THALES

payShield® 10K

Release Note - Base Software Version v1.4a

PPRN0559-013

Date: October 2021

Doc. Number: PPRN0559-013, updated 27th October 2021

Contents

1 Introduction

1.1 Summary

This version of the Release Note has been updated to include the following:

> New feature release v1.4a

> Confirmation that software support for PS10-S - payShield 10K Special Edition Hardware Platform is provided in v1.3d and later releases

> Details of v1.4a deployment version 1.8.1 which is deployment version 1.8.0 with 2 additional fixes only

The following general information is included:

> Summary of software version numbers

> Information on PCI HSM v3 Compliance

> How to download and install the software

The details provided for each release are:

> Version Details

> PCI HSM Compliance

> Manuals to be used

> payShield Manager compatibility Information

> New functions provided

> Known Issues

> Bugs and errors corrected

The update to the Release Note on October 1st confirms the Hosted HSM End User Guide is now available via the account manager instead of the support portal - see page 8.

1.2 Latest Software Numbers

> Version 1.4 Development Stream   1500-0030 (v1.4a)   Deployment Version: 1.8.1

> Version 1.3 Development Stream   1500-0029 (v1.3d)   Deployment Version: 1.7.1

> Version 1.2 Development Stream   1500-0024 (v1.2a)   Deployment Version: 1.5.3

> Version 1.1 Development Stream   1500-0023 (v1.1a)   Deployment Version: 1.4.2

> Version 1.0 Development Stream   1500-0022 (v1.0f)   Deployment Version: 1.3.2

1.3 PCI HSM Compliance

Selected versions of payShield 10K from v1.0c onwards will be certified to the PCI HSM v3 requirements. Please note the following:

1. Information is included for each release later in this document to indicate which versions of payShield 10K software are certified to PCI HSM v3.

2. Please note that in order to allow backwards compatibility, some settings are not compliant with PCI HSM. The certified software becomes PCI HSM compliant only when these settings are set as required by PCI HSM.

   As an indicator that all the settings are compliant, the software revision number (accessible using, for example, the payShield Manager Summary Dashboard or the VR Console command) is in the format nnnn-10nn.

If the software revision is shown in the format nnnn-00nn, then some settings are not compliant with PCI HSM.

3. Further information about PCI HSM is included in the payShield 10K Manuals.

1.4   Upgrading Software

Customers with appropriate Thales support contracts can download new software releases from the support portal. Please contact support for further information.

Instructions on upgrading the software are provided in the payShield 10K Installation and User Guide which is also available from Thales support.

2 1500-0030 (v1.4a) – Released Sept 2021

2.1 Summary

This is a general release for all customers.

2.2 Version Details

Base Release:	1.4a	
Revision:	1500-0030	
Deployment Version:	1.8.1 Released October 2021	1.8.0 with 2 additional fixes only
	1.8.0 Released September 2021	Feature Release

2.3 PCI HSM Compliance

This software release is undergoing certification to the PCI HSM V3. Assuming this completes successfully, the software will be listed on the PCI web site at the following location:

https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices?agree=true

2.4 Manuals

The following payShield 10K manuals should be used with this release:

> PUGD0535-010 Installation User Guide
> PUGD0541-005 Host Programmers Manual
> PUGD0537-007 Core Host Commands
> PUGD0538-005 Legacy Host Commands
> PUGD0536-005 Security Operations Manual
> PUGD0539-003 Applications Manual
> 007-000997-003 payShield 10K Console Guide

2.5 payShield Manager

This table indicates the combinations of operating system and browser supported by payShield Manager in this release.

It is possible that other combinations will work, either completely or partially, but this should not be relied upon.

Operating System	Windows 10 64-bit			Linux Ubuntu 18 64-bit		macOS Big Sur
Browser	Chrome 64-bit	Firefox 64-bit	Internet Explorer 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K v1.4a	☑	☑	☑	☑	☑	☑

2.6   New Functions

Deployment Version	Reference	Description
1.8.0	PA-885	Hosted HSM introduces a new capability to payShield to support the deployment of HSMs into Service Provider environments.

This feature is license enabled and provides a new REST API – Out of Band (OOB) Management – to allow a service provider to allocate HSMs, and perform limited device management. With the Hosted HSM license enabled, the HSM can transition from Data Centre to Allocated, and finally End User state, enforcing role separation between the Service Provider and End User.

Once allocated, a customer is able to fully manage the device through payShield Manager in the same way as their on-premises HSMs.

Some of the key differences between a hosted payShield and an on-prem (or non-hosted) payShield include:

- Service provider has no access to customer or end user data (key material, logs, settings, etc.)
- Physical keylocks are completely decoupled from Online/Offline/Secure states
- Position of the physical keylocks do not impact payShield Manager and payment services
- End user can only use the payShield Manager to switch application states between Online/Offline/Secure
- Very limited set of commands are allowed at the local console (see later section for allowed command list)
- Aux interface is not available to the end user
- Service provider has a separate audit log and is completely independent of the end user audit log
- Service provider has no access to error log while the device is in use by end user
- In case of a medium tamper, unlike on-prem payShield, customer will not be able to use HRK recovery mechanism to recover a payShield that was previously tampered. Encrypted logs can be retrieved via the service provider.

Please see the Hosted HSM End User Guide (available via your account manager) for more information. |

2.7   Known Issues

Deployment Version	Reference	Description
1.8.0 & 1.8.1	PA-236	When using payShield Manager and selecting the "Get More" button in the Status Tab in the drop down list for the error log, no additional information is displayed. The work around is to use the "ERRLOG" Console Command in the payShield Manager Virtual Console.
	PA-7446	When using Payshield Manager with Internet Explorer, the error "Incompatible smart card terminal" is displayed. Selecting RUN CONTROL allows connection.

2.8   Bugs and Errors Corrected

Deployment Version	Reference	Description
1.8.1	PA-10064	Hosted HSM Out of Band (OOB) REST API returning 'Undefined' for the provisioning state. This has been fixed in this release.
1.8.1	PA-9876	Hosted HSM Out of Band (OOB) REST API now supports an LMK override of 1 in addition to 2, 5, 10 and 20.
1.8.0	PA-8384	The following security vulnerabilities in OpenSSL have been addressed by upgrading to OpenSSL 1.1.1k: • CVE-2021-3449
	PA-5157 PA-3170	The Security Setting "Enforce minimum key strength of 2048-bits for RSA?" when set to "Yes" prevented a number of valid operations that can be undertaken with an RSA key length less than 2048-bits. This has now been fixed. If enabled, the HSM will not permit RSA operations (signing, generation, encryption, decryption) using a key smaller than 2048 bits. Enforcement is now only provided for PCI payment brand relevant transactions and so does not apply to host commands used for Card and Mobile Issuance, Multos and OBKM as well as the Australian Commands and WebPIN Commands. Only the following host commands are now impacted by this security setting: • ES Validate a Certificate and Import the Public Key – only the CA RSA Public Key must be 2048 bits or greater. • GI Import Key or data under an RSA Public Key • GK Export Key under an RSA Public Key – only the RSA Public Key in the request in the command must be 2048 bits or greater. • QE Generate a Certificate Request

Deployment Version	Reference	Description
		• EW Generate an RSA Signature • JW Build a JSON Web Token. • JY Decode a JSON Web Token. • EY Validate an RSA Signature • AQ Translate an RSA-encrypted PIN to a ZPK/TPK-encrypted PIN • B8 TR-34 Key Export

1.8.0	PA-8518
	PA-8519
	PA-8529
	PA-8530
	PA-8531
		Host commands 'CA' (Translate a PIN from TPK to ZPK/BDK Encryption), 'CC' (Translate a PIN from One ZPK to Another) and 'G0' (Translate a PIN from BDK to BDK or ZPK Encryption) have been updated to address a number of issues reported with the translation operations when using PIN Block ISO Format 4. Included in the updates are the following:
		
		• Host Commands CA, CC and G0 now give error 23 in all cases if the following conditions are not met:
		    o AES PIN encryption keys can only be used with PIN Block ISO Format 4.
		    o 3DES PIN encryption keys cannot be used with PIN Block ISO Format 4.

	PA-2463	The following issue has been addressed with Host Command 'A4' (Form a Key from Encrypted Components): • payShield 10K closed the connection when processing the command when using an AES KeyBlock LMK
	PA-6568	The following update has been made for Host Command 'GK' (Export Key under an RSA Public Key): • Authorized mode is now correctly required to export the TMK, as specified in the Key Type Table
	PA-7231	The following issue has been addressed with Host Commands 'A6' (Import a Key) and 'A8' (Export a Key) • Authorized mode is now correctly required to export the TMK, as specified in the Key Type Table
	PA-8205	A fix is included for Host Commands 'P6' (Load OPINPad to HSM Memory) and 'P8' (Decode OPIN and translate to ZPK) to address an issue with access to the PADid stored in memory.
	PA-5368	payShield Manager now allows text to be copied and pasted when using the Virtual Console
	PA-6139	payshield Manager now allows Key Usage code 22 (ZEK) to be authorized for import or export when using an AES Key Block LMK.

Deployment Version	Reference	Description
	PA-8250	Continued use of Console Commands using the Virtual Console on payShield Manager caused the Virtual Console response to slow down when using v1.2a or above software. This is fixed in this release.
1.8.0	Various	payShield 10K Manuals have been updated for this release as follows: • The Installation and User Guide has new sections on Fraud Detection, Secure Host Comms, Utilization Data, Health Check Data and the Audit Log. • The Core Host Commands Manual includes a number of updates, corrections and clarifications, including updates to host commands 'CA', 'CC' and 'G0'. • The Host Programmer's Manual includes a number of updates and corrections including updates to the PIN Block information provided in Chapters 16 and 18. • The Security Operations Manual also includes a small number of corrections to the descriptions of the Security Settings.

3 1500-0029 (v1.3d) – Released August 2021

3.1 Summary

This is a general release for all customers.

3.2 Version Details

Base Release: 1.3d
Revision: 1500-0029
Deployment Version: 1.7.1 Released August 2021   Maintenance Release

3.3 PCI HSM Compliance

Note this release is **not** planned to undergo certification to PCI HSM V3.

3.4 Manuals

The following payShield 10K manuals should be used with this release:

> PUGD0535-007 Installation User Guide
> PUGD0541-005 Host Programmer's
> PUGD0537-005 Core Host Commands
> PUGD0538-005 Legacy Host Commands
> PUGD0536-004 Security Manual
> PUGD0539-003 Applications Manual
> 007-000997-002 payShield 10K Console Guide

3.5 payShield Manager

This table indicates the combinations of operating system and browser supported by payShield Manager in this release.

It is possible that other combinations will work, either completely or partially, but this should not be relied upon.

Operating System	Windows 10 64-bit			Linux Ubuntu 18 64-bit		macOS Big Sur
Browser	Chrome 64-bit	Firefox 64-bit	Internet Explorer 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K v1.3d	☑	☑	☑	☑	☑	☑

3.6 New Functions

Deployment Version	Reference	Description
1.8.0	NA	PS10-S - payShield 10K Special Edition Hardware Platform is a new variant of the standard payShield 10K hardware platform supporting the following performance levels only: • 25, 60 and 250 cps For further information, please contact your account manager.

3.7 Known Issues

Deployment Version	Reference	Description
1.7.1	PA-5157	The Security Setting "Enforce minimum key strength of 2048-bits for RSA?" when set to "Yes" prevents a number of valid operations that can be undertaken with an RSA key length less than 2048-bits.
	PA-236	When using payShield Manager and selecting the "Get More" button in the Status Tab in the drop down list for the error log, no additional information is displayed. The work around is to use the "ERRLOG" Console Command in the payShield Manager Virtual Console.
	PA-7446	When using Payshield Manager with Internet Explorer, the error "Incompatible smart card terminal" is displayed. Selecting RUN CONTROL allows connection.

3.8 Bugs and Errors Corrected

Deployment Version	Reference	Description
1.7.1	PA-8995 PA-9025 PA-9596	Improved error handling and increased entropy redundancy for the random number generator.
	PA-4037	For all customers using "UTILSTATS" to monitor the command utilisation statistics, the following issue has been resolved in this release: • Once the total transaction value reaches the maximum value of 4,294,967,295 you may experience performance problems with the HSM. The following workaround must be used for previous releases:

Deployment Version	Reference	Description
		• It is recommended to clear the UTILSTATS before the above value is reached. This can be achieved by using the UTILSTATS console command to the view the values and then selecting Y to the "RESET ALL STATS option. This can be done while the HSM is online. Please also see the UTILSTATS command in the payShield 10K Console Manual.
	PA-7444	When using the 'VR' Console Command to view the software revision number and other details, the ECC algorithm is now shown.

4 1500-0026 (v1.3b) – Released June 2021

4.1 Summary

This is a general release for all customers.

4.2 PCI HSM Compliance

Please note this release is now **not** planned to undergo certification to PCI HSM V3.

4.3 Version Details

Base Release: 1.3b
Revision: 1500-0026
Deployment Versions: 1.6.2 Released July 2021   1.6.1 with 3 additional fixes only
                       1.6.1 Released June 2021   Feature Release

4.4 Manuals

The following payShield 10K manuals should be used with this release:

> PUGD0535-007 Installation User Guide
> PUGD0541-004 Host Programmer's
> PUGD0537-005 Core Host Commands
> PUGD0538-005 Legacy Host Commands
> PUGD0536-004 Security Manual
> PUGD0539-003 Applications Manual
> 007-000997-001 payShield 10K Console Guide

4.5 payShield Manager

This table indicates the combinations of operating system and browser supported by payShield Manager in this release.

It is possible that other combinations will work, either completely or partially, but this should not be relied upon.

Operating System	Windows 10 64-bit			Linux Ubuntu 18 64-bit		macOS Big Sur
Browser	Chrome 64-bit	Firefox 64-bit	Internet Explorer 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K v1.3b	☑	☑	☑	☑	☑	☑

4.6　　New Functions

Deployment Version	Reference	Description
1.6.1	PA-71	PS10-F payShield 10K FICON is a new variant of the standard payShield 10K hardware platform supporting the FICON host interface. This is supported in base software version v1.3a and above. The product provides a port for connection to an IBM mainframe host computer to allow host commands and responses to be transmitted using a FICON fiber optic interface. Note: • Two physical FICON ports are provided, but only one port is supported by software. • The FICON transceiver provided by Thales must be ordered for compatibility reasons – options are provided for short wave and long wave transceivers. • PS10-PRM-X Premium package is the **only** package and performance licence available for payShield 10K FICON and must be ordered with the product. • payShield 10K FICON can be configured to use either the FICON host port or the standard Ethernet host ports – simultaneous use of the FICON and Ethernet host ports is **not** supported. • The Ethernet Management and Auxiliary ports can be used when the host port is configured to use either the FICON host port or the Ethernet host ports. • The FICON interface is integrated into the HSM's application software, and the Utilization and Health Check reporting facilities will report on the FICON interface. Further information is provided in the latest payShield 10K Installation & User Guide. Note this functionality is also included in v1.3a which is for restricted distribution.

4.7　Known Issues

Deployment Version	Reference	Description
1.6.1 & 1.6.2	PA-5157	The Security Setting "Enforce minimum key strength of 2048-bits for RSA?" when set to "Yes" prevents a number of valid operations that can be undertaken with an RSA key length less than 2048-bits.
	PA-236	When using payShield Manager and selecting the "Get More" button in the Status Tab in the drop down list for the error log, no additional information is displayed. The work around is to use the "ERRLOG" Console Command in the payShield Manager Virtual Console.
	PA-7444	When using the 'VR' Console Command to view the software revision number and other details, the ECC algorithm is not shown.
	PA-7446	When using Payshield Manager with Internet Explorer, the error "Incompatible smart card terminal" is displayed. Selecting RUN CONTROL allows connection.

4.8　Bugs and Errors Corrected

Deployment Version	Reference	Description
1.6.2	PA-9063	The following issue is found **only** in v1.3b deployment version 1.6.1 - this has been fixed in this release: • after installing v1.3b deployment version 1.6.1, using the erase button on the rear of payShield 10K to erase keys, the unit freezes after rebooting. • the workaround is to install v1.3b deployment version 1.6.2 or v1.2a – please contact support for assistance.
	PA-9018 PA-9080	The following issues in earlier releases have been fixed to improve the error handling for the Solid State Drive (SSD): • A check and recovery mechanism has been added to ensure the health of the SSD partitions before they are mounted. • Failure of factory reset if a severe error is found in the format of the Solid State Drive (SSD) when using v1.2a Deployment Version 1.5.3. If file operation errors are shown in the Error Log, it is strongly recommended to upgrade to this or a later release that includes this fix.

Deployment Version	Reference	Description
1.6.1	PA-8363	The following issue found **only** in v1.3a has been fixed in v1.3b: • When v1.3a has been installed on payShield payShield 10K and has subsequently been downgraded from v1.3a to an earlier release, a **Factory Reset should not be used with the earlier release**. • This issue will **not** occur if v1.3a has **not** been installed. • If v1.3a has been installed, upgrade to v1.3b to solve this issue. Once this is done, a downgrade to all earlier releases except v1.3a can be performed.
	PA-8274	The following security vulnerabilities in OpenSSL have been addressed in an OpenSSL patch: • OpenSSL CVE-3449 and CVE-3450

5 1500-0025 (v1.3a) – Released for Restricted Distribution April 2021

5.1 Summary

Please note this software release is intended for specific customers that require the fixes included only – it is not for general release. All other customers should continue with v1.2a or use a later release.

Note also this release is not planned to undergo certification to PCI HSM V3.

5.2 Version Details

Base Release: 1.3a

Revision: 1500-0025

Deployment Version: 1.6.0 Released April 2021   Maintenance Release - Restricted

5.3 Manuals

The following payShield 10K manuals should be used with this release:

> PUGD0535-007 Installation User Guide
> PUGD0541-004 Host Programmer's
> PUGD0537-005 Core Host Commands
> PUGD0538-005 Legacy Host Commands
> PUGD0536-003 Security Manual
> PUGD0539-003 Applications Manual
> 007-000997-001 Rev A payShield 10K Console Guide

5.4 payShield Manager

This table indicates the combinations of operating system and browser supported by payShield Manager in this release.

It is possible that other combinations will work, either completely or partially, but this should not be relied upon.

Operating System	Windows 10 64-bit			Linux Ubuntu 18 64-bit		macOS Big Sur
Browser	Chrome 64-bit	Firefox 64-bit	Internet Explorer 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K v1.3a	☑	☑	☑	☑	☑	☑

5.5   Known Issues

Deployment Version	Reference	Description

1.6.0	PA-8363	The following issue has been found when **downgrading** from v1.3a to an earlier release.
		
		• When payShield 10K has been downgraded from v1.3a to an earlier release, a **Factory Reset should not be used with the earlier release**.
		• After downgrading, if a Factory Reset is required:
		   o payShield 10K should first be upgraded to v1.3a using payShield Manager or the Console in the usual way.
		   o a Factory Reset should then be undertaken with v1.3a loaded.
		   o payShield 10K should then be downgraded using payShield Manager or the Console in the usual way.
		• If payShield 10K is downgraded from v1.3a to and earlier release and a Factory Reset is undertaken with the earlier release, an error is given and payShield Manager can no longer be used. To recover from this error:
		   o The software must be upgraded to v1.3a using the Console with the software provided on USB stick. This requires local access to payShield 10K as **payShield Manager cannot be used** in this case
		   o a Factory Reset should then be undertaken with v1.3a loaded.
		   o payShield 10K should then be downgraded using payShield Manager or the Console in the usual way.
		• If v1.3a has been installed, upgrade to v1.3b to solve this issue. Once this is done, a downgrade to all earlier releases except v1.3a can be performed without problem.

	PA-5157	The Security Setting "Enforce minimum key strength of 2048-bits for RSA?" when set to "Yes" prevents a number of valid operations that can be undertaken with an RSA key length less than 2048-bits.
	PA-236	When using payShield Manager and selecting the "Get More" button in the Status Tab in the drop down list for the error log, no additional information is displayed. The work around is to use the "ERRLOG" Console Command in the payShield Manager Virtual Console.
	PA-7444	When using the 'VR' Console Command to view the software revision number and other details, the ECC algorithm is not shown.
	PA-7446	When using Payshield Manager with Internet Explorer, the error "Incompatible smart card terminal" is displayed. Selecting RUN CONTROL allows connection.

5.6   Bugs and Errors Corrected

Deployment Version	Reference	Description
1.6.0	PA-6579 PA-7651 PA-7567	The following issue has been addressed with Host Command 'CA' (Translate a PIN from TPK to ZPK/BDK (3DES DUKPT) Encryption): • Issue when translating from Thales PIN Block Format 01 to 48 and from PIN Block Format 48 to 01.
	PA-7562 PA-7563 PA-7566	The following 3 issues have been addressed with Host Command 'CC' (Translate a PIN from One ZPK to Another): • Error given when translating PIN Block from encryption under a 3DES ZPK to encryption under an AES ZPK • PIN Block Translation to Encryption Under a ZPK now gives error 23 if the ZPK in not an AES key. • Issue when translating a PIN Block from 48 to ISO Format 01.
	PA-6831 PA-8064	The following 2 issues have been addressed with Host Command 'G0' (Translate a PIN from BDK to BDK or ZPK Encryption): • PIN Block Translation to Encryption Under a ZPK now gives error 23 if the ZPK in not an AES key. • Issue when translating a PIN Block from 48 to ISO Format 01.
	PA-7186	Import of EMV Keys with key usages E0 to E6 will now accept a Mode of Use of 'X' (the key may only be used to derive other keys) as well as 'N' (no special restrictions apply) when using the following commands: • Host Command 'A6' (Import a Key) • Console Command 'IK' (Import Key)
	PA-7869	Entries are now made to the Error Log to inform the user that the log has reached 90%, 95% and 99% of capacity. The entries advise the user to download and clear the Error Log before the capacity is reached in each case. The capacity of the Error Log is now 10,000 entries and another entry is added when the Error Log is full and then no further entries are added.
	PA-8172	payShield 10K Manuals have been updated for this release as follows: • The Console Commands are now covered in a separate manual instead of in an Appendix in the Installation and User Guide. • The description of the 'GK' (Generate LMK Component) Console Command has been corrected to remove the references to the entry of secret values which are not supported in payShield 10K.

6 1500-0024 (v1.2a) – Released Feb 2021

6.1 PCI HSM Compliance

This software release has completed certification to the PCI HSM Version 3 standard.

The software is listed on the PCI web site at the following location:

https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices?agree=true

6.2 Version Details

Base Release:	1.2a	
Revision:	1500-0024	
Deployment Versions:	1.5.3 Released June 2021	1.5.2 with 1 additional fix only
	1.5.2 Released April 2021 for restricted distribution	1.5.1 with 1 additional fix only
	1.5.1 Released February 2021 for custom software only	1.5.0 with 1 additional fix only
	1.5.0 Released February 2021	Feature Release

6.3 Manuals

The following payShield 10K manuals should be used with this release:

> PUGD0535-006 Installation User Guide
> PUGD0541-004 Host Programmer's
> PUGD0537-005 Core Host Commands
> PUGD0538-005 Legacy Host Commands
> PUGD0536-003 Security Manual
> PUGD0539-003 Applications Manual

6.4 payShield Manager

This table indicates which combinations of operating system and browser are supported by payShield Manager in this release.

 It is possible that other combinations will work, either completely or partially, but this should not be relied upon.

Operating System	Windows 10 64-bit			Linux Ubuntu 18 64-bit		macOS Big Sur
Browser	Chrome 64-bit	Firefox 64-bit	Internet Explorer 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K v1.2a	☑	☑	☑	☑	☑	☑

6.5 New Functions

Deployment Version	Reference	Description
1.5.0	PA-70	Support for Elliptic Curve Cryptography (ECC) is introduced in this release. Elliptic Curve Cryptography (ECC) is an asymmetric algorithm that supports Public Key cryptography. It is based on a branch of mathematics called elliptic curve and is an alternative technique to RSA. Functions are provided for: > ECC Key Management: • Key pair generation • Generation of a certificate signing request • Load a private key into User Storage • Import a public key • Translate private and public keys when LMK changed > ECC Signature Functions: • Generate and validate signatures on a message using ECDSA > ECC Key Derivation Functions: • Key Derivation Using Key Agreement: Derives keys using an Elliptic Curve Key Agreement Algorithm (ECKA) providing a secure method of symmetric key exchange between parties. Methods supported are: ▪ either ECKA-EG (El-Gamal) using ephemeral/static keys ▪ or ECKA-DH (Diffie-Hellman) using ephemeral keys only The ECC Prime Curves currently supported for payments are defined in FIPS 186-3 and are as follows: • '00' – P-256 • '01' – P-384 • '02' – P-521 The following host commands now support ECC functionality: • 'FY' – Generate ECC Key Pair (new host command for v1.2a) • 'QE' – Generate Certificate Request • 'EO' – Import Public Key • 'EK' – Load Private Key • 'EM' – Translate a Private Key • 'EU' – Translate a Public Key • 'EW' – Generate Signature

Deployment Version	Reference	Description
		• 'EY' – Validate Signature • 'IG' – Key Derivation Using Key Agreement (new host command for v1.2a). Please note: • Further Information on the support for ECC provided is given in the payShield 10K Host Programmer's Manual and the Core Host Commands Manual. • Performance for the 'FY' and 'IG' host commands in this release are lower than the cps performance rating for the payShield 10K – performance improvements may be provided in a later release • The ECC algorithm is scheduled to be NIST approved later.

6.6 Known Issues

Deployment Version	Reference	Description
1.5.3	PA-9080	The following issue is found **only** in v1.2a deployment version 1.5.3.: The solution to this issue is to upgrade to a release that includes the fix (for example v1.3b deployment version 1.6.3). Please contact support for assistance.
1.5.0	PA-3265	There is a problem when using the payShield 10K Console to ping localhost (127.0.01). The following is returned: 0 packets received and 100% packet loss.
1.5.0	PA-5157	The Security Setting "Enforce minimum key strength of 2048-bits for RSA?" when set to "Yes" prevents a number of valid operations that can be undertaken with an RSA key length less than 2048-bits.
1.5.0	PA-236	When using payShield Manager and selecting the "Get More" button in the Status Tab in the drop down list for the error log, no additional information is displayed. The work around is to use the "ERRLOG" Console Command in the payShield Manager Virtual Console.

Deployment Version	Reference	Description
1.5.0	PA-7444	When using the 'VR' Console Command to view the software revision number and other details, the ECC algorithm is not shown.
1.5.0	PA-7446	When using Payshield Manager with Internet Explorer, the error "Incompatible smart card terminal" is displayed. Selecting RUN CONTROL allows connection.

6.7   Bugs and Errors Corrected

Deployment Version	Reference	Description
1.5.3	PA-9018	The following issues in earlier releases have been fixed to improve the error handling for the Solid State Drive (SSD): • A check and recovery mechanism has been added to ensure the health of the SSD partitions before they are mounted. If file operation errors are shown in the Error Log, it is strongly recommended to upgrade to this or a later release that includes this fix.
1.5.2	PA-4863	payShield 10K was not issuing zero length keep-alive TCP segments. This has been fixed.
1.5.1	PA-7461	Internal problem with custom software builds resolved.
1.5.0	PA-3960	Host Command 'A0' (Generate Keys) is now able to generate an AES key with key usage 'E2' (EMV/Chip card Master Key: Secure Messaging for Integrity - MK-SMI).
	PA-3272	Intermittent failures were occurring when using host command PM which verifies a dynamic CVV/CVC. This has been fixed.
	PA-3405	Fixed issue with the host command to translate encrypted PIN to encrypted alphanumeric PIN (ZK) for WEBPIN which returned error 14.
	PA-3538	Fixed issue with Host Command 'M6' (Generate MAC) which was returning the incorrect CMAC when supplied with an empty message.
	PA-4582	Fixed issue with host command 'IY' (Generate Digitized Card Single Use Keys) which was not operating correctly in EBCDIC mode.

Deployment Version	Reference	Description
	PA-4586	Host command 'CC' (Translating PIN from One ZPK to Another) was failing to translate a PIN Block encrypted using an AES Key to encryption under a TDES ZPK with a PAN length of 15. This has been fixed.
	PA-5164	Fixed issue with generation of an IPEK and export in TR-31 format encrypted under a TMK in host command 'A0'.
	PA-5168	The Korean SEED related host and console commands have been updated to correct an issue found in the implementation of the algorithm.
	PA-5218	Problem with Host Command 'QY' (Generate a Dynamic CVV) fixed when using Key Derivation Method 'B' (EMV 4.1 Book 2 Option B method).
1.5.0	PA-5219	Fixed problem with Host Command 'IC' (Establish Secure Session with Chip Card) when using Secure Channel Method 5 and key scheme 'U' and 'S' and also when using Secure Channel Method 4 and key scheme 'U'.
	PA-6109	Host Command 'GW' (Generate/Verify a MAC (3DES & AES DUKPT) was giving an error when generating a MAC using BDK-2 and the AS2805 MAC Method and verifying using BDK-4. This has been fixed.
	PA-5952	Host Command 'EI' (Generate a Public / Private Key Pair) now correctly allows the key usage of 'N' when using Key Usage '06' and Key Type Indicator '4' (for data encryption/decryption (e.g. TLS/SSL pre master secret)). Host Command 'GI' (Import Key or data under an RSA Public Key) now supports an RSA key with key usage '06' and mode of use 'N'.
	PA-6507	Host Command 'NO' (HSM Status) was responding with '0' instead of '2' when some of the security settings relevant to PCI HSM compliance have non-compliant values but the "Enforce key type 002 separation for PCI HSM compliance" setting is not one of these. This has been fixed.
	PA-6542	An update to Host Command 'QE' (Generate a Certificate Request) has been implemented to place the blank attributes tag in the CSR. Further details are provided in the Core Host Commands Manual.
	PA-5654	Fixed issue with 'AQ' host command (Translate an RSA-encrypted PIN to a ZPK or TPK-encrypted PIN) when being used in a Multiple LMK configuration and the LMK was configured to select the LMK using the port number. In this case, payShield 10K was always using LMK 00 when another LMK was requested.
	PA-4851	The performance ratings for the payShield 10K are expressed in terms of "calls per second" (cps) instead of "transactions per second" (tps) as used with the payShield 9000.

Deployment Version	Reference	Description
		The payShield 10K Console, payShield Manager and Utilstats now correctly use the new term cps in place of tps. This is a change to the way the performance rating is displayed only – this update does not affect the actual performance of payShield 10K in any way. Please note the performance ratings for the payShield 10K in cps are comparable to the payShield 9000 tps rating noting the performance of RSA signature generation and verification is greatly enhanced in the payShield 10K when compared to the payShield 9000.
	PA-6466	Fixed issue when trying to authorize an installed LMK with "Enable multiple authorized activities" setting disabled on payShield Manager - an error was displayed and remote authorization failed for the LMK.
1.5.0	PA-3969	payShield Manager is now prevented from loading settings from smart card when payShield 10K is in PCI compliant mode.
	PA-2192	The virtual console in payShield Manager, did not clear all the contents when the 'Clear' button is selected. This has been fixed.
	PA-4694	Update to the internal Console driver is included to improve stability.
	PA-1424	Console Command 'FK' (Form Key from Components) is now able to import an AES key with key usage 'E2' (EMV/Chip card Master Key: Secure Messaging for Integrity - MK-SMI).
	PA-6476	The JQuery library has been updated to a later version.
	PA-2417 PA-5808	Intermittent failure in reporting information relating to the fans and the power supplies. This has been fixed in this release.
	PA-6298	Information on using payShield Manager with MacOS Catalina has been added to the Installation User Guide.
	Various	payShield 10K Manuals have been updated for this release as follows: • PUGD0537 Core Host Commands V1: Includes information on the new ECC functionality. Support for storage of PINs encrypted under an AES Key Block LMK has been removed. A small number of corrections and updates are also included. • PUGD0541 Host Programmer's: The new information on ECC has been incorporated. The section on User Storage has been updated. A small number of corrections and updates are also included.

Deployment Version	Reference	Description
		• PUGD0535 Installation User Guide: Information on the Trusted Management Device (TMD) has been added. The chapters on payShield Manager have been reorganized.

7 1500-0023 (v1.1a) – Released August 2020

7.1 PCI HSM Compliance

This software release has completed certification to the PCI HSM Version 3 standard.

In addition for this release, payShield Manager has completed certification as a PCI HSM v3 Remote Access Platform (RAP).

https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices?agree=true

7.2 Version Details

Base Release: 1.1a
Revision: 1500-0023
Deployment Versions: 1.4.2 Released June 2021   Maintenance Release
                     1.4.0 Released August 2020   Feature Release

7.3 Manuals

Issue 004 of the payShield 10K manuals should be used with this release.

7.4 New Functions

Deployment Version	Reference	Description
1.4.2	PA-5862	New Console Command QMAC added to show MAC addresses of all network interfaces.
1.4.0	PA-3112	A variant of the standard payShield 10K hardware platform is now available supporting 10G Ethernet. This is supported in base software version v1.1a and above. The new variant is the PS10-D payShield 10K 10G Ethernet Hardware Platform. This can be ordered in place of the standard PS10-S payShield 10K Ethernet Hardware Platform. 10G Ethernet is provided on all four Ethernet ports - Host Port 1, Host Port 2, the Management Port and the Auxiliary Port. Transceivers for connection to either copper or optical networks must also be ordered for each port. As with the standard PS10-S model, a Software Package with Performance must be included in the order together with the Hardware Platform as well as any optional licenses and hardware accessories as required.

Deployment Version	Reference	Description
		Further information is provided in the latest payShield 10K Installation User Guide.
1.4.0	PA-2711	Bancontact manage the standards for the Bancontact debit card used widely in Belgium. To allow import and export of AES session keys in accordance with their specifications, two host new commands (N6 and N8) are provided. These allow import and export of AES session keys and are used for encryption of PINs, cardholder data and to generate and to verify a MAC to protect the integrity of the messages. These host commands require use of an AES Key Block LMK. A Premium Licence is also required to use these commands.
	PA-2716	Updates to the standard DUKPT commands to support an option for the Italian Standard Key Derivation Method are included. The following DUKPT host commands now support the Italian Standard Key Derivation Method when using a key block LMK: • G0, GO, GQ, GS, GU. The following new key type is used with the above commands to specify that the Italian Standard Key Derivation Method is to be used: • BDK-5 with key usage 44. The following host commands used for key management have been updated to support the new key BDK-5: • A0, A6, A8, GK, BW.
	PA-2575 PA-4665	Host Command KY 'Generate Secure Message (EMV 4.x)' has been enhanced to support Visa VIS CVN '18'. Also a correction to this command for Visa VIS CVN '22' is included and this also now correctly supports ISO PIN Format 1.
	PA-3939	payShield Manager now also supports Chrome 80. This required the Thales smart card bridge to support the Chrome 'SameSite' feature.
	PA-2573	The import/export of a ZMK encrypted under another ZMK is now supported in host commands A6 and A8 as well as host command BY. Two Configure Security Settings control the capability (default is OFF): "Enable import of a ZMK under a ZMK? [Y/N]" with a default value of "N". • When set to "Y", the host command A6 and console command IK allow the import of a ZMK under a ZMK. "Enable export of a ZMK under a ZMK? [Y/N]" with a default value of "N". • When set to "Y", the host command A8 and console command KE allow the export of a ZMK under a ZMK.

7.5   Significant Corrections to Functionality

Deployment Version	Reference	Description
1.4.0	PA-4010 PA-4425	A number of host commands have been updated to correct an issue with the support provided for ISO PIN Block Format 4 (Thales PIN Block Format 48). This is the format used to encrypt a PIN Block using the AES cryptographic algorithm. The Host Commands that have been changed in this releases are as follows: • CA - Translate a PIN from TPK to ZPK/BDK (3DES DUKPT) Encryption • CC - Translate a PIN from One ZPK to Another • G0 - Translate a PIN from BDK to BDK or ZPK Encryption (3DES & AES DUKPT) The Host Commands that only required a documentation update in the new manuals for this release are as follows: • BK - Generate an IBM PIN Offset (of a customer selected PIN) • FW - Generate an ABA PVV (of a customer selected PIN) • DU - Verify a PIN & Generate an IBM PIN Offset (of customer selected new PIN) • CU - Verify a PIN & Generate an ABA PVV (of a customer selected PIN) • JE - Translate a PIN from ZPK to LMK Encryption • JC - Translate a PIN from TPK to LMK Encryption • JG - Translate a PIN from LMK to ZPK Encryption • DA - Verify a Terminal PIN Using the IBM Offset Method • EA - Verify an Interchange PIN Using the IBM Offset Method • CG - Verify a Terminal PIN Using the Diebold Method • EG - Verify an Interchange PIN Using the Diebold Method • DC - Verify a Terminal PIN Using the ABA PVV Method • EC - Verify an Interchange PIN Using the ABA PVV Method • BC - Verify a Terminal PIN Using the Comparison Method • BE - Verify an Interchange PIN Using the Comparison Method • KU - Generate Secure Message (EMV 3.1.1) • KY - Generate Secure Message (EMV 4.x) • IY - Generate Digitized Card Single Use Keys Note that all the above host commands are backward compatible with v3.4c for all PIN Block Formats **except** ISO PIN Block Format 4 (Thales PIN Block Format 48). Changes will **only** be required to applications using ISO PIN Block Format 4 in order to include the check digit in the PAN/Token as documented in the Host Command Manual for v3.5a.

7.6   Bugs and Errors Corrected

Deployment Version	Reference	Description
1.4.2	PA-9018 PA-9080	The following issues in earlier releases have been fixed to improve the error handling for the Solid State Drive (SSD): • A check and recovery mechanism has been added to ensure the health of the SSD partitions before they are mounted. • Failure of factory reset if a severe error is found in the format of the Solid State Drive (SSD) when using v1.2a Deployment Version 1.5.3. If file operation errors are shown in the Error Log, it is strongly recommended to upgrade to this or a later release that includes this fix.
1.4.0	PA-1002 PA-4046	Fixed issue with Host Command M4 when translating data from encryption using a 3DES key to an AES key if the data is not 16-byte blocks in size.
	PA-1106	SNMP log type of "Failed to get IP address" log has been changed from an error to a warning. This is because it could mislead customers to believe that the interface did not obtain the DHCP IP address even though the interface may have obtained the IP address at a later time.
	PA-1577	The error has been corrected which is displayed when attempting to install a Null LMK.
	PA-4549	The text displayed when using the VR Console Command has been updated to show the PCI information given on the payShield 10K label.
	PA-4583 PA-2526	Two problems have been fixed when generating and installing a Key Transport Key (KTK) for the legacy Key Management Device (KMD): • A problem with the check value (KCV) has been corrected. When creating a KTK with the KM Console Command with the security setting "RESTRICT KCV to 6 CHARACTERS" set to YES, the individual components are now 6 in length and the KCV is now also 6 in length (previously 16). • A problem when using the Console Command KN to load the KTK components which caused a crash.
	PA-4585 PA-4588 PA-4589 PA-4590	A number of issues have been corrected with host command B8 which is used to export keys in TR-34 format: • The LMK ID was included in the TR-34 key block header in error. This has been corrected. • A problem with the ASN1 encoding was corrected. • The sequence tag length was not included in the digest calculation • The key block parameters at the end of the command were read incorrectly
	PA-4783 PA-4741 PA-4561	When using payShield Manager with Internet Explorer 11 the following three problems have been fixed: • A Web Socket error would pop-up and the session was terminated intermittently.

Deployment Version	Reference	Description
		• When downloading the audit log, the session terminated expectantly. • The 'Configure Commands' option (>Configuration->Configure Command) was not being displayed correctly.
	PA-5188	payShield 10K Core Host Commands Manual: The description of host command to export a key under an RSA public key (GK) has been corrected to include the correct position of the delimiters.
	PA-4256	The audit log printed an incorrect version when the payShield 10K software version is downgraded. This is now fixed.
1.4.0	PA-4462	A fix is included to address a problem whereby the host command to generate keys (A0) gave error 17 when generating an MK key with key usage 90.
	PA-1767	The error message when an attempt to use the CA Console Command to configure the auxiliary port in Online State has been corrected.
	PA-4580	A fix is included to host command G0 which translates a PIN using the DUKPT standard. The problem occurred when the same key is used.
	PA-1422	Host Command KG which is used to validate an Issuer Public Key Certificate gave an incorrect error when using an AES LMK and with the exportability of the key set to sensitive. This has been fixed.
	PA-2835	A number of ports on the host interface have been enabled.
	PA-4150	Fixed a problem with host command GW that generates or verifies a MAC when using DUKPT. The problem occurred if the data provided was not a multiple of 16 bytes.
	PA-4185	When using payShield Manager with Chrome or Internet Explorer and the security setting "Display general information on payShield Manager landing page = YES", the payShield Manager landing page takes a long time to display the Summary, Health and Software & License details. The login with the RACC cards also fail. This has been fixed.
	PA-4983	A fix is included for the problem whereby Authorization is not maintained after a reboot.
	PA-5186	A problem with Console Command GS (Generate Key & Write Components to Smartcard) is fixed and the components are now correctly written to smart card.
	PA-3259	When disabling healthstats data collection using payShield Manager the endtime did not update automatically in the displayed report. This was fixed in v1.1a.

8 1500-0022 (v1.0f) – Released April 2020

8.1 PCI HSM Compliance

This software release has completed certification to the PCI HSM Version 3 standard. The software is listed on the PCI web site at the following location:

https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices?agree=true

8.2 Version Details

Base Release: 1.0f

Revision: 1500-0022

Deployment Version: 1.3.2 Released April 2020   1.3.0 with 1 additional fix only

8.3 Manuals

Installation User Guide will use Issue 004 and all other payShield 10K manuals should use Issue 003 with this release.

8.4 Bugs and Errors Corrected

Reference	Description
PA-4357	Tested and modified RSA Host Commands for 10K (AQ, EI, EK, EM, ES, GI, GK, QE, JW, J0, KO, L8 and L6) so that they work with the Security Setting for RSA key length of 2048 when the setting is as follows: "Enforce minimum key strength of 2048-bits for RSA: YES".

9 1500-0021 (v1.0e) – Released March 2020

9.1 PCI HSM Compliance

This software is not planned to undergo certification to the PCI HSM Version 3 standard.

9.2 Version Details

Base Release: 1.0e

Revision: 1500-0021

Deployment Versions: 1.3.0 Released March 2020   Maintenance Release

9.3 Manuals

Installation User Guide will use Issue 004 and all other payShield 10K manuals should use Issue 003 with this release.

9.4 New Functions

Reference	Description
PA-162	Added Licensing for FF1 algorithm to payShield 10K

9.5 Bugs and Errors Corrected

Reference	Description
PA-1432	Fixed ACL list so it cannot be disabled in the online mode and only in the secure mode
PA-2491	Notarized macOS Bridge with Apple
PA-2496	Modified SNMP for changes with kernel updates as a result of Ethernet interface name changes
PA-2888	Modified VR console command to display ADK version
PA-3382	Updated payShield Manager to return the semantic version
PA-3386	Corrected Upgrade/Downgrade detection
PA-3505	Fixed the inability to load PTI in payshield, when PTI name contains "+"
PA-3539	Corrected 10K Custom App PTI filename
PA-3875	Changed "Base Version" to "Firmware Version"
PA-3968	Updated SNMP to return semantic version

Reference	Description
PA-4186	Fixed HRK recovery fails between 1.0d and 1.0e
PA-4187	Modified payShield Manager to accept '+' symbol in filename while using "Update Software" in payShield Manager
PA-1124	Corrected MAC calculation in KY Host Command
PA-1143	Fixed EW Host Command when returning Error when using 2048 bit RSA keys
PA-1391	Fixed L6 returning error L726
PA-1408	Corrected inability to execute /sbin/ifconfig command because there was not enough memory
PA-1412	Modified Host Command A0 allowing it to generate a key with Algorithm 1 that can be used in the Host Command M0
PA-1417	Fixed problem with importing AES keys using 05 Optional Header
PA-1436	Fixed CS Host Command to work with AES Keys
PA-1564	Fixed a failure with HMAC keys using the Host Command 'L0', with HMAC Key Usages 01 or 02
PA-1570	Fixed error 50 - Invalid CRT component length byte for Host Command I8
PA-3210	Fixed Mode Flag 4 Scheme ID A in Host Command 'KY'
PA-3468	Fixed the M4 Host Command returning M506
PA-1433	Fixed A0 Host Command failing on AES key generation and export
PA-2954	Fixed BW so that translation can be done with a single length PVK w/ KTC 002 from 2DES LMK to AES LMK
PA-1433	Fixed A0 Host Command so that it does not fail on AES key generation and export

10   1500-0020 (v1.0d) – Released Dec 2019

10.1   PCI HSM Compliance

This software release has completed certification to the PCI HSM Version 3 standard. The software is listed on the PCI web site at the following location:

https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices?agree=true

10.2   Version Details

Base Release: 1.0d
Revision: 1500-0026
Deployment Version: 1.2.5 Released December 2019   Feature Release

10.3   Manuals

Issue 002 of the payShield 10K manuals should be used with this release.

10.4   New Functions

Reference	Description
PA-146, 148 and 149	Merge payShield 9K v3.4b and v3.4c into ps10K v1.0d
PA-201	Descriptions of commands for enable and disable configuration were added to payShield Manager.
PA-305	SNMP MIB-2 settings for payShield Manager were updated
PA-801	Messaging for situations where payShield Manager must be commissioned via local console was improved.
PA-918	.CSR from Secure Host communications used SHA1 and now uses SHA-2
PA-2179	Hardware Version now shown in 'VR' command
PA-913	Added verification of audit log integrity after reboot of payShield

10.5   Bugs and Errors Corrected

Reference	Description
PA-2304	Fixed to allow assure that only alphanumeric characters can be used in the console 'CH' network names.
PA-2529	Corrected issue where Host command descriptions in payShield Manager were not shown if command was not enabled.
PA-2544	Fixed "invalid range" for payShield Manager ACL host entry when the IP address of the beginning is greater than the end IP address.
PA-2545	Prevented the entry of duplicate entries for ACL.
PA-750	Fixed rebooting causing under voltage tamper.
PA-836	Corrected issue with DHCP misconfigures on lease renewal.
PA-1011	Corrected issue where security scan produces error.
PA-1207	Corrected memory errors with MyPINpad PIN tables.
PA-1723	Corrected issue where FRU status on payShield Manager health dashboard was delayed in updating.
PA-1725	Corrected issue where boot manager would not attempt to clear tamper during update.
PA-1733	Corrected issue where 'XR' console command could not connect to card.
PA-1734	Added validation on port numbers from payShield Manager.
PA-1739	Corrected issue where Fan controller fails to account for stopped fan.
PA-1741 PA-1757	Corrected issue where UI for payShield Manager does not show FIPS Status
PA-2778	Corrected issue where the 'KY' host command fails with invalid PIN block format codes. Add Support for ISO Pin Format 1 for CVN22
PA-215	Corrected SNMP issue where Fan state shows as OK when the fan is disconnected
PA-243	Corrected issue where payShield Manager does not apply changes to host settings if disabled interface has invalid settings.
PA-638	Corrected issue where 'JL' Host command is missing a flag in the response causing customer to not be able to parse it out.
PA-994	Corrected issue where payShield Manager session was not restoring console access.
PA-1686	Corrected issue where Configuration Host Settings: Enable TLS should be greyed out indicating HSM is not in Secure Mode
PA-1687	Corrected issue where SNMP - agent gets blocked under heavy trap load
PA-1689	Corrected Error "Failed to validate the server's Chain of Trust" while logging into payShield Manager UI

Reference	Description
PA-1690	Corrected issue where payShield Manager login failure keeps console disabled
PA-1694	Corrected issue with payShield Manager and Console mismatch - Secure Host comms vs Host TLS
PA-1695	Corrected issue where payShield Manager negatively impacts host command processing
PA-1696	Corrected issue with 'GI' host command returning A8 error where on the 9000 it returns successful.
PA-1697	Corrected issue where 'IK' console command is not clearing clear data.
PA-1698	Corrected issue in payShield Manager option "User must change PIN on first use" does not work after toggle.
PA-1699	Corrected 'SV' console command requesting invalid user input.
PA-1700	Updated manual for host commands 'CC', 'G0' and 'CI'
PA-1701	Corrected issue where error log entry is added when FAN is inserted due to initial low speed
PA-1703	Corrected issue where setting session timeouts with payShield Manager does not apply to the current session.
PA-1706	Corrected issue with payShield Manager where administrator attempted to log into PSM using an invalid RACC card and it was not recorded in the audit log.
PA-1710	Corrected issue where 'CA' and 'AQ' host commands were not checking appropriate security setting for Tokens in pin operations.
PA-1711	Corrected issue where MIB field payShieldUtilHostCmdVolume description was misleading.
PA-1712	Corrected issue where running Console command 'XR' generates an Audit log entry on HMAC validation.
PA-1714	Corrected issue where payShield Manager fails to refresh properly.
PA-1715	Corrected issue where temperature alarm information needed to be removed from the 'QL' console command.
PA-291	Corrected payShield Manager error message when logging in.
PA-312	Corrected issue where payShield Manager is left in a bad state after changing the IP address on the management port.
PA-334	Corrected issue where payShield Manager does not display any signed certs that are loaded on the payShield.
PA-1168	Corrected issue where MIB2 systems values were cleared after software upgrade.
PA-1369	Corrected issue where payShield Manager hangs and does not complete saving all settings onto the smart card.
PA-1607	Corrected payShield Manager UI on a defect related to showing host command descriptions.

Reference	Description
PA-1755	Corrected a corruption in the error log caused by a console RESET command.
PA-1758	Corrected payShield Manager Information (?) icon for TLS and Secure Host Communications where it did not display relevant information
PA-1762	Corrected to not record and error in the Error Log when modifying security settings are updated successfully.
PA-1763	Corrected to prevent payShield Manager from writing to error logs constantly after cancelled console RESET
PA-1795	Corrected payShield Manager so that it does will display signed certs that are loaded.
PA-1143	Corrected receipt of error A5 with 'EW' host command on 10K using 2048 bit RSA keys
PA-1390	Corrected issue where 'EY' host command fails to verify a No Hash Signature created with 'EW' host command
PA-1423	Corrected issue where host command 'A6' returns authorization failure when using sub category method PA-1764] USB to Serial Driver (93183)
PA-2385	Corrected 'I8' host command, sub command 08, version 3 to return an 8 byte MAC.

11 1500-0010 (v1.0c) – Released April 2019

11.1 PCI HSM Compliance

This software release has completed certification to the PCI HSM Version 3 standard. The software is listed on the PCI web site at the following location:

https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices?agree=true

11.2 Manuals

Issue 001 of the payShield 10K manuals should be used with this release.

11.3 New Functions

The table below describes the list of major new functions introduced in this release:

Reference	Description
Compared to payShield 9000	New payShield Maintenance Light, activated at units front panel or remotely through payShield Manager
	New Secure Console UPLOAD command
	Faster and more reliable software updates
	New High Tamper Feature
	New Self Configuring USBC port for Console
	New (more secure) defaults for security configuration settings, command and PIN configurations
	Larger and more robust Audit Log
	Higher Performance Level

11.4 Bug Fixes and Errors

Reference	Description
PA-799	Fixed error log entries from factory

12   payShield 9000 vs 10K

Function/Feature	payShield 9000	payShield 10K
Form Factor	2U	1U
Power Sockets	x1 or x2 (factory fit option)	X2 Hot Swappable
Power Consumption	100W	60W
Fans	Stationary	X2 Hot Swappable
Ethernet Host Ports	x2 (10/100/1000 Mbps)	x2 (10/100/1000 Mbps)
Management Port	x1 (10/100/1000 Mbps)	x1 (10/100/1000 Mbps)
Ethernet Printer Port	x1 (10/100/1000 Mbps)	x1 (10/100/1000 Mbps)
Console Port	via USB-to-serial cable	USB-C
Async Host Port	via USB-to-serial cable	No Longer Supported
FICON Host Port	Option	PCIe Slot in Hardware Currently not supported in software, but will be added as option.
Serial Printer Port	via USB-to-serial cable	via USB-to-serial cable
Parallel Printer Port	via USB-to- Parallel cable	via USB-to- Parallel cable
Erase Sensitive Data	Recessed Erase button	Recessed Erase button with completion indicator
Reset HSM	Red reset button	Through payShield Manager or power button on rear panel
LMK(s) loaded indicator	LMK LED	None – information in payShield Manager
Host Activity indicator	Host 1 & Host 2 LED	None – information in payShield Manager
Management Activity indicator	Management LED	None
Power supply indicator	Power LED (various colours)	Power LED, rear panel
Unit serial number	Front & rear panel	Front and rear panel
Motion Detector (Sensitivity)	Off/Low/Medium/High	Off/Low/Medium/High
Console Port speed	300…38400 baud	N/A Self Configuring
Async Host Port speed	300…38400 baud	N/A Removed
Serial Printer Port speed	300…38400 baud	300…38400 baud
IP routing	via gateway or static route	via gateway or static route
ROUTE console command	Yes	No
Software Update	via FTP or USB	Secure HTTPS via payShield Manager or Secure 'UPLOAD' console command with USB
Licence Update	via FTP	Secure HTTPS via payShield Manager or Secure 'UPLOAD' console command with USB
Start-up time	~20 seconds	~20 seconds

Function/Feature	payShield 9000	payShield 10K
Maximum performance	1500 tps	2500 cps (calls per second)
PCI HSM certification	Yes PCI HSM Version 1.0 (selected hardware & software versions) Expires end of April 2019	Yes PCI HSM Version 3.0 (Selected software versions)
FIPS Certification	FIPS 140-2, Level 3	Pending FIPS 140-2, Level 3

13 Technical Support Contacts

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

https://supportportal.thalesgroup.com/csm

13 Technical Support Contacts

THALES

Contact us

For all office locations and contact
information, please visit
cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <