat 5, Cat 5e, or Cat 6 cables.

The HSM acts as a TCP/UDP server supporting up to 64 simultaneous connections on each port. These can be either 64 simultaneous TCP ports/sockets or 64 simultaneous TCP port/sockets and a UDP port (multiplexed). Applications establish connections to the HSM by connecting to the Well-Known-Port at the HSM's host IP addresses. The Port Numbers and IP Addresses are defined for the HSM at configuration.

It is recommended that the two host ports are on different subnets from the other Ethernet ports on the HSM (e.g. the Management Port).

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

FICON Host Ports

There are two host FICON ports on the rear panel to allow connection of the HSM to an IBM host computer using fiber optics. For further information on these ports, see Appendix B.

Configuration/Management Interfaces

The HSM can be configured and managed using a number of methods: a console terminal, a locally-attached PC running the payShield Manager, or a remote station running the payShield Manager (which requires HSM9-LIC037).

Console Port

The payShield 9000 HSM can be managed using a console (i.e. a "dumb terminal") with a serial asynchronous communications interface. The console is connected to one of the HSM's USB ports using a USB-to-serial converter cable available from Thales: one of these converter cables is delivered with each new payShield 9000. (***Note****: you should not use any other USB-to-Serial converter cables – these converters are intelligent devices incorporating microprocessors, and the payShield 9000 software includes drivers only for the converter supplied by Thales.*)

Almost any asynchronous ASCII terminal is suitable for use with the HSM. The default settings for the Console Port are: 9600 baud, eight data bits, no parity and one stop bit. When the Console is operational, the baud rate and word format can be changed to any convenient value.

Console operations include generating and loading the LMKs and Passwords, setting the HSM into the Authorized state by using the two Passwords or Smartcards and PINs, generating manually-distributed master keys and performing diagnostic functions. The terminal must therefore be located in a secure access-controlled area.

Management Port

An Ethernet management port is located on the rear panel of the payShield 9000 HSM. The management Ethernet interface uses the TCP/IP protocol for 10/100/1000Mbps transmission over a standard Cat 5, Cat 5e, or Cat 6 cable. Connections to payShield Manager must be made via the use of this management port.

It is recommended that the Management Portis on a different sub-net to the other Ethernet ports on the HSM (e.g. the Host Ports).

Note: When shipped from the factory with v3.x software, the payShield 9000's Management Port is configured to request an IP address using DHCP.

Printer Interfaces

A printer is required to print PIN mailers, print the internal audit log or generate and print components of manually-distributed keys. The payShield 9000 HSM can utilize a variety of serial or parallel interface printers connected using USB converter cables available from Thales.

In normal operation, the HSM is set into the Authorized state by the use of the Console, and then printing can start. Due to the sensitive nature of the data being transmitted to the printer and the actual printed output, the printer must be located in a secure access-controlled area.

Any printer that supports ASCII can be used with the payShield 9000. Thales recommends that customers use printers that support printing languages PCL or Postscript as they support ASCII and are industry standards, but other ASCII-supporting languages such as ESC/P will work as well.

Serial Printer

The payShield 9000 HSM can communicate with a printer via an asynchronous serial connection by employing a USB-to-serial converter cable (supplied by Thales). The USB cable end should be inserted into one of the 4 USB ports on the rear panel of the HSM; the serial cable end should be connected to the printer. If it is not needed, the USB-to-

Serial converter provided with the payShield 9000 for attachment of a Console can be used for serial printer connection. (***Note**: you should not use any other USB-to-Serial converter cables – these converters are intelligent devices incorporating microprocessors, and the payShield 9000 software includes drivers only for the converter supplied by Thales.*)

The console (CP command) or payShield Manager can then be used to select the appropriate configuration for the port.

Parallel Printer

For parallel printing, printers must follow the IEEE 1284 interface protocol and have an IEEE 1284 compliant parallel port. Both Uni-Directional and Bi-Directional parallel connections are supported.

The payShield 9000 HSM can communicate with a printer supporting an industry-standard IEEE 1284 parallel connection by employing a USB-to-parallel converter cable available from Thales: Centronics and 25-Pin parallel converter cables are available. The USB cable end should be inserted into one of the 4 USB ports on the rear panel of the HSM; the parallel cable end should be connected to the printer. (***Note**: you should not use any other USB-to-Parallel converter cables – these converters are intelligent devices incorporating microprocessors, and the payShield 9000 software includes drivers only for the converter supplied by Thales.*)

The console (CP command) or payShield Manager can then be used to select the appropriate configuration for the port.

USB Printer

The payShield 9000 HSM can communicate with a native-USB printer via a standard USB cable. The USB cable end should be inserted into one of the 4 USB ports on the rear panel of the HSM. The console (CP command) or payShield Manager can then be used to select the appropriate configuration for the port.

SNMP Interface

The payShield 9000 can provide utilization and health check data via SNMP. The data can be accessed by sending SNMP requests to either of the Ethernet host ports or the Management Port.

Chapter 16 of the *payShield 9000 Host Programmer's Manual* provides an overview of these capabilities and how the SNMP interface may be configured.

The software provided with your payShield 9000 includes the SNMP MIB, which you will need to build your SNMP interface to the payShield 9000.

Chapter 2 – Installation

Important!

Before installing and using this product, please read the Warnings and Cautions in the following document, which is supplied with the HSM in paper format:

payShield 9000 Regulatory User Warnings & Cautions

Ref: 1270A579

Wichtig!

Vor der Installation und Verwendung dieses Produktes lesen Sie bitte die Warnhinweise in den folgenden Dokument, das mit dem Produkt in Papierform geliefert wird:

payShield 9000 Regeln Benutzer Warnungen und Vorsichtshinweise

Ref: 1270A579

General

This chapter describes the physical installation of the HSM in the computer room. It then requires configuration, as described in Chapter 3, and Local Master Key loading as described in the *payShield 9000 Security Operations Manual*. Please also refer to Appendix A, "Warnings, Cautions and Statutory Statements".

Should any malfunction be suspected in the unit, return the apparatus to your supplier for service and/or repair to ensure continued compliance.

The payShield 9000 series HSMs contain no user serviceable parts except for the mains fuses which are detailed in this chapter.

The unit should be installed in an environment compatible with the maximum operating temperature of the unit.

Installation of the unit in a rack should not reduce air flow so as to compromise safe operation of the unit. Particular attention should be made to make sure that the side ventilation holes are not obstructed which could reduce the airflow through the unit.

When installed in a rack make sure that the unit is securely installed using all the appropriate mechanical fixings so that it will not cause a hazardous condition.

Installing the HSM into a Rack

A payShield 9000 system can consist of a number of payShield 9000 HSMs in a standard 19-inch rack.

The rack should be installed as a peripheral device in a computer room. The maximum recommended ambient temperature for operating payShield 9000 HSMs is 40°C. Consideration must be given to the airflow and temperature when the units are installed in a rack to ensure this temperature is not exceeded. Additional racks and units may be added as needed.

Each payShield 9000 HSM is delivered in a box with its power cables.

A set of blank Smartcards and a unique set of physical keys are supplied with each unit. The keys are sometimes taken to the installation site by an installation engineer.

Positioning the Rack and Cables

Access is required to the front and the rear of the rack, about 1220mm (4ft) in each case. The rack or cabinet has no base so, if the computer room has a raised floor, cables can be passed up to each HSM, from under the rear left-hand corner.

Fitting the HSM into the Rack

The payShield 9000 HSM is fitted into the rack using the standard L-shaped fittings supplied by the rack manufacturer. If these are not available then runner kits for fitting the HSM can be obtained from Thales e-Security.

Locks

Two keys are required to fit an HSM into a rack and, subsequently, to change the HSM between the offline, secure and normal (online) operation states. One key is for the left-hand lock and the other for the right-hand lock (see Figure 1). The keys are unmarked when they leave the factory (except for a number tag). Note the tag numbers, because it is impossible to replace a key without this number (the keys CANNOT be copied legally by a locksmith). The keys are normally retained by independent security officers to provide dual control. Duplicates of each key are supplied with each unit.

For each HSM, make a note of its serial number and associated key tag numbers, and store this information in a secure location; it may be useful if a key needs to be replaced later.

The keys have labeled tags which identify the correct key for each lock.

Battery

A battery housed within the HSM maintains the sensitive key material stored in protected memory whilst the external AC power is removed. Without any AC power, the battery will maintain the contents of protected memory for around 10 years. When the HSM is running on AC power, the battery is not used, and discharge is minimal.

Power Supply and Fuses

This equipment 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.

Preparing the payShield 9000 for Use

Connecting Power

The payShield 9000 HSM may be provided with one or two IEC style power sockets and 20 mm fuse holders. Each socket provides power to a separate distribution unit within the HSM.

You can connect a power supply to either or both sockets.

The use of two sockets distribution units allows the HSM to receive power from two independent supplies. This redundancy is designed to help prevent any break in the operation of the HSM in the event of:

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

Note: There is no on/off switch on the payShield 9000 HSM, so it powers-up as soon as it is connected and power supply is turned-on.

Booting Up

If a Console terminal is connected to the HSM when power is applied or when the HSM is reset using the Reset button on the front panel, the following booting up message is displayed:

```
Local Bus Controller v. X.X
Bootstrap            v. X.X.X
Boot Manager         v. X.X.X

Hit any key to interrupt the load process and enter the boot manager:

0__10___20___30___40___50___60___70___80___90__100%
##################################################

Transferring control to application
```

Note that the console must be set to 115,200 bps, 8 data bits, 1 stop bit, and no parity to see this booting up message. The message indicates the revision of boot software, and identifies the USB port used by the console connection.

When control is transferred to the application, the console configuration changes to the factory default (9,600 bps, 8 data bits, 1 stop bit, no parity) or to any other settings entered by the user during a previous session. (The 9,600 bps setting provides consistency with the earlier HSM 8000.) A prompt reflecting status of the PCI HSM-relevant security settings and the position of the keys on the front panel, such as the following, will be seen if the console is set to the appropriate speed:

Example 1:

```
WARNING: Some security settings are not PCI HSM compliant

Online>
```

Example 2:

```
All security settings are PCI HSM compliant

Secure>
```

For more information about PCI HSM, see Chapter 10 of the *payShield 9000 General Information Manual*.

Because the booting up message is generally not important to the user, it is recommended that the console is set to 9,600bps (or the different speed that the user has previously configured). This means that the booting up message will not be legible.

If the payShield 9000 is fitted with a FICON interface, see Appendix B for a description of the diagnostic information provided by the LEDs on the FICON interface.

Connecting to the Console Terminal

The console is connected to one of the USB port on the console, using the USB-to-Serial converter cable supplied with the payShield 9000. (Note: you should not use any other USB-to-Serial converter cables – these converters are intelligent devices incorporating microprocessors, and the payShield 9000 software includes drivers only for the converter supplied with the unit.)

The USB ports on the HSM have a hierarchy, and it is important that no serial devices are attached to a USB port with a higher priority than the Console. (Attaching a serial device to a higher priority port than the console means that console output will be sent to that device when the HSM is re-booted.) The port hierarchy (from highest to lowest) is:

Front left port
Front right port
Rear port labeled "3"
Rear port labeled "4"
Rear port labeled "1"
Rear port labeled "2"

Attaching a parallel device to a port with a higher priority than the Console will not cause a problem.

If a Console is being attached to a payShield 9000 that has already been in use, it must not be attached to a USB port which has been configured for a printer.

The USB-to-Serial converter cable supplied with the payShield 9000 is 1.85 metres long and offers a 9-pin female serial connector. *(**Note**: you should not use any other USB-to-Serial converter cables – these converters are intelligent devices incorporating microprocessors, and the payShield 9000 software includes drivers only for the converter supplied by Thales.)* Standard off-the-shelf gender converters, connector adaptors (e.g. 9-pin to 25-pin), and extension leads available from PC shops, etc., can be used to provide flexibility of attachment (subject to a total length of 50 feet or 30.5 metres).

The Console terminal is not supplied with the HSM and must be provided by the user. It can be any type of standard terminal, e.g. a VT100.

The Console may be used during installation, and for operations in which secret data is entered into the HSM. Console operations include generating and loading the Local Master Keys (LMKs) and passwords, putting the HSM into the Authorized state, generating manually-distributed master keys and performing diagnostic functions. The terminal must therefore be located in a secure access area.

The Console terminal is not required for normal day-to-day HSM operation, so a single terminal can be shared across a set of HSMs.

Notes:

- Remote or local management using payShield Manager replaces the need for a console during normal operation. A console may still be required for initial set-up of the HSM. See the payShield Manager User Guide for further information.
- For security reasons, a PC or other computer running terminal emulation software should not be used as the HSM console unless security measures approved by the customer's security staff or auditors are in place.

Console Specification

Character set:	ASCII
Interface:	RS-232-C
Baud:	1200 bps to 115200 bps (default 9600 bps)
Stop bits:	1 or 2 (default 1)
Data bits:	5, 6, 7 or 8 (default 8)
Parity:	Odd, Even or None (default: None)
Flow control:	None, Software or Hardware (default: None)

The Console must not be able to store information and display it at a later time (because some data may be of a sensitive nature).

Character transmission rates and formats are specified by the user and can be configured at the time of installation. The Console must be capable of operating at the factory default settings. See the *payShield 9000 Security Operations Manual*.

Confirming Correct Console Configuration

Assuming the default settings (as shipped from the factory, or after a cold start) apply, configure the Console as instructed in the *payShield 9000 Security Operations Manual*, and for full duplex with no local echo.

Press the <Return> key twice. The HSM should respond with:

```
Online>
```

which indicates that correct communications have been achieved but a valid command has not been entered.

Connecting to the Printer

A printer can be connected to allow the payShield 9000 HSM to print PIN mailers or generate and print components of manually-distributed keys. A serial or parallel printer can be used.

Serial Printer Connection

The printer is connected to a USB port on the payShield 9000 by employing a USB-to-serial converter cable available from Thales. If it is not needed, the USB-to-Serial converter provided with the payShield 9000 for attachment of a Console can be used for serial printer connection. *(**Note**: you should not use any other USB-to-Serial converter cables – these converters are intelligent devices incorporating microprocessors, and the payShield 9000 software includes drivers only for the converter supplied by Thales.)*

The USB-to-Serial converter cable supplied with the payShield 9000 is 1.85 metres long and offers a 9-pin female serial connector. Standard off-the-shelf gender converters, connector converters (e.g. 9-pin to 25-pin), and extension leads available from PC shops, etc., can be used to provide flexibility of attachment (subject to limitations imposed by the serial communication standards).

The USB cable end should be inserted into one of the 4 USB ports on the rear panel of the HSM – see the comments on USB port hierarchy in the earlier section on Connecting to the Console Terminal. The serial cable end should be connected to the printer. The console (CP command) or payShield Manager can then be used to select the appropriate configuration for the port.

Serial Printer Specification

Character set:	ASCII
Interface:	RS-232-C (via USB-to-serial converter cable)
Baud:	1200 to 115200 bps (default 9600 bps)
Stop bits:	1
Data bits:	7 or 8 (default 8)
Parity:	Odd, even or none (default none)
Flow control:	XON, XOFF

Parallel Printer Connection

The payShield 9000 HSM can communicate with a printer via an industry-standard IEEE 1284 parallel connection by employing a USB-to-DB25 or USB-to-Centronics converter cable available from Thales. *(**Note**: you should not use any other USB converter cables – these converters are intelligent devices incorporating microprocessors, and the payShield 9000 software includes drivers only for the converters supplied by Thales.)*

Standard off-the-shelf gender converters, connector converters, and extension leads available from PC shops, etc., can be used to provide flexibility of attachment (subject to limitations imposed by the appropriate communication standards).

The USB cable end should be inserted into one of the 4 USB ports on the rear panel of the HSM; the parallel cable end should be connected to the printer. The console (CP command) or payShield Manager can then be used to select the appropriate configuration for the port.

Parallel Printer Specification

Character set:	ASCII
Interface:	IEEE 1284 (via USB-to-DB25 or USB-to-Centronics converter cable)

Installing Software and Licenses

When a payShield 9000 is initially delivered, it will have the appropriate software and licenses already installed, and so there is no need for the user to install these before using the HSM.

If at a later time it is required to update the software or add additional licenses to the payShield 9000, it will be necessary to load the new software or license. The process for doing this is described at *Appendix C – Installing Software and Licenses*.

Chapter 3 – Configuration

License File

An HSM license is an electronic file which when loaded into a payShield 9000 HSM, determines the features available to the user. The license is associated with a particular unit's serial number and is therefore not transferable between units. The license will affect such areas as the communication interfaces and the cryptographic algorithms available. It will also determine which of the unit’s commands are active, i.e., although all available commands are displayed only those covered by the license will be active. The range of features and commands will be those specified by the customer at the time of purchase.

The payShield 9000 is delivered with the license file already installed. A new license file must be installed when the software or functionality options of the HSM are upgraded – see *Appendix C – Installing Software and Licenses*.

The View Revision console command can be executed whatever the state of the HSM. It displays the version of the HSM Application, and the license attributes of the HSM.

Example:

```
Online> VR <Return>
Base release: X.XX
Revision:     XXXX-XXXX
Build Number: XXXX

HSM Core API Version:    X.X.XX

Serial Number:  XXXXXXXXXXXX
Unit info:      Licenced

Host Configuration: Async,Ethernet,FICON
Licence Issue No:   1
Performance:        800 TPS
Base Software:      Version 1
Ship Counter:       1
Crypto:             3DES,AES,RSA
LMKs Enabled:       5 LMKs

Press "Enter" to view additional information... <Return>

HSM9-LIC001 Base Software
HSM9-LIC002 RSA
HSM9-LIC005 User Authentication
HSM9-LIC006 X9 TR-31
HSM9-LIC008 Message Encryption
HSM9-LIC013 5 LMKs

Bootstrap Version:         X.X.X
Bootmanager Version:       X.XX.X
LBC Version:               X.X
Microcontroller Version:   X.XX

AGS Cryptographic Library:           X.XX.XXXX
FIPS Validated DRBG/RNG Algorithm:   TSPP-XXXXXXX
FIPS Validated SHA Algorithm:        TSPP-XXXXXXX
FIPS Validated HMAC Algorithm:       TSPP-XXXXXXX
FIPS Validated TDES Algorithm:       TSPP-XXXXXXX
FIPS Validated RSA Algorithm:        TSPP-XXXXXXX
FIPS Validated AES Algorithm:        TSPP-XXXXXXX
FIPS Validated CMAC Algorithm:       TSPP-XXXXXXX
Online>
```

It can be seen from the above example that the HSM is operating under the initial license and is licensed for 800 TPS performance, Version 1 Base Software, 3DES and RSA Cryptographic algorithms, and has Asynchronous, Ethernet, and FICON communication interfaces.

Error codes will be returned if an attempt is made to use unlicensed commands.

AB67 If command is not licensed (whether exists or not).

AB15 If command is licensed but does not exist.

General

The remaining sections of this chapter describe how to physically configure the payShield 9000 HSM to work with the Host system. Configuration of the alarms and the security settings can be found in the *payShield 9000 Security Operations Manual*.

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. Thus:

```
0123456789ABCDEF
```

is shown on the screen as:

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

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

```
TERMINATED
```

Configure the Console Port

The HSM Console port can be configured while the HSM is in online, offline or secure state.

The new values take effect immediately after the command has completed.

Enter **CC** `<Return>` (Configure Console) to initiate the following example in which user input is shown underlined. The Console baud rate is to be changed to 9600, and the word format is to be changed to 8 data bits, no parity and one stop bit.

Example:

```
Offline> CC <Return>

Serial Port:

    BAUD RATES
 1.   1200
 2.   2400
 3.   4800
 4.   9600
 5.  19200
 6.  38400
 7.  57600
 8. 115200 (current value)
Console baud rate (ENTER for no change): 4 <Return>

  DATA BITS
 1. 5
 2. 6
 3. 7 (current value)
 4. 8
Console data bits (ENTER for no change): 4 <Return>

  STOP BITS
 1. 1 (current value)
 2. 2
Console stop bits (ENTER for no change): <Return>

  PARITY
 1. none (current value)
 2.  odd
 3. even
Console parity (ENTER for no change): <Return>

  FLOW Control
 1. none (current value)
 2. software
 3. hardware
Console flow_ctl (ENTER for no change): <Return>

Serial Port will be configured as:
 Baud: 9600
 Word format: 8 bits, none parity, 1 stop
 Flow control: none

Offline>
```

Configure the Management Port

The HSM must be in the offline or secure state for configuration of the Management port.

The Management port is an Ethernet port used only for management of the HSM, and cannot be used to process host commands.

The new values take effect immediately after the command has completed.

Enter **CM** `<Return>` (Configure Management) to initiate the following example in which user input is shown underlined.

Example:

```
Offline> CM <Return>
Management Ethernet Port:
IP Configuration Method? [D]HCP or [S]tatic (DHCP): s <Return>
Enter IP address: 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:
  Enabled or Disabled? (E): D <Return>

Offline>
```

Where a firewall is used to protect the network link to the management port, the following ports should be opened as appropriate:

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
80 & 443	TCP	payShield Manager

It is recommended that the Management Ethernet Port and Host Ethernet Port(s) have independent IP subnets.

Configure the Printer Port

The Printer port can be configured while the HSM is in offline or secure state.

The user is invited to select 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. The converter cables can be supplied by Thales.

The values entered take effect immediately after the command has been completed.

Enter **CP** `<Return>` (Configure Printer) to initiate the following example in which user input is shown underlined.

Example 1: (Serial printer)

```
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 Prolific Technology Inc. located at Rear 4
        (current selection)
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: (Parallel printer)

```
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.   USB2.0-Print  by  located at Rear 1
Your selection (enter for no change): 1 <Return>
Timeout [in milliseconds, min=1000, max=86400000] (1000): 1000<Return>
Delay [in milliseconds, min = 0, max=7200000] (0): <Return>
Print test page? [Y/N]: Y <Return>

Offline>
```

Example 3: (Native-USB printer)

```
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 EPSON located at Front left (current selection)
Your selection (ENTER for no change): 1 <Return>
Timeout [in milliseconds, min=1000, max=86400000] (1000): 1000 <Return>
Delay [in milliseconds, min = 0, max=7200000] (0): <Return>
Print test page? [Y/N]: N <Return>

Offline>
```

Default Serial Printer Settings

The default settings for a serial printer are:

Character Set:	ASCII
Interface:	RS 232-C
Baud rate:	9600 bps
Stop bits:	1
Data bits:	8
Parity:	None
Flow Control:	XON, XOFF

Configure the Host Ports

The payShield 9000 HSM Host interfaces can be configured using the Console to emulate a number of types of data communications equipment and control equipment (as outlined in Chapter 1). At the end of the configuration, the user is given the option to save the host interface settings to a Smartcard.

Configuring the Software

To configure the Host port, set the HSM into the offline state (insert the key in one of the key switches on the front panel and rotate it fully), with power applied and the Console terminal connected.

The Console displays:

```
Offline>
```

Enter **CH** `<Return>` to initiate the following examples in which user input is shown underlined. The **CH** command can also be used while the HSM is in the secure state.

The values entered take effect immediately after the command has been completed.

Asynchronous Emulation

In Asynchronous Emulation the HSM is viewed by the Host as a DCE (data communications equipment) device, and does not require a modem.

To configure the HSM for asynchronous communications:

- The port must be defined as a DCE.
- Details held in software must be configured.

The following variables can be configured:

- The required length of the message header. This is normally set to 4, but can be set between 1 and 255. This depends on the value used by the Host computer application.
- The baud rate of the Host computer port.
- The word format of the Host computer port.
- The required communications protocol, either standard or transparent asynchronous characters.

- The asynchronous terminating characters. The terminating sequence can be either one or two characters. To select the terminating characters four hexadecimal values must be entered. If only one terminating character is required, enter the first two hexadecimal values followed by 00.

Note: The payShield 9000 HSM automatically detects whether an incoming command message uses ASCII or EBCDIC characters, and process the command accordingly, returning the result in the same format.

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.

Transparent Asynchronous Communications

In the standard asynchronous mode of communication, codes like STX (X’02) and ETX (X’03) have a special meaning, but they can sometimes occur in a stream of binary data, where that special meaning does not apply.

To avoid ambiguity, Transparent Asynchronous Communications mode is used. This has a simplified message format (for details, see Chapter 2 of the *payShield 9000 Host Programmer’s Manual*).

The Host port of the payShield 9000 HSM must be configured for Transparent Async Communications and 8-bit data transfers.

Example

```
Offline> CH <Return>

Please make a selection.  The current setting is in parentheses.
Message header length (1-255): 6 <Return>
Host interface [[A]sync, [E]thernet] (E): A <Return>
Transparent mode [Y/N](NO): Y <Return>
* No interface device configured *

The following possible asynchronous interface devices were found in
the system:
 1. USB-Serial Controller by Prolific Technology Inc. located at Rear
3
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
5.  19200
6.  38400
7.  57600
8. 115200 (current value)
Device baud rate (ENTER for no change):  <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 (current value)
2. hardware
3. software
Host flow control (ENTER for no change): <Return>
Save HOST settings to smartcard? [Y/N]: Y <Return>
Insert card and press ENTER: <Return>
HOST settings saved to the smartcard.
Offline>
```

Ethernet Communications

The payShield 9000 Host port provides two auto-sensing Ethernet interfaces, which support 10 base-T, 100 base-TX or 1000 base-TX.

The payShield 9000 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.

Note: If the host computer and HSM are on different networks, then the HSM's ROUTE console command should be used to add static routes to the HSM.

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 00000_{10} to 65535_{10} representing an address in the range 0000_{16} to FFFF_{16}.
- 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 9000 HSM automatically detects whether an incoming command message uses ASCII or EBCDIC characters, and process the command accordingly, returning the result in the same format.

Example: (Ethernet communication with UDP and TCP/IP)

```
Offline> CH <Return>
Please make a selection.  The current setting is in parentheses.
Message header length [1-255] (4): <Return>
Host interface [[A]sync, [E]thernet, [F]icon] (E): <Return>
Enter Well-Known-Port (1500): <Return>
UDP [Y/N] (Y): N <Return>
TCP [Y/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:
Enter IP Address (192.168.200.36):192.168.200.100 <Return>
Enter subnet mask (255.255.255.0): <Return>
Enter Default Gateway Address (192.168.200.1): <Return>

Interface Number 2:
Enter IP Address (192.168.202.110): <Return>
Enter subnet mask (255.255.255.0): <Return>
Enter Default Gateway Address (192.168.202.1): <Return>

Save HOST settings to smart card? [Y/N]: n<Return>
Offline>
```

To read the current configuration, use command **QH**:

```
Offline> QH <Return>
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 autoselect (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 autoselect (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:

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 9000, 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 9000 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.

FICON Communications

The payShield 9000 Host port provides two auto-sensing FICON interfaces, which support connection speeds of 2, 4, and 8 Gbps.

Appendix B gives further information about the FICON interface.

Software Parameters

There are a number of prompts for configuring the software using the console (CH command) or payShield Manager:

- The message header length
- The Control Unit Image.
- Unit Address for this Control Unit
- Missing Interrupt Handler

See Appendix B for further information.

Appendix A – Warranty Statement

Hardware

Thales e-Security warrants that Product (excepting software products) supplied will be free from defect resulting from faulty manufacture or workmanship for 12 months from the date of delivery.

Product found to the Company's satisfaction to be defective will, at the sole discretion of the company, either be replaced free of charge or repaired free of charge provided that:

- the Products (or samples thereof showing the alleged defects) are returned properly packed carriage paid to one of the Company's facilities at the customer's risk within 12 months from the date of delivery as defined in our normal terms and conditions of trading, and
- the Products have not been misused mishandled overloaded amended modified or repaired in any way by the customer its servants or agents, or used for any purpose other than that for which they were designed, and
- the Product’s functions have not been restricted, or the Product has not been damaged, by the use of non-Thales supplied or approved accessories, and
- if the Products have been manufactured to the Customer's design the defects are not as a result of faulty design by the Customer.

Repaired or replaced Products will be returned free of charge to destinations within the country to which they were originally delivered or will be returned FCA (at Thales e-Security' nominated port) to other destinations.

This warranty is the only warranty given by the Company and specifies the entire liability of the Company including liability for negligence and in particular but without limitation all statutory or other express implied or collateral terms conditions or warranties are excluded.

Note: The limits on Thales e-Security liabilities and a customer's legal rights as expressed in these warranties are applicable to the maximum extent allowed by the appropriate governing law in the customer's state or jurisdiction.

Appendix B – FICON Interface

Overview

The payShield 9000 can ordered with a factory-fitted FICON interface. This provides 2 ports for connection to an IBM mainframe host computer to allow host commands and responses to be transmitted using a FICON fiber optic interface: only one FICON port can currently be used.

The HSM's FICON interface supports speeds of 2, 4, or 8 Gbit/s using auto-negotiation. If using a switched fabric, the connecting switch must have the connecting port type set to fabric port (F_port).

The FICON interface can be ordered with a choice of transceivers to support:

- Short wavelength (850 nm) on OM1, OM2, or OM3 multi-mode cables; or
- Long wavelength (1310 nm) on OS1/2 single-mode cables.

The recommended emulation is for a DUMMY device running on a NOCHECK Control Unit, although 3490 tape drive emulation is also supported.

The FICON interface is fully integrated into the HSM's application software, and the Utilization and Health Check reporting facilities will report on the FICON interface.

NOTE: the FICON interface must be specified when the payShield 9000 is ordered and installed in the factory. It cannot be added to an existing payShield 9000.

Layout of the FICON Interface

The FICON interface (if fitted) can be found on the rear panel of the HSM towards the left-hand side, as indicated in the schematic Rear Panel layout in Chapter 1. The schematic layout of the FICON interface is shown below:

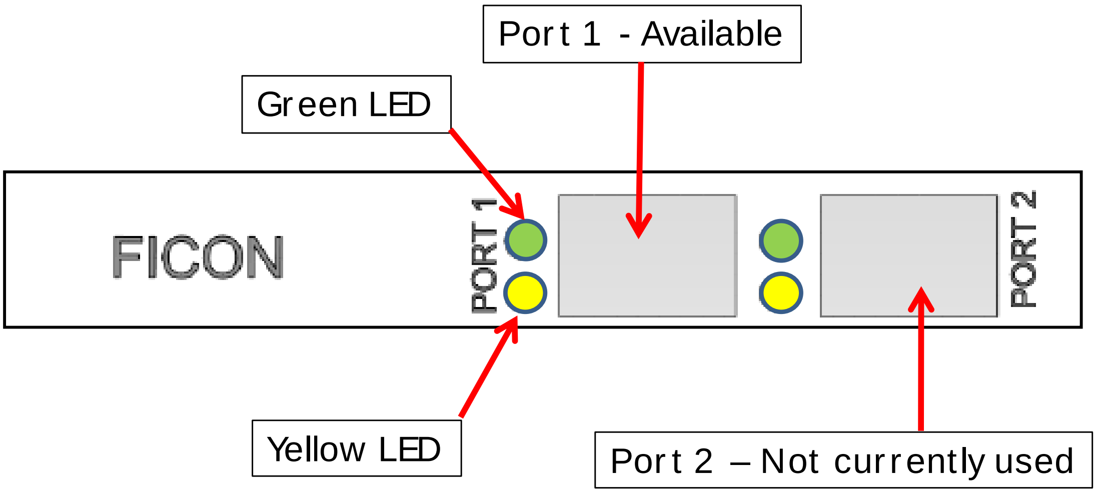


Figure 3 - Layout of the FICON interface

Although the FICON interface has two physical ports, only Port 1 can be used.

Specification of the Host Bus Adapter (HBA)

Characteristic	Short Wavelength Transceiver			Long Wavelength Transceiver		
Data Rate	2.125, 4.25, 8.5 Gbps (auto-detected)			2.125, 4.25, 8.5 Gbps (auto-detected)		
Optics	Short wave (850 nm) laser			Long wave (1310 nm) laser		
Cable Types	Multimode: OM3 – 50/125 µm OM2 – 50/125 µm OM1 – 62.5/125 µm			Single Mode: OS2 – 9 µm OS1 – 9 µm		
Connector Type	LC			LC		
Min. cable length	0.5 metres			0.5 metres		
Max. cable length (*Maximum cable length may be less than shown in this table, dependent on the fiber material used in the cable.*)	**Cable**	**Data Rate**	**Metres**	**Cable**	**Data Rate**	**K'metres**
	OM3	2.125 Gbps	500 m	OS1 & OS2	2.125 Gbps	10 Km
		4.25 Gbps	380 m		4.25 Gbps	10 Km
		8.5 Gbps	150 m		8.5 Gbps	10 Km
	OM2	2.125 Gbps	300 m			
		4.25 Gbps	150 m			
		8.5 Gbps	50 m			
	OM1	2.125 Gbps	150 m			
		4.25 Gbps	70 m			
		8.5 Gbps	21 m			

Table 1 - Specification of the Host Bus Adapter

Device emulation

The recommended emulation is for a DUMMY device running on a NOCHECK Control Unit, although 3490 tape drive emulation is also supported.

Confirming presence of the FICON interface

You can confirm that your payShield 9000 is fitted with a FICON interface by doing the following:

- Looking at the rear panel of the HSM and checking that there is a FICON interface, as shown in Figure 3 in Chapter 2 of the *payShield 9000 General Information Manual*. If no FICON interface is fitted, the FICON interface is replaced with a blanking plate.
- Use the CH and QH Console commands or payShield Manager to confirm that FICON is configured – see the following section.
- Run the VR Console command or payShield Manager to check that:
    - The serial number begins with a D
    - The "Host Configuration" entry includes the word "FICON".

FICON Interface configuration

The FICON interface is configured using the CH Console command or payShield Manager. FICON should be selected as the active host interface – for example, by specifying F in the CH Console command:

```
Host interface [[A]sync, [E]thernet, [F]icon] (E): F <Return>
```

The following parameters are required to configure the interface:

Parameter	Type	Min	Max	Default	Explanation
Message header length	Numeric	-	-	-	The same as in Ethernet or Async
Control Unit Image	Numeric	0	255	0	This is the control unit address defined in the mainframe I/O definition. (CUADD on CNTLUNIT statement.) *
Unit Address	Numeric	0	255	0	The starting unit address for this control unit. 16 devices are enumerated from this point. (UNITADD on CNTLUNIT statement.) *
Missing Interrupt Handler (mih) Minutes	Numeric	0	60	0	This specifies the missing interrupt handler value to be used in the read device characteristics CCW for the mainframe. If set to 0, the mainframe setting is used.

Table 2 - FICON Configuration Parameters

* In most circumstances, installations will code 0 (the default) for both the Control Unit Image and the Unit Address.

Example (using the Console):

```
Secure>CH <Return>

Please make a selection.  The current setting is in parentheses.
Message header length [1-255] (4): <Return>
Host interface [[A]sync, [E]thernet, [F]icon] (E): F <Return>
Control Unit Image [0-255] (0): <Return>
Unit address [0-255] (0): <Return>
Missing Interrupt Handler (mih) Minutes [0-60] (0): <Return>
Save HOST settings to smart card? [Y/N]: N <Return>

Secure>
```

To read the current configuration, use command **QH**:

```
Online>QH <Return>

Message header length: 04
Protocol: FICON
Control Unit Image: 0
Control Unit Address: 0
Missing Interrupt Handler (mih): 0 minutes

Online>
```

Performance

Full performance (in terms of throughput) is achieved by using multiple connections to the HSM. Optimum performance is normally achieved by using 4-8 connections (dependent on the host command being used and the payShield 9000 performance model), but with the 1500 tps model performance continues to improve slowly up to the maximum of 16 connections.

SRM

FICON-enabled payShield 9000 units can be connected to the host application using the optional Thales SRM software for IBM hosts, subject to the following conditions:

- SRM software version 2.4 or later must be used.
- Where version 2.4 software is used, the following patches must be installed:
    - SL24011
    - SL24016

Inserting and Replacing the Transceivers

Depending on what was specified in your payShield 9000 order, the FICON version of the payShield 9000 will have been delivered with either 2 Shortwave or 2 Longwave transceivers. The transceivers will be either:

- already fitted into the payShield 9000 unit, or
- provided in separate packaging, in which case you will need to insert them into appropriate FICON port socket(s).

Currently only Port 1 can be used for connection to a Host computer. However, both transceivers must be fitted in order to allow the FICON diagnostic test to be run (see below).

An example of one type of transceiver used is shown in the following diagram:

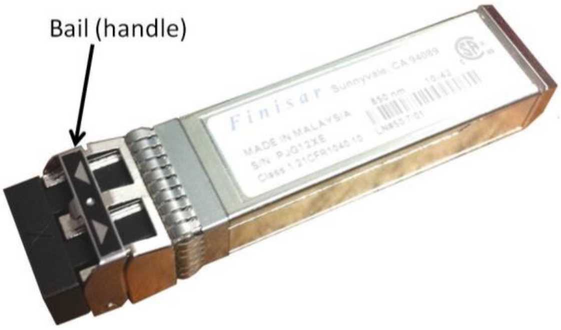


Figure 4 - Typical FICON Transceiver

Dust plugs (see fig. B5) will be inserted in any FICON port sockets which are not fitted with a transceiver.

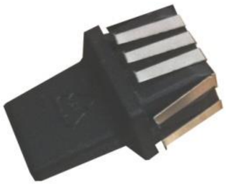


Figure 5 - FICON Dust Plug

If it is required to adapt a payShield 9000 ordered with Shortwave transceivers to Longwave (or vice versa) this can be done by removing the supplied transceiver and replacing it with the required type. The specification of the replacement transceiver to be used can be obtained through Thales Support.

A transceiver can be fitted as outlined below. **Important**: please note that:

- This is a delicate operation – take care not to damage the transceivers.
- Observe standard ESD (Electrostatic Discharge) precautions for handling electronic components.
- The fitted or replacement transceiver may be different from the type shown below.

1. Disconnect the payShield 9000 from its electrical power supply.
2. To remove a transceiver, pull the bail (handle) out and down to release the latch and gently pull the transceiver out without forcing it: after the latch is released, the transceiver slides out easily.

   The following diagram shows the Port 1 transceiver partially extracted with the Port 2 transceiver still latched in place.

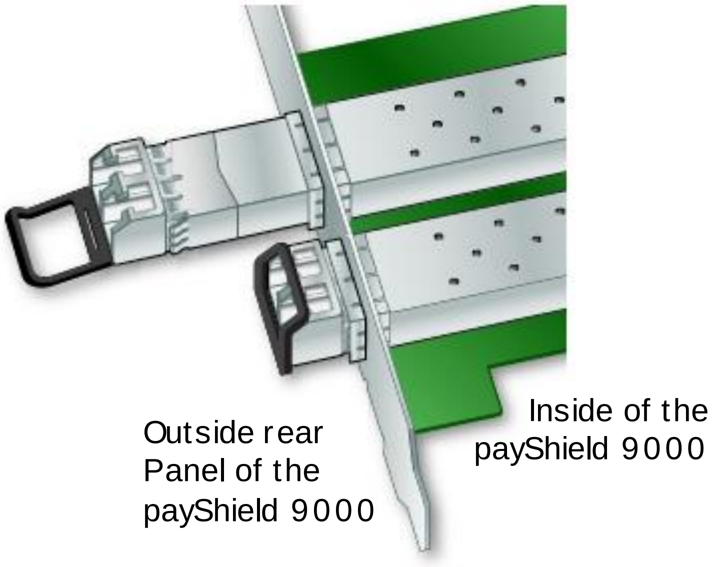

Outside rear Panel of the payShield 9000
Inside of the payShield 9000

Figure 6 - Partially Extracted FICON Transceiver

3. If a Dust Plug is fitted to the port socket, this can be removed by holding the protruding grip.
4. Store the removed transceiver in an ESD-safe place.
5. Install the new transceiver by sliding it into the housing. When the latch engages, it clicks.
6. Push the bail of the new transceiver back into place.
7. Ensure that a Dust Plug is inserted into any port socket which does not have a transceiver fitted.

Connecting your fiber optic cable

Ensure that the payShield 9000 is disconnected from its electrical power supply and that you are using the appropriate fiber optic cable and connector type as defined in Table 1. Plug the cables connectors into the LC connectors of Port 1:

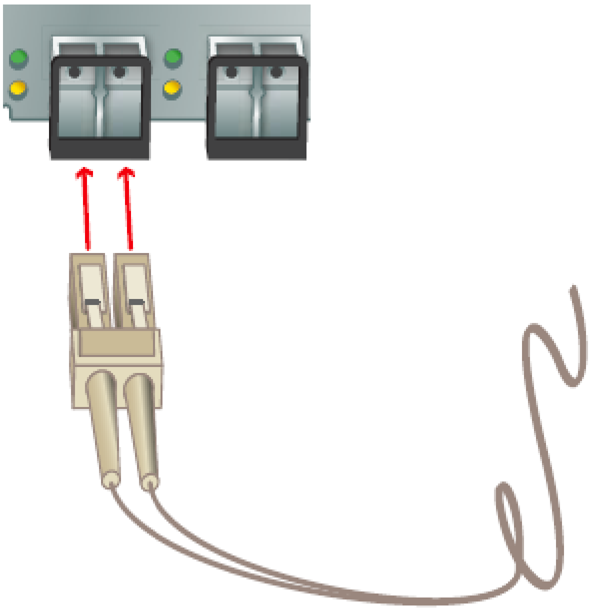


Figure 7 - Connecting the Fiber Optic Cable

Starting the payShield 9000

Connect the payShield 9000 to its electrical power supply.

As shown in Figure 3, the FICON port has 2 LEDs:

- A yellow LED to indicate port activity;
- A green LED to indicate firmware operation.

After the payShield 9000 is powered up/restarted, the FICON interface performs a Power On Self-Test (POST): the results of the POST are presented using the LEDs as shown in Table 3.

Yellow LED	Green LED	Interpretation
●	●	Failure on wake-up (FICON board has failed)
🟡	●	Failure during POST (FICON board has failed)
⊗	●	Wake-up failure monitor
⊛	●	Failure during POST
✹	●	POST is in progress
●	🟢	Failure during operation
🟡	🟢	Failure during operation

Yellow LED	Green LED	Interpretation
2 x ❋*	🟢	Connection established at 2 Gbps
3 x ❋*	🟢	Connection established at 4 Gbps
4 x ❋*	🟢	Connection established at 8 Gbps
●	⊗	Normal, but connection not established
⊗	⊗	Off-line for download
❋	⊗	Awaiting Restart, in limited off-line mode
☀	⊗	Test in progress, in limited off-line mode

🟡 🟢	LED permanently lit
●	LED permanently extinguished
☀	LED continuously flashing
⊗ ⊗	LED continuously blinking slowly
❋	LED continuously blinking rapidly
*	Number of rapid blinks, as specified. Repeated after a 1-second pause during which the LED is extinguished. It is important to check the LED pattern for several seconds to make sure that the LED sequence is correctly identified.

Table 3 - LED Indications after Start-up

FICON Diagnostic Test

The FICON board and transceivers can be tested by using the FICONTEST console command. This is described in the *payShield 9000 Console Reference Manual*.

To run FICONTEST you will need the loopback cable provided with your transceiver. The loopback cable has an appearance similar to that shown below.

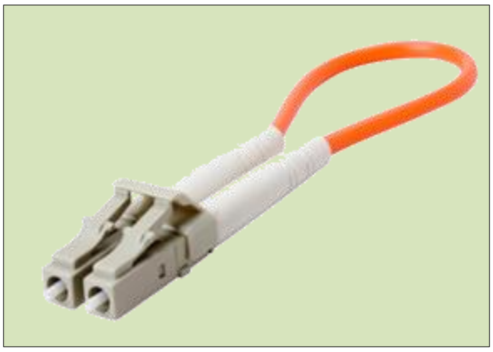


Figure 8 - Typical Loopback Cable

Basic Installation Trouble-shooting

If you are having difficulty in establishing communications between the payShield 9000 and the Host, the following checks should be made. The LED indications described above will assist in identifying issues.

a. If you are cannot get the port into an online state at the switch:

1. Check that the payShield 9000 is in Online state (i.e. both keylocks are in a vertical position).
2. Check that you are using Port 1 of the payShield 9000 FICON interface.
3. Check that you have selected FICON as the Host interface (using the *CH* Console command or payShield Manager), and entered the correct parameters.
4. Check that the optical transceivers in the payShield 9000 and the Host (or switch, etc.) that the HSM is connected to are using the same wavelength. The wavelength (850 nm or 1310nm) used by the payShield 9000 transceiver is printed on the transceiver’s label.
5. Check that the fiber optic cable being used is compatible with the transceiver – see *Specification of the Host Bus Adapter (HBA)*
6. Check that the transceiver at the Host, switch, etc. supports at least one of the speed options supported by the payShield 9000 transceiver – 2, 4, or 8 Gbps. Other speeds (e.g. 1 Gbps) will not work.
7. Check that the FICON interface is operating on the payShield 9000 by connecting a loopback cable between the connectors on the transceiver. The green LED should light up permanently, and the yellow LED should blink 4 times repeatedly. Run the FICONTEST Console command – see the *payShield 9000 Console Reference Manual*.
8. If using a switched fabric, check that the connecting switch has the connecting port type set to fabric port (F_port), auto-negotiation.

b. If the port is online at the switch, but you cannot get paths or the device online:

9. Check security or firmware issues with the switch. Some switches can be configured such that they will only allow a specific port to talk to a specific world-wide port name (WWPN). Some switches have been reported as having firmware issues which cause the same problem: once a given device with a WWPN is plugged into the switch it will not talk to any other WWPN and shuts down, and the switch has to be re-booted.
10. Check the domain ID in the IOGEN at then Host. (If other devices on other control units for the same CHPID and switch are working, then the domain ID is not incorrect.)
11. If the switch has a port offset, check that this has been used in the IOGEN for the control unit switch port, and has been entered in Hex.
12. Check for correct zoning.
13. Check that the device type for the payShield 9000 has been set up as 3490 or Dummy.
14. Check that the Control Unit Image set up at the HSM (e.g. using the CH Console command) matches the Control Unit Image in the IOGEN.
15. Check that the range of Unit Addresses set up at the HSM (i.e. the 16 starting from the specified address) match those in the IOGEN.

Z Series I/O Configuration for FICON-attached payShield 9000

This section discusses how a FICON HSM should be configured for use on a z Series Mainframe, so that it can be used by applications running on an Operating System (usually z/OS) within that Mainframe.

This section is presented in four parts:

1. Relationship between the payShield 9000 configuration and the I/O Definition shows which parts of the I/O Definition need to match the HSM configuration, in order for the device to be accessible.
2. Relationship between the I/O Definition and the application shows how the application can address the HSM, specifically each of the logical devices provided by the HSM.
3. Relationship between the I/O Definition and the SRM Configuration demonstrates this relationship, using the z/OS SRM application as an example. (The SRM, or Security Resource Manager, is an optional software product from Thales which can more effectively manage estates of payShield 9000 HSMs attached to IBM mainframes.)
4. The example presents the specifications required to correctly configure a slightly more complicated example, where two HSM devices were attached to one z Series Mainframe and used by two different Operating Systems running on that Mainframe.

Note that the description and the example present standard configurations. Some users will require more complicated configurations, for example to allow the HSM to be shared between multiple Operating Systems. Specifying this for an HSM, is achieved in the same way as any similarly attached device, by adjusting the I/O Definition appropriately. So by reviewing the information presented here, users will have enough knowledge to configure the HSM in the way that they require.

Relationship between the HSM Configuration and the I/O Definition

z Series Mainframes see a FICON connected HSM as a Control Unit with associated logical devices. Like any such device, to configure this for use in a z Series Mainframe the I/O definition must be updated to:

- Define paths to the Control Unit
- Define the associated logical devices, which the executing operating system will reference.

Paths to the Control Unit are specific to each installation and have no impact on the actual configuration of the HSM device.

By contrast, the Control Unit specification included in the I/O Definition and the HSM configuration must match. Specifically the Control Unit Address must match the Control Image specification and the Unit addresses must match the Control Unit Address. This relationship is shown in the following.

An example I/O definition for an HSM "control unit" is as follows.

```
CNTLUNIT CUNUMBR=02A0,PATH=(…),UNITADD=((00,16)),UNIT=DUMMY,
              CUADD=00
```

In this case, the Control Unit is at address 0, and the 16 devices are defined starting at 0. Note that you should always define 16 devices and the type of control unit should be specified as DUMMY.

The HSM configuration which matches this I/O Definition is shown below. Note the colours which indicate the values that should match.

```
Message header length: 04
Protocol: FICON
Control Unit Image: 0
Control Unit Address: 0
Missing Interrupt Handler (mih): 0
```

The protocol must be specified as FICON. The header length will vary depending on the application that is using this HSM, note that if the HSM is shared between applications, they must all use the same header length.

Relationship between the I/O Definition and application

In addition to the control unit specification, the I/O Definition will also include the specification of an IODEVICE, which specifies how the Operating System will address and use the device. The IODEVICE specification also ties back to the Control Unit specification.

Here is a sample IODEVICE specification:

```
IODEVICE ADDRESS=(02A0,16),CUNUMBR=(02A0),UNIT=DUMMY,UNITADD=00
```

The most important part is the Address and the number that follows this address. In this case, the HSM device will be known to the Operating System as device 02A0 – 02AF. These 16 devices can be bought online and used individually as though they were distinct devices. However they are all managed by the one HSM unit. If that HSM unit is powered down, or disconnected, all 16 devices will fail at that time.

Other parts of the IODEVICE specification relate back to our previous Control Unit specification. Firstly the associated Control Unit is specified by the CUMNUMBER (in this case 02A0). The UNITADD matches back to the similarly named parameter on the Control Unit specification, and the quantity of devices specified (16) matches back to that specified in the UNITADD parameter on the Control Unit specification too.

Relationship between the IO Definition and the SRM Configuration

SRM is an example of an application that can use FICON connected HSM devices from within the z/OS Operating system.

Using the IODEVICE specification presented previously, the z/OS system will provide access to devices using the following addresses: 02A0 – 02AF.

SRM will use as many or as few of these as are configured. Configuration of these devices is managed using two HSM statements, as the following sample shows:

```
HSSLOAD TASK=HSMD0003,PROG=HSSHSMD
* … other statements may separate these two
HSSDEVCE TASK=HSMD0003,…,DEV=02A3,…
```

The HSSLOAD statement specifies the program to be used to support this HSM device – in this case it is HSSHSMD, which is the program used to manage channel attached devices.

The HSSDEVCE statement tells the program how to find the specific device that it is talking to. In this case, the address is 02A3. This is within the range specified on the IODEVICE I/O definition statement.

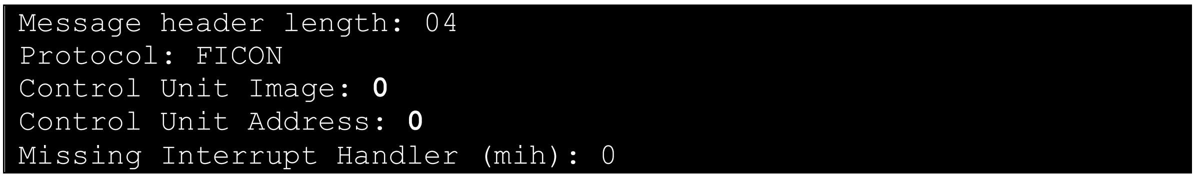
Example: Dedicated HSM per LPAR

This is probably the simplest configuration. Here there are two LPARS and two HSMs, and the HSM devices are not shared by the LPARS.

The following is an Example I/O Definition for this configuration. Only relevant statements are included:

```
 CHPID PCHID=141,PATH=(CSS(1),80),TYPE=FC,SHARED
 CHPID PCHID=151,PATH=(CSS(1),81),TYPE=FC,SHARED
*
*    --- HSM CU for both HOSTs ---
 CNTLUNIT CUNUMBR=0210,PATH=(80),UNITADD=((00,16)),UNIT=DUMMY,+
               CUADD=0
 CNTLUNIT CUNUMBR=0220,PATH=(81),UNITADD=((00,16)),UNIT=DUMMY,+
               CUADD=0
*
*    --- HSM IODEVICE for host SY07 ---
 IODEVICE ADDRESS=(0210,16),CUNUMBR=(0210),UNIT=DUMMY,UNITADD=00,
               PART=((CSS(1),SY07))

*    --- HSM IODEVICE for host SY71 ---
 IODEVICE ADDRESS=(0220,16),CUNUMBR=(0220),UNIT=DUMMY,UNITADD=00,
               PART=((CSS(1),SY71))
```

With this configuration, both HSMs will be specified with Control Unit Image and Control Unit Address of 0, as follows:



```
Message header length: 04
Protocol: FICON
Control Unit Image: 0
Control Unit Address: 0
Missing Interrupt Handler (mih): 0
```

The Operating System on SY07 will use the address 0210 to 021F. The Operating System on SY71 will use 0220 to 022F.

Appendix C – Installing Software and Licenses

This appendix describes the process of updating the software and license files of the payShield 9000 Hardware Security Module.

When a payShield 9000 is delivered from the factory it has the appropriate software and licenses already installed, and so the user will not need to load these prior to using the HSM.

However, software and/or licenses will need to be installed by the user if updated software is acquired or additional licenses are purchased. The required files will be delivered by download from the Thales Support site or on CD, depending on what has been ordered.

Note for payShield Manager users: the payShield Manager product includes a feature to load software and licenses onto the payShield 9000. It is recommended that on payShield 9000s running software v3 and later, users use payShield Manager to upgrade the software or license on their HSM: instructions are provided in the *payShield Manager User Guide*.

⚠ **ATTENTION**

If the payShield 9000 is currently running software v2.2 or earlier, please follow the steps below in order to ensure that a software upgrade via FTP is completed successfully.

1. **Erase the Audit Log.** This can be achieved using the CLEARAUDIT console command.
2. **Erase the Error Log.** This can be achieved using the CLEARERR console command.
3. **Power cycle the HSM.** Remove power, wait for approximately 10 seconds, and then reapply power.
4. Follow the *Standard Update Procedure* as described in the next section.

Standard Update Procedure

Note: See ATTENTION box on previous page when upgrading from v2.2 or earlier.

The payShield 9000 software and/or license can be updated using an FTP connection over TCP/IP on the HSM's Management Ethernet port. The Management port's configuration can be viewed and changed via the Console's *CM* (Configure Management) command.

In order to update the HSM's software or license, you must use an FTP client, which is typically either:

- A command line utility (often included with a PC's Operating System)
- A graphical utility (generally available)

Although they employ different user interfaces, they both require the same information:

Parameter	Value
HSM's Management port's IP address	xxx.xxx.xxx.xxx
FTP account name	anonymous
FTP account password	<blank>
Software file	xxxxx.tkp ***or*** xxxxx.tki *
License file	xxxxx.licence

* Files with a .psp extension which have been provided as part of the delivered software are not required when you use this standard update procedure. They are required for the alternative method described later in this document.

Additionally, the HSM must be in the Secure state before the FTP process starts.

Once the transfer is complete, the HSM immediately moves any uploaded file(s), so they will not appear on the HSM, and processes the uploaded file (and flashes the front panel Management LED various colours to indicate progress). Valid license files are applied immediately. Valid software files result in the HSM automatically restarting in order to complete the update process.

IMPORTANT NOTE: software updates can take several minutes to complete after the file has been transferred to the HSM: please wait for the Management LED to stop flashing and the HSM to automatically restart before using. If any actions are taken before this the application may be corrupted resulting in the HSM becoming unserviceable.

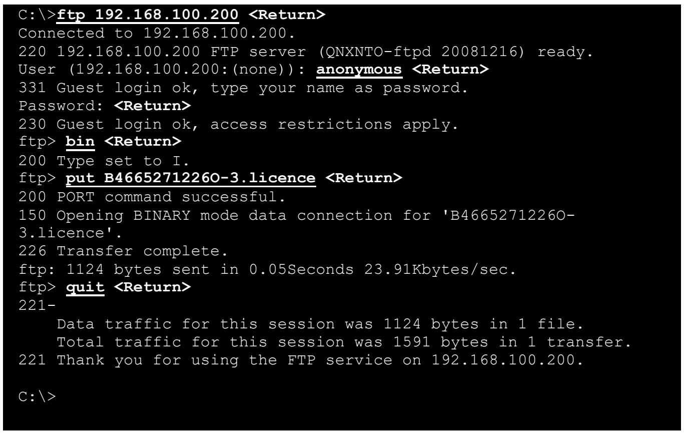
Retention of LMKs

LMKs which are installed on the payShield 9000 before the software update will still be in place after the software update except for the following case:

Where version 1 software is being updated to another major release (i.e. v**1**.x is updated to v**2**.y, v**3**.z, etc.) then the LMKs will be erased.

Example – Command Line FTP Client

1. Start the FTP client in the folder containing the files to be uploaded, and specify the HSM's management port's IP address as a parameter.
   E.g. "`ftp <address>`"
2. Use "anonymous" as the username, and leave the password blank.
3. Type "`bin`" to switch to binary transfer mode.
4. Type "`put`" followed by the name of the file to be transferred. You should use the delivered file with an extension of "`.tkp`" or "`.tki`" if loading software, or with an extension of .licence" if loading a license.
5. Type "`quit`" to exit the utility when the transfer is complete.
6. Software updates can take several minutes to complete after the file has been transferred to the HSM: ***to prevent corruption of the application and the HSM becoming unserviceable it is important to wait for the Management LED to stop flashing and the HSM to automatically restart before using the HSM.***



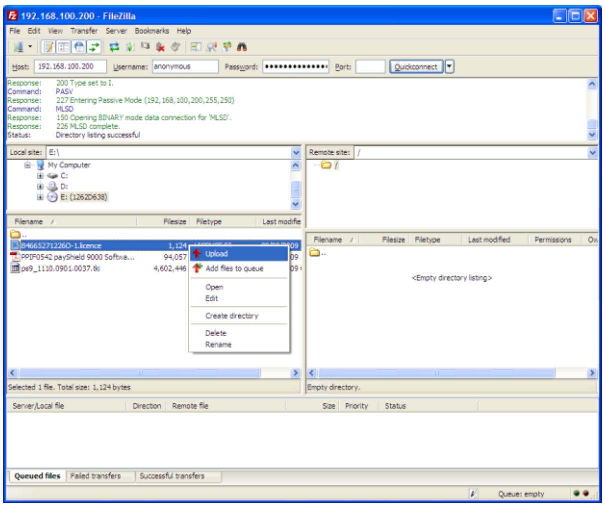
```
C:\>ftp 192.168.100.200 <Return>
Connected to 192.168.100.200.
220 192.168.100.200 FTP server (QNXNTO-ftpd 20081216) ready.
User (192.168.100.200:(none)): anonymous <Return>
331 Guest login ok, type your name as password.
Password: <Return>
230 Guest login ok, access restrictions apply.
ftp> bin <Return>
200 Type set to I.
ftp> put B46652712260-3.licence <Return>
200 PORT command successful.
150 Opening BINARY mode data connection for 'B46652712260-
3.licence'.
226 Transfer complete.
ftp: 1124 bytes sent in 0.05Seconds 23.91Kbytes/sec.
ftp> quit <Return>
221-
    Data traffic for this session was 1124 bytes in 1 file.
    Total traffic for this session was 1591 bytes in 1 transfer.
221 Thank you for using the FTP service on 192.168.100.200.

C:\>
```

The example above shows a licence file (B46652712260-3.licence) being uploaded into an HSM at address 192.168.100.200.

(*Note: some FTP clients require that leading zeroes in the address segments are suppressed, e.g. an address should be entered as 192.168.3.4 rather than 192.168.003.004*.)

Example – Graphical FTP Client

1. Start the graphical FTP client, and (depending on specific client) enter details to identify the host (i.e. the HSM's Management port's IP address).
2. Use "anonymous" as the username, leave the password blank.
3. Select the folder containing the file(s) to be uploaded.
4. Select the file(s) to be uploaded, and start the upload process.
5. Exit the application when the transfer is complete.
6. Software updates can take several minutes to complete after the file has been transferred to the HSM: ***to prevent corruption of the application and the HSM becoming unserviceable it is important to wait for the Management LED to stop flashing and the HSM to automatically restart before using the HSM.***



Host: 192.168.100.200 Username: anonymous Password: •••••••••••••• Port:

```
Response:   200 Type set to I.
Command:    PASV
Response:   227 Entering Passive Mode (192,168,100,200,255,250)
Command:    MLSD
Response:   150 Opening BINARY mode data connection for 'MLSD'.
Response:   226 MLSD complete.
Status:     Directory listing successful
```

Local site: E:\

- My Computer
  - C:
  - D:
  - E: (1262D638)

Filename	Filesize	Filetype	Last modifie
..			
B46652712260-1.licence	1,124		
PPIF0542 payShield 9000 Softwa...	94,057		
ps9_1110.0901.0037.tki	4,602,446		

Selected 1 file. Total size: 1,124 bytes

Remote site: /

Filename	Filesize	Filetype	Last modified	Permissions	Ow
..					

<Empty directory listing>

Empty directory.

Server/Local file	Direction	Remote file	Size	Priority	Status

Queue: empty

The example above shows a licence file (B46652712260-3.licence) being uploaded into an HSM at address 192.168.100.200.

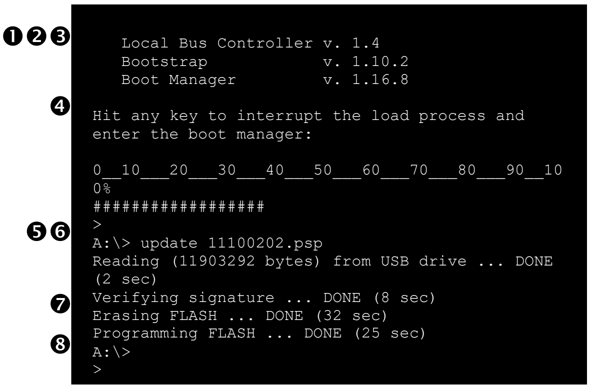
Alternative Update Procedure

Customers may use the following alternative method of loading new firmware into the unit - for example, if the standard (FTP) update procedure fails, or the payShield 9000 becomes unresponsive (even after power cycling). Licenses cannot be loaded using this procedure.

Caution: This method will cause all sensitive data to be erased, including (if present) LMK(s) and remote management data.

This alternative method uses a regular USB flash drive to transfer the new firmware file into the payShield 9000. However, please note the following:

- Firmware files loaded via USB are different to firmware files loaded via FTP. The USB method uses a firmware file with extension ".psp"*.
- This alternative method cannot be used to load licenses into the payShield 9000 unit. All licence files must be loaded into the unit via the FTP procedure, described in the previous section.
- Standard single-purpose USB memory sticks should be used rather than multifunctional devices with USB memory capability.



```
    Local Bus Controller v. 1.4
    Bootstrap            v. 1.10.2
    Boot Manager         v. 1.16.8

Hit any key to interrupt the load process and
enter the boot manager:

0__10___20___30___40___50___60___70___80___90__10
0%
##################
>
A:\> update 11100202.psp
Reading (11903292 bytes) from USB drive ... DONE
(2 sec)
Verifying signature ... DONE (8 sec)
Erasing FLASH ... DONE (32 sec)
Programming FLASH ... DONE (25 sec)
A:\>
>
```

1. Locate the appropriate firmware file from the distribution media (either CD or ZIP file). This should be a single file, with extension ".psp". Copy this file onto the root of the USB flash drive.
2. Establish a terminal connection to the payShield 9000 (using the supplied console cable). Irrespective of the settings for the console port on the HSM, set the communications parameters on your console or terminal emulator to 115200 baud, 8 data bits, 1 stop bit, no parity.
3. Push the (recessed) "Erase" button on the back panel of the payShield 9000. This will automatically cause the HSM to reboot: do not turn the electrical power off/on to cause a reboot.
4. When the prompt "`Hit any key to interrupt the load process and enter the boot manager:`" appears, quickly press, while the extending row of `#` symbols is being displayed, the "↲" (or Enter or Return) key, and you should observe a ">" prompt.
5. Insert the flash drive into one of the payShield 9000's USB sockets. The console prompt should change to "`A:\>`".
6. Type "`update <filename.ext>`" specifying the name of the firmware file on the flash drive.
7. The console will display the following output while the firmware is being updated:
   a. `Reading (XXXX bytes) from USB drive`
   b. `Verifying signature`
   c. `Erasing FLASH`
   d. `Programming FLASH`
8. Once the console prompt returns, remove the flash drive and power-cycle the unit (i.e. disconnect and reconnect the mains electrical supply: do not use the “Reset” button). The new firmware is now installed.

Note: If you changed your console or terminal emulator settings at step 2, will need to return them to those appropriate for the HSM console connection (default: 9600 baud, 8 data bits, 1 stop bit, no parity).

* Files with a .tki or .tkp extension which have been provided as part of the delivered software are not required when you use this alternative update procedure. They are required for the standard method described earlier in this document.

THALES

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

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

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

> cpl.thalesgroup.com <