payShield® 10K

Release Note - Base Software Version 2.2a

007-001511-022 Rev A4

Date: March 2025

Doc. Number: 007-001511-022 Rev A4

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

Contents

1   Introduction

1.1   Summary

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

> Details of 2.2a deployment version 1.16.1 for general release.

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.

1.2   Latest Software Numbers

> Version 2.2 Development Stream   2200-0000 (v2.2a)   Deployment Version: 1.16.1

> Version 2.1 Development Stream   2100-0001 (v2.1a)   Deployment Version: 1.15.1

> Version 2.0 Development Stream   2000-0020 (v2.0c)   Deployment Version: 1.14.6

> Version 1.9 Development Stream   1500-0039 (v1.9b)   Deployment Version: 1.13.3 (Note 1)

> Version 1.8 Development Stream   1500-0037 (v1.8b)   Deployment Version: 1.12.2

> Version 1.7 Development Stream   1500-0034 (v1.7b)   Deployment Version: 1.11.4

> Version 1.6 Development Stream   1500-0032 (v1.6a)   Deployment Version: 1.10.4

> Version 1.5 Development Stream   1500-0031 (v1.5a)   Deployment Version: 1.9.2

> Version 1.4 Development Stream   1500-0030 (v1.4a)   Deployment Version: 1.8.3

> 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

Please note that because different software versions (e.g., v1.7b and v1.8a) may be in development at the same time, it may be that some fixes and enhancements in the lower-numbered version may not be included in the higher-numbered version.

Note 1: v1.9c and v1.9d are now also available but the contents of these are not included in 2.0c. The contents of 1.9c and 1.9d are included in 2.1a.

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   2200-000x (2.2a) – Released March 2025

2.1   Summary

This is a general release for all customers.

2.2   Version Details

Base Release: 2.2a

Revision: 2200-0000   Deployment Version: 1.16.1   This is a feature release.

2.3   PCI HSM Compliances

This software release is planned to undergo approval to 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 manuals have been updated for use with this release:

> 007-001512-022 Rev A payShield 10K Installation and User Guide
> 007-001518-022 Rev A payShield 10K Host Programmers Manual
> 007-001515-022 Rev A payShield 10K Core Host Commands
> 007-001516-022 Rev A payShield 10K Legacy Host Commands
> 007-001513-022 Rev A payShield 10K Security Operations Manual
> 007-001517-022 Rev A payShield 10K Applications Manual
> 007-000997-022 Rev A payShield 10K Console Guide
> 007-001443-022 Rev A payShield 10K Host Command Examples

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.

Please note that payShield Manager no longer supports Internet Explorer as this is no longer supported by Microsoft.

Operating System	Windows 10 and 11 64-bit			Linux Ubuntu 20 64-bit		macOS Monterey & Ventura
Browser	Chrome 64-bit	Firefox 64-bit	Edge 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K 2.2a	☑	☑	☑	☑	☑	☑

2.6   New Features

Deployment Version	Reference	Description
1.16.1	PA-17964	New host command 'B6' has been added to support import a symmetric key using TR-34 standard. Please note in order to use the new host command the latest license is required - please contact the support team.
	PA-12462	Host Command 'B8' (TR-34 Export) has been updated with a new Scheme 3 to export a Key Block Protection Key (KBPK) using Verifone's proprietary VRKv2 format. This feature is restricted to customers with the appropriate contractual agreement with both Verifone and Thales and requires the optional license PS10-LIC-VRKV2.
	PA19443	Host Commands 'A0' (Generate Key), 'A6' (Import Key) and 'A8' (Export Key) have been updated to support alternative formats for the Timestamp and Key Check Value (KCV) in ANSI X9.143/TR-31 format. The current formats supported are: o Timestamp: YYYY-MM-DDTHH:MM:SSZ o Key Check Value: XXXXXX (6 hex digits) The additional formats supported in this release are: o Timestamp: YYYYMMDDHHMMSSZ o Key Check Value: XXXXXXXXXX (10 hex digits)
	PA-18786	Host Command CA (Translate a PIN from TPK to ZPK/BDK Encryption) has been updated to support AES DUKPT as well as 3DES DUKPT.

Deployment Version	Reference	Description

	PA-19605	Host Command G0 (Translate a PIN from BDK to BDK or ZPK Encryption (3DES & AES DUKPT) has been updated to support derivation of the GBIC "Send" PIN encryption key as part of the PIN translation process.
		
		There has been a new update to the GBIC requirements released earlier in 2024 and customers acting as Network Operators (NSPs) using payShield 10K are required to meet these. The new requirements impact the method used by Network Operators (NSP) to encrypt PIN Blocks as detailed below, noting that the use of a Variant LMK is no longer compliant.
		
		The new method is supported in payShield 10K v2.2a and later releases. A security setting is provided in v2.2a to allow customers to continue using the existing non-compliant method until they are ready to use the new compliant method.
		
		Acquirers: There are no changes required.
		
		Network Operators (NSPs): GBIC now require the Network Operators (NSPs) to derive the key used to encrypt PIN Blocks (PEK/ZPK) from the ZKA in a one step process using an updated version of Host Command 'G0' (Translate PIN from BDK to ZPK). This is in place of the existing method i.e., first deriving the key using Host Command 'A0' (Derive Key) and then translating the PIN Block to encryption under the key using Host Command 'G0'. In more detail:
		
		• The new restrictions are controlled using a security setting which impacts the functionality used by the NSP only.
		
		   o This allows customers to operate in a temporary backward compatible non-compliant mode if required.
		
		   o When the security setting is set for GBIC compliance:
		
		      ▪ Derivation of the key used to encrypt the PIN Block (PEK/ZPK) by the NSP is no longer allowed when using host command 'A0' (Derive Key)
		
		      ▪ There is no change to the functionality the NSP uses to derive the MAC Key (ZAK) or the Data Encryption Key (ZEK).
		
		• The NSP is now required to use an updated version of host command 'G0' (Translate PIN from BDK to ZPK) as follows:
		
		   o The updated 'G0' host command takes the Master Key (ZKA) as input in the 'Destination Key' field and returns the PIN Block encrypted under the PEK/ZPK together with the randomly generated RNDI.

	PA-18077	Host Command P4 (Generate a Proof of Host Value) has been updated to support TMK2. This is added to provide the support to the customers migrating from Luna EFT.

2.7 Bugs and Errors Corrected

Deployment Version	Reference	Description
1.16.1	PA-20262	For customers using the 'PM' (Verify a Dynamic CVV/CVC) and 'QY' (Generate a Dynamic CVV) host commands only, if a PAN field is supplied with fewer than 8 digits when using Scheme ID '5' for Visa dCVV2, a serious issue has been fixed in this release. The issue required payShield 10K to be power cycled in order to resume operation in this situation. For customers using these host commands in earlier releases the workaround is to ensure that the application can only supply a PAN field of 8 digits or more as input to these commands.
	PA-19618	A problem with the Host Command 'LW' (Export an HMAC key under a ZMK) has been corrected. The maximum length of HMAC Key recommended to be used is the same as the length of hash algorithm output - i.e., for SHA-512, an HMAC Key with a length of 512 bits (64 bytes) would be recommended. However, if payShield 10K is in Authorised State AND a key length longer than 100 bytes was used, this caused payShield 10K to halt communication temporarily for 5-10 seconds.
	PA-20219	PA-181612 was not fixed in the 1.9d and 2.1a release. The following corrections have been made to address this. o Host Command 'A0' (Generate Key) has been updated to correct a problem whereby an invalid key was generated approx. 1 in 50,000 times in certain cases when using a Variant LMK. o Host Command 'A8' (Export Key) has been updated to return the correct error code should the above scenario ever be encountered again.
	PA-19464	A problem with the Host Command 'PE' (Print PIN/PIN and Solicitation Data) has been fixed in this release. The issue occurred when EBCDIC format was used. The host command now accepts this format and no longer returns an error.
	PA-19574	The error "Status --> Error log" displayed in payShield Manager when performing Login/Logout/refresh operations. after payShield 10K is rebooted when using payShield Cloud HSM. This error is no longer displayed in this release.
	PA-19440	This is for GBIC AES ZKA. A problem with Host Command 'A6' (Import a Key) failing to import Numeric Key Usage 11 is fixed in this release. When the ANSI X9.143/TR-31 contains Key Usage 11, This now correctly converting the Key Usage 53 in Thales Key Block format.

Deployment Version	Reference	Description
	PA-19442	A problem with Host Command 'QE' (Generate a Certificate Request) was fixed in this release. The problem was that the Host command returned an invalid CSR due to failing to decode CSR in ASN1.
	PA-19612	An error code was not given for console command test print and host command printing when not connected to a printer, this has been fixed in this release.
	PA-20316	A problem with the Host Command KW (ARQC Verification and/or ARPC Generation) has been fixed in this release. The problem was that for Mode '3' & '4', EMV 4.x Method 2, AES, the 4-byte CSU was not concatenated in the resultant ARPC.
	PA-18198	A problem with Key Usage K1 not supported for ZMK in the Host Commands LU (Import an HMAC key under a ZMK) and LW (Export an HMAC key under a ZMK) has been fixed in this release.
	PA-18758	Manual for the Host Command 'KW' (ARQC Verification and/or ARPC Generation) has been updated to clarify the PAN values for Scheme ID = 'D' for Interac.
	PA-10339	Core Host Command Manual is updated with UTILSTATS information for 'J2' (Get HSM Loading).
	PA-20389	Manual for the Host Command IG (Key Derivation using ECKA-EG) has been updated with Error 56 and the description, which was not defined previously.
	PA-20525	Description of SETTIME in the payShield 10K Console Guide is updated to say that SETTIME is enabled in Secured Mode only.
1.16.0	PA-18860	Host Command 'BG' (Translate PIN and PIN Length) has been updated to correct an issue when translating a PIN Block to legacy format Tag 'J' when using an AES Key Block LMK.
	PA-13204	When restoring settings from smart card using the 'RS' (Restore Settings) Console Command, the text displayed indicates the Temperature alarm is set to OFF. This text has been removed as the Temperature alarm is not included in the settings and it is not possible to disable the temperature alarm.
	PA-15696	The description in the SNMP MIB for 'payShieldManagementEthernetEnabled' has been updated as follows to clarify that it is just payShield Manager that is disabled and not the Management Port: Whether payShield Manager web interface is enabled or disabled

Deployment Version	Reference	Description
		'1' - payShield Manager is enabled. '2' - payShield Manager is disabled.
	PA-16445	When using the Console to view the Error Log, the following statement has been removed as it is not required: "Please copy this log to a text file and send it to your regional Thales eSecurity Support center"

3   2100-000x (2.1a) – Released November 2024

3.1   Summary

This is a general release for all customers. This is 2.0c deployment version 1.14.6 with the addition of new features and bug fixes. This also includes the new features and bug fixes that were included in 1.9c and 1.9d but not included in 2.0c.

3.2   Version Details

Base Release: 2.1a

Revision: 2100-0001   Deployment Version: 1.15.1 This is 1.15.0 with 1 bug fix only.
                     2100-0000   Deployment Version: 1.15.0 Feature release.

3.3   PCI HSM Compliances

This software release is planned to undergo approval to 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

3.4   Manuals

The following manuals have been updated for use with this release:
  > 007-001512-021 Rev A payShield 10K Installation and User Guide
  > 007-001518-021 Rev A payShield 10K Host Programmers Manual
  > 007-001515-021 Rev A payShield 10K Core Host Commands
  > 007-001516-021 Rev A payShield 10K Legacy Host Commands
  > 007-001513-021 Rev A payShield 10K Security Operations Manual
  > 007-001517-021 Rev A payShield 10K Applications Manual
  > 007-000997-021 Rev A payShield 10K Console Guide
  > 007-001443-021 Rev A payShield 10K Host Command Examples

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.

Please note that payShield Manager no longer supports Internet Explorer as this is no longer supported by Microsoft.

Operating System	Windows 10 and 11 64-bit			Linux Ubuntu 20 64-bit		macOS Monterey & Ventura
Browser	Chrome 64-bit	Firefox 64-bit	Edge 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K 2.1a	☑	☑	☑	☑	☑	☑

3.6   New Features

Deployment Version	Reference	Description
1.15.0	PA-12468 PA-17476	An enhancement to the process of installing and renewing Host TLS Certificates is including, simplifying the process. Two TLS stores for TLS Keys and Certificates for the Host Port are now supported - A and B. One store is active and is used for host connections. The other is inactive and is used to prepare the next set of keys and certificates in Online State. Secure State is required to allocate the Inactive Key Store to Active. A facility is also provided to allow selected Host TLS Key and certificates to be copied from one key store to the other. The new facility provides additional flexibility to the configuration process. The new facility is backward compatible so the functionality previously provided can be used using Secure State. When upgrading or downgrading from/to a release supporting this functionality, the existing TLS store is maintained. For TLS support, the following is also provided in this release: • Documentation on how to import multiple TLS certificates contained in one file is included for both the host port and payShield Manager. • Documentation is also provided on how to change and also sign the TLS certificates used for the payShield Manager connection by an external CA. • A problem when importing Host TLS certificates using a file which logged the user out of payShield manager has been fixed. Documentation updates describing how to manage the TLS keys and certificates are included in Chapter 11 in the Installation and User Guide and also with the description of the user interface for payShield Manager and the Console.

Deployment Version	Reference	Description
1.15.0	PA-18124	Host Command 'KI' (Derive Card Unique Keys) has been updated to export the card keys derived using ECB mode of encryption using ISO 9797-1 padding mode 2 format, supporting use of a 128 or 256-bit AES KEK. Note that export using the NIST SP800-38F format is already supported when using a 128 or 256-bit AES KEK.
	PA-17832	Host Command 'BU' (Generate a Key Check Value) and Console Command 'CK' (Generate a Key Check Value) have been updated to provide the option to return the key length of AES Keys.
	PA-19112	Host Command 'BU' (Generate a Key Check Value) has been updated to provide an option to determine whether a 3DES key is masquerading as a single length DES key.
	PA-17475	It is now possible to delete the Remote Syslog Server.
	PA-14606	Enhancement to the Out of Band (OOB) REST API provided when using the Hosted HSM Optional Licence included to allow a change in the IP address of the Host and Management port when in provisioned state.
	The following features are also included in 1.9c & 1.9d. **These features were not included in 2.0c.**	
	PA-15795 PA-18045	The specifications for processing PINs using the VISA ABA PVV method currently use a 3DES PVK. The specifications have now been updated by Visa to support an AES PVK. The following host commands have been updated to support the new method: • DG - Generate an ABA PVV (of an LMK encrypted PIN) • FW - Generate an ABA PVV (of a customer selected PIN) • CU - Verify a PIN & Generate an ABA PVV (of a customer selected PIN) • DC - Verify a Terminal PIN Using the ABA PVV Method • EC - Verify an Interchange PIN Using the ABA PVV Method • GQ - Verify a PIN Using the ABA PVV Method (3DES & AES DUKPT)
	PA-17404	Host Command 'KI' (Derive Card Unique Keys) has been updated to export the card keys derived using ECB mode of encryption. This uses ISO 9797-1 padding mode 4 format and only supports use of a 128 or 256-bit AES KEK. Note that export using the NIST SP800-38F format is already supported when using a 128 or 256-bit AES KEK.

Deployment Version	Reference	Description
	PA-16446 PA-18118	Host Command 'KW' (ARQC Verification and/or ARPC Generation) has been updated to provide support for the following: • For Scheme ID 4 supporting Visa Cloud Based Payments (VCP) (CVN '43') this now supports an AES MK-AC (Issuer Master Key for generating and verifying Application Cryptograms) in addition to a DES MK-AC. The MK-AC is used to derive the LUK (Limited Use Key). • A new Scheme ID 'E' is also supported. This is identical to the current Scheme ID '9' with the following update. The ARQC Mask is now present for the new Scheme ID 'E' as well as Scheme ID '5' and '6' and this is used in the process to compare the supplied ARQC with the generated ARQC.
	PA-15804	Host Command 'IC' (Establish Secure Session with Chip Card) has been updated to support Secure Channel Protocol 03 (SCP03) with Card Key Generation Mode '0' where the card key(s) are derived from the master KMC key (EMV/Chip Issuer Master Key: Card Personalization). This requires use of an AES KMC - this is imported using 'A6' (Import Key) host command using ECB or CBC format. Host Command 'A6' (Import Key) has been updated to support import of AES keys in both ECB and CBC format: ECB key encryption schemes:

Key Scheme	KEK	Wrapped key
'PG'	128/192/256-bit AES key	128-bit AES key
'WG'	128/192/256-bit AES key	256-bit AES key

CBC key encryption schemes:

Key Scheme	KEK	Wrapped key
'P'	128/192/256-bit AES key	128-bit AES key
'W'	128/192/256-bit AES key	256-bit AES key

To allow import of keys in ECB/CBC format (which is untrusted), the following security setting must be set as follows:

• Key export and import in trusted format only: **No**

Deployment Version	Reference	Description
	PA-18119	Generation, import and export of the following keys using the AES algorithm is now supported using host commands 'A0', 'A6', & 'A8': • EMV keys with key usages **E1** (EMV/Chip card Master Key: Secure Messaging for Confidentiality (MK-SMC)) & **E3 (**EMV/Chip card Master Key: Data Authentication Code (MK-DAC)) • CVK keys with key usages **C0** (Card Verification Key) & **13 (**Card Verification Key (Visa CVV)). These are included at this stage to allow keys to be generated ready for use with updated commands in a later release.

3.7   Known Issues

Deployment Version	Reference	Description
1.15.0	N/A	The SETTIME Console Command cannot be used in the payShield Manager Virtual Console. The payShield Manager user interface can be used to set the time instead.

3.8   Bugs and Errors Corrected

Deployment Version	Reference	Description
1.15.1	PA-19763	A problem with host command 'IG' (Elliptic Curve Key Agreement) has been fixed in this release. The problem caused payShield 10K to reboot after approximately 15 million calls to this host command. Following a reboot caused by this issue, payShield 10K continues to function normally. The workaround for customers using earlier releases that do not include this fix is to schedule a reboot of payShield 10K before 15 million calls are made. The number of calls made to host command 'IG' can be monitored using payShield Manager, the Console or payShield Monitor using the Utilization Statistics feature.
	PA-18766 PA-18672	Host Command 'CS' (Modify Key Block Header) has been updated to allow the following changes in Mode of Use: • From Mode of Use 'N' (No special restrictions or not applicable) to 'X' (Key derivation for EMV Master Keys with Key Usages E0, E1, E2, E3, E4, E5, E6, and E7.

Deployment Version	Reference	Description
1.15.0		• From Mode of Use 'N' (No special restrictions or not applicable) to 'C' (Generate and Verify) for CVK with Key Usage 'C0' and PVK with Key Usages 'V1' and 'V2'.
	PA-18634	A correction to Host Command 'KY' (Generate Secure Message (EMV 4.x)) is included in this release when using Mode '4' (Integrity and PIN Change) and Scheme 'B' (Visa VIS 3.0 using EMV 4.4 Option 'C' ICC Master Key derivation and EMV Common Session Key Derivation). The key used to encrypt the PIN Block when using PIN Block Format 48 is now derived from the MK-SMC using the Common Core method as described in EMV 4.4 Book 2 Annex A1.3.1.
	PA-19018	The K-DEK was not being returned in the Response Message when using Host Command 'IC' (Establish Secure Session with Chip Card), Secure Channel Method '7' (Secure Channel Protocol 03 (SCP03)) and Card Key Generation Mode '0' (Card key(s) derived from master KMC key). This has been corrected.
	PA-17864	Host Command 'CC' (Translate a PIN from One ZPK to Another) has been updated to correct an issue when using a 12 digit PAN and translating from encryption under an AES ZPK to a 3DES ZPK. When encrypting a 12 digit PAN under a 3DES ZPK, the check digit is now correctly removed and the PAN pre-pended with '0' as required by the standard.
	PA-8087	A problem with the LMK Identifier in Host Command 'K2' (Verify Truncated Application Cryptogram (Mastercard CAP)) when using Scheme ID '01' (Mastercard CAP with TDS) has been fixed.
	PA-10830	Host Command 'JY' (Jason Web Token Decode) has been updated with a fix to allow support when using EBCDIC mode.
	PA-16418	Host Command 'BU' (Generate a Key Check Value) has been updated to correctly support EBCDIC mode.
	PA-18719	Host Commands 'LU' (Import HMAC Key) and 'LW' (Export HMAC Key) were giving an error when using EBCDIC mode when using Transport Format '05 (ANSI X9.143/TR-31). This has been fixed.
1.15.0	PA-18674	Host Command 'LW' (Export an HMAC key under a ZMK) has been corrected to allow export in ANSI X9.143/TR-31 Format with the Exportability field set to 'E' (may only be exported in a trusted Key Block, provided the wrapping key itself is trusted).
	PA-10686	Host Command 'NI' (Return Network Information) now correctly returns information on the UDP ports as well as the TCP ports as specified in the Core Host Commands Manual.

Deployment Version	Reference	Description
1.15.0	PA-18026	When using a Variant LMK, Console Commands 'KE' (Key Export) and 'KG' (Key Generate) now allow the following Key Block Versions to be selected: • 'B' (Key block protected using the Key Derivation Binding Method • 'C' (Key block protected using the Key Variant Binding Method).
	PA-18275	A bug has been fixed to allow a separate Authorised Activity can now be used to authorize import of an HMAC using Host Command 'LU' (Import an HMAC key under a ZMK) and a Key Block LMK.
	PA-18817	A stability issue was fixed for Host Command 'I8' (MULTOS ALU Generator).
	PA-17507	Host Command 'A6' (Import Key) has been updated to correct an intermittent error in a corner case when using a Variant LMK.
	PA-10377	The payShield Manager user interface did not allow the TCP and UDP protocols to be disabled when TLS is enabled. This could only be achieved when using the payShield Manager Virtual Console. This has been fixed.
	PA-17329	When using payShield Manager, after updating the Initial Security Settings in Secure State and selecting Offline or Online State, the "Apply" button is still visible although this cannot be used to change the settings. This has been corrected in this release.
	PA-18081	When using "Settings per LMK" the following issue has been fixed in payShield Manager when saving and restoring settings: • Save settings to smart card with both "Settings per LMK" and "UDP" disabled. • Enable "Settings per LMK". • Restore settings from smart card. • It is now not possible to change either the "Settings per LMK" or to disable "UDP" using payShield Manager. • The workaround is to use the Virtual Console or the Console to change these settings.
	PA-12601	In payShield Manager, when selecting Authorised Activities with the options 'Until Reboot' or 'Persistent', the values '-2" and '-1' were displayed in the 'minutes' box. This has been corrected.
	PA-18089	The following issue has been fixed in payShield Manager when using the Hosted HSM (HHSM) functionality when the Service Provider reclaims payShield 10K for use by another end user: • End user uses payShield Manager to disable 'UDP' and enable 'Settings per LMK'. • payShield 10K is reclaimed by the Service Provider.

Deployment Version	Reference	Description
		• payShield 10K is then allocated to another end user. • End user uses payShield Manager to view the settings and both "Settings per LMK" and "UDP" are enabled and cannot be changed. • The workaround is to use the Virtual Console to change these settings.
	PA-18818	When using Hosted HSM, after the Service Provider reclaims payShield 10K from the end user ready for allocation to another end user, the Model Number and Serial Number are no longer displayed. This has been corrected in this release.
	PA-13903	When restoring settings from smart card using the Console Command 'RS' (Restore Settings), the Audit options were not being restored. This has been corrected.
	PA-16428	Occasionally, when inserting the smartcard into the embedded smart card reader on the front panel of payShield 10K, the Console Command will return the below error. This has been fixed. • Card not formatted or card inserted incorrectly. • Unable to read card - Card invalid or incorrectly inserted
	PA-18232	When continuously opening and closing multiple TLS sessions, in certain circumstances under very heavy load using 256 sessions and 20 LMKs with "Settions per LMK" enabled, payShield 10K occasionally restarts and the current host commands being processed fail. After the restart, processing continues as normal. This has been fixed in this release.
1.15.0	PA-15742	The following error message was occasionally being added to the error log although the real time clock was operating correctly. This has been fixed in this release: • ERROR: [Real-Time Clock: FAILED (RTC is stuck)]
	PA-14034	When using the payShield 10K printer port, the printing speed has been increased in this release.

	PA-18627
	PA-13134
	PA-16589
	PA-15912
	PA-18269
	PA-14500
	PA-14043
	PA-11551
		payShield 10K Manuals have been updated for this release to include information on the new features as well as updates as required for the bug fixes listed above. They have also been updated to include several corrections as follows. In summary:
		
		• Installation and User Guide
		  o Chapter 9 updated to include information on the new features and also the numbering of Section 9.10 has been updated.
		  o Chapter 11 updated to include information on the new TLS feature, how multiple certificates are imported in one file and also how to change the Management TLS keys and certificates used for payShield Manager.

Deployment Version	Reference	Description
1.15.0		- o Update to Section 9.10.10, "Load/Save Settings" - o The following Chapters and Appendices have been moved from the Programmer's Guide to the Installation and User Guide: • Chapter 18, "SNMP". • Chapter 19, "Remote Syslog". • Appendix E, "SNMP MIB Security Settings" - o Other minor updates and corrections. • Core Host Commands Manual: - o Updated to include information on new features as well as to address several corrections and clarifications. - o An explanation of Error Code '75' (Invalid Public key / Private key pair) has also been included in the Core Host Command Manual for Host Command 'L6' (Import an RSA Private Key). • Host Programmer's Manual: - o Chapter 11 has been updated to include references to ANSI X9.143 Key Block Standard as well as TR-31. All references in the document now refer to both X9.143 and TR-31. - o Update to Key Usage table in Section 8.5.1.2, Key Usage (Bytes 5-6) for key usages C0, 13, E1, E3, V2, - o Update to Appendix A - Key Scheme Table for Key Scheme Tags XI, PG, PI, P, WG, WI, W - o Update to Section 5.4.6 for Pad Mode. - o Update to Section 11.2.3, Key Usage (Bytes 5-6) to include key usage M7. - o The following Chapters and Appendices are more appropriate for the Installation and User Guide and so have been moved here: • "SNMP". • "Remote Syslog". • "SNMP MIB Security Settings" - o The SNMP MIB Appendix has been removed as this is provided with the software release and is readable using a standard text editor. • Security Manual - o Information previously provided on Secure Host Communications that is not security related has been moved to the Installation and User Guide Chapter 11. • Legacy Host Command Manual - o Minor correction to Host Commands 'AE' and 'HC'.
	The following bug fixes are also included in 1.9d. They were not included in 2.0c.	
	PA-18136 PA-18871	The following issues have been fixed in host command 'B8' (TR-34 Export) when exporting an AES Key: • When the "Key Block Encryption Algorithm" Field is set to '00' (192-bit TDES key – CBC), the export of an AES key is now prevented when

Deployment Version	Reference	Description
		Security Setting "Enforce PCI HSMv3 Key Equivalence for Key Wrapping" is set to Yes. • When the "Key Block Encryption Algorithm" Field is set to '01' (128-bit AES key – CBC), an AES ephemeral key is now correctly used.
	PA-18729 PA-18182	The following host commands are only used to support the Australian Standard AS2805.6.2 - 2002 standard. The commands have been corrected so the MAC Residue (MARX) in the output can be the rightmost 64 bits of the Extended MAB as implemented in other systems. The corrections have been applied to the following host commands: • 'RE' (Host Command (Verify a Transaction Request, without PIN)). • 'RG' (Verify a Transaction Request, with PIN, when CD Field Available) • 'RK' (Generate Transaction Response, with Auth Para Generated by Acquirer (when selected Transaction Key Scheme is Australian)). In addition, for 'RK', a bug was fixed when 'AP Include Flag' = 'H'.
	PA-18112	An issue with Host Command 'A6' (Import Key) was found when importing a 3DES Key using the CBC mode of encryption using key schemes 'M' and 'O'. This issue was that odd parity was not forced on the imported key. This has been corrected.
	PA-14958	Section 4.3 of the Host Programmers Manual covering the Derived Unique Key per Transaction (DUKPT) scheme has been substantially revised and updated.
	PA-18301	There was a problem found which prevented the use of custom key usage '07' in custom software – this has now been fixed. Note that the fix has no impact on the base release which does not use Key usage '07'.
1.15.0	PA-18162	The following corrections have been made: • Host Command 'A0' (Generate Key) has been updated to correct a problem whereby an invalid key was generated approx. 1 in 50,000 times in certain cases when using a Variant LMK. • Host Command 'A6' (Import Key) and Host Command 'A8' (Export Key) have also been updated to return the correct error code should the above scenario ever be encountered again.
	The following bug fixes are also included in 1.9c. They were not included in 2.0c.	
	PA-17525	Host Command 'KY' (Generate Secure Message) has been updated to support a 256-bit AES SMI as well as a 128-bit key.

Deployment Version	Reference	Description
	PA-15420	A problem with importing and exporting an RSA private key in component format has been fixed in this release. The fix impacts host commands 'L6' (Import an RSA Private Key) and 'L8' (Export an RSA Private Key) when the CRT components of the RSA Private Key are not all the same length.
	PA-17402	A problem has been fixed with Host Command 'M6' (Generate MAC). When using CBC-MAC, the size of the MAC returned was restricted to 8 bytes (16 hex digits) whereas the standards place no restrictions on the MAC size. To address this, a new MAC size without a size restriction has been added as follows: • '2': MAC size of 32 hex digits (only valid for MAC Algorithm '6' CMAC & MAC Algorithm '5' CBC-MAC) When using the above 'MAC Size' and Mode '0' or '3': For Host Command 'M6', the MAC returned is 32 H in size
	PA-17653	The 'BG' host command utilized for translating a PIN from encryption under an 'old' LMK to encryption under the 'new' LMK encounters an error 46, signifying 'Invalid tag for encrypted PIN.' This has been fixed in this release.
	PA-18060	When support for Network Time Protocol (NTP) is configured, a problem with the time obtained when the payShield 10K is powered off and then on again has been fixed.

4 2000-002x (2.0c) – Released September 2024

4.1 Summary

This is a general release for all customers. This is v2.0b deployment version 1.14.5 with the addition of 1 bug fix only.

4.2 Version Details

Base Release: 2.0c

Revision: 2000-0020 Deployment Version: 1.14.6 This is 1.14.5 with the addition of 1 bug fix only.

Please note:

1. v1.9c and v1.9d are now also available but the contents of these releases are not included in v2.0c.
2. v2.0a deployment versions 1.14.3 and 1.14.4 were not for general release.
3. With the release of v2.0, the scheme for numbering the Revision has been updated as follows:

   Revision is in the format $M_3M_2M_1M_0 . N_3N_2N_1N_0$
   - M_3 and M_2 follow the base release, e.g.;
     - **20**00-1000 for base release 2.0a
     - **21**00-1000 for base release 2.1a
   - M_1 and M_0 are **00**
   - N_3 indicates whether the Security Settings are PCI HSM v3 compliant as with earlier releases:
     - **1** indicates the Security Settings compliant.
     - **0** indicates the Security Settings are not compliant.
   - N_2 is **0** to indicate the release is for payShield 10K as with earlier releases.
   - N_1 is incremented for releases that include enhancements that require PCI HSM v3 approval.
   - N_0 is incremented for releases that do not require additional separate PCI HSM v3 approval:
     - This is indicated by inclusion of 'x' as the last digit of the revision shown on the PCI website.

4.3 PCI HSM Compliance

This software release is planned to undergo approval to 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

4.4 Manuals

The following manuals have been updated for use with this release:

> 007-001512-020 Rev C payShield 10K Installation and User Guide
> 007-001518-020 Rev C payShield 10K Host Programmers Manual
> 007-001515-020 Rev C payShield 10K Core Host Commands
> 007-001516-020 Rev C payShield 10K Legacy Host Commands
> 007-001513-020 Rev C payShield 10K Security Operations Manual
> 007-001517-020 Rev C payShield 10K Applications Manual
> 007-000997-020 Rev C payShield 10K Console Guide
> 007-001443-020 Rev C payShield 10K Host Command Examples

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.

Please note that payShield Manager no longer supports Internet Explorer as this is no longer supported by Microsoft.

Operating System	Windows 10 and 11 64-bit			Linux Ubuntu 20 64-bit		macOS Monterey & Ventura
Browser	Chrome 64-bit	Firefox 64-bit	Edge 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K 2.0c	☑	☑	☑	☑	☑	☑

4.6　New functions

None

4.7　Known Issues

Deployment Version	Reference	Description
1.14.6	PA-17575	If two Remote Syslog Servers have been configured, it is not possible to change the configuration to support only one Remote Syslog Server. If Remote Syslog Server is no longer required, it can be disabled instead.
	N/A	The SETTIME Console Command cannot be used in the payShield Manager Virtual Console. The payShield Manager user interface can be used to set the time instead.

4.8　Bugs and Errors Corrected

Deployment Version	Reference	Description
1.15.0	PA-19763	A problem with host command 'IG' (Elliptic Curve Key Agreement) has been fixed in this release. The problem caused payShield 10K to reboot after approximately 15 million calls to this host command. Following a reboot caused by this issue, payShield 10K continues to function normally. The workaround for customers using earlier releases that do not include this fix is to schedule a reboot of payShield 10K before 15 million calls are made. The number of calls made to host command 'IG' can be monitored using payShield

Deployment Version	Reference	Description
		Manager, the Console or payShield Monitor using the Utilization Statistics feature.
1.14.6	PA-19583	The following issue has been fixed in host command 'B8' (TR-34 Export) when exporting an AES or 3DES Key: • When the "Key Block Encryption Algorithm" Field is set to '01' (128-bit AES key – CBC), a 192-bit TDES key ephemeral key was used instead of a 128-bit AES key.

5   2000-001x (2.0b) – Released August 2024

5.1   Summary

This is a general release for all customers. This is v2.0a deployment version 1.14.2 with the addition of 1 minor enhancement and 3 bug fixes.

5.2   Version Details

Base Release: 2.0b

Revision: 2000-0010   Deployment Version: 1.14.5   This is 1.14.2 with the addition of
                                                                   1 minor enhancement and 3 fixes only

Please note:

4. v1.9c and v1.9d are now also available but the contents of these releases are not included in v2.0b.
5. v2.0a deployment versions 1.14.3 and 1.14.4 were not for general release.
6. With the release of v2.0, the scheme for numbering the Revision has been updated as follows:

Revision is in the format $M_3M_2M_1M_0 . N_3N_2N_1N_0$
- M_3 and M_2 follow the base release, e.g.;
  - **20**00-1000 for base release 2.0a
  - **21**00-1000 for base release 2.1a
- M_1 and M_0 are **00**
- N_3 indicates whether the Security Settings are PCI HSM v3 compliant as with earlier releases:
  - **1** indicates the Security Settings compliant.
  - **0** indicates the Security Settings are not compliant.
- N_2 is **0** to indicate the release is for payShield 10K as with earlier releases.
- N_1 is incremented for releases that include enhancements that require PCI HSM v3 approval.
- N_0 is incremented for releases that do not require additional separate PCI HSM v3 approval:
  - This is indicated by inclusion of 'x' as the last digit of the revision shown on the PCI website.

5.3   PCI HSM Compliance

It is important to note that the next release (2.0c) will now be submitted for PCI HSM approval in place of 2.0a and 2.0b. Therefore 2.0b **will not** be PCI HSM v3 approved due to known issue PA-19583 referenced later.

5.4   Manuals

The following manuals have been updated for use with this release:

> 007-001512-020 Rev B payShield 10K Installation and User Guide
> 007-001518-020 Rev B payShield 10K Host Programmers Manual
> 007-001515-020 Rev B payShield 10K Core Host Commands
> 007-001516-020 Rev B payShield 10K Legacy Host Commands
> 007-001513-020 Rev B payShield 10K Security Operations Manual
> 007-001517-020 Rev B payShield 10K Applications Manual
> 007-000997-020 Rev B payShield 10K Console Guide
> 007-001443-020 Rev B payShield 10K Host Command Examples

5.5   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.

Please note that payShield Manager no longer supports Internet Explorer as this is no longer supported by Microsoft.

Operating System	Windows 10 and 11 64-bit			Linux Ubuntu 20 64-bit		macOS Monterey & Ventura
Browser	Chrome 64-bit	Firefox 64-bit	Edge 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K 2.0b	☑	☑	☑	☑	☑	☑

5.6   New functions

Deployment Version	Reference	Description
1.14.5	PA-18125	Host Command 'IG' (Key Agreement using Elliptic Curve Key Agreement) has been updated to require authorization when deriving keys. This is included to increase the security of this command. Two additional Authorised Activities are now provided specifically for this purpose. These are: • **eckai.{key}.host** - For the Initiator to derive keys with key usage {key}, this activity must now be authorized, where 'key' is the key usage code of the key being derived. • **eckar.{key}.host** - For the Recipient to derive keys with key usage {key}, the following activity must now be authorized, where 'key' is the key usage code of the key being derived. The following table summarizes the authorization required for the derivation of keys using key usage:

Mode	Agreement Type	Authorization required	Description
2	0	**eckai.{key}.host** or **eckar.{key}.host**	ECKA-EG: initiator's 2nd call or recipient's 2nd call. ECKA-DH: recipient's 2nd call.
1	0	**eckar.{key}.host**	ECKA-EG: recipient's single call (when deriving keys).
2	1	**eckai.{key}.host**	ECKA-DH: initiator's 2nd call.
1	1	**eckar.{key}.host**	ECKA-DH: recipient's single call (when deriving keys).

5.7   Known Issues

Deployment Version	Reference	Description
1.14.5	PA- 19583	The following issue has been found in host command 'B8' (TR-34 Export) when exporting an AES or 3DES Key: • When the "Key Block Encryption Algorithm" Field is set to '01' (128-bit AES key – CBC), a 192-bit TDES key ephemeral key is used instead of a 128-bit AES key.
	PA-17575	If two Remote Syslog Servers have been configured, it is not possible to change the configuration to support only one Remote Syslog Server. If Remote Syslog Server is no longer required, it can be disabled instead.
	N/A	The SETTIME Console Command cannot be used in the payShield Manager Virtual Console. The payShield Manager user interface can be used to set the time instead.

5.8   Bugs and Errors Corrected

Deployment Version	Reference	Description
1.14.5	PA-18871	The following issue has been fixed in host command 'B8' (TR-34 Export) when exporting an AES Key: • When the "Key Block Encryption Algorithm" Field is set to '00' (192-bit TDES key – CBC), the export of an AES key is now prevented when Security Setting "Enforce PCI HSMv3 Key Equivalence for Key Wrapping" is set to Yes.
	PA-17948 (Same issue reported in PA-13579 & 13498)	A very small number of payShield 10K are still reporting "Fan x too fast" error when running the self-diagnostics. Once this error is reported, it is then seen each time the self-diagnostics are run (typically each day). This issue has mainly been seen on PS10-D payShield 10K 10Gb and PS10-F payShield 10K FICON hardware platforms. A fix for this issue was included in 1.8a but a further fix is now required. It is important to note that in this case the error does not impact the operation of the HSM other than generating the error message. The Fan Tray is not faulty and replacing the fan tray does not solve the issue. This issue has been fixed in software in this release. After upgrading to this release, payShield 10K should not start reporting this issue unless there is a genuine fan failure. Any payShield 10K already reporting this issue should no longer report this issue after upgrading.

Deployment Version	Reference	Description
1.14.5	PA-18655	A problem was found with custom software based on 2.0a could not be used with custom keys. This has now been fixed. Note that the fix has no impact on the base release which does not use custom keys.

	PA-14958
	PA-19017
		Documentation updates:
		
		• Host Programmers Manual:
		   o Section 2.1.2 regarding Sending commands and receiving responses.
		   o Section 4.3 covering the Derived Unique Key per Transaction (DUKPT) scheme has been substantially revised and updated.
		   o Section 8.5.1.2 covering key usages includes a small number of corrections and updates.
		   o Appendix F includes the new authorised activities required for the new minor enhancement in this release.
		• Core Host Commands Manual:
		   o The description of the format of the Source and Destination PAN field has been corrected for the case when the Source PIN Block was formed using a token PAN (instead of the real PAN) in the following Host Commands:
		      ▪ 'CA' (Translate a PIN from TPK to ZPK/BDK Encryption.
		      ▪ 'CC' (Translate a PIN from One ZPK to Another)
		      ▪ 'G0' (Translate a PIN from BDK to BDK or ZPK Encryption)
		   o Host Command 'B8' (TR-34 Export) has been updated to clarify that the Modified Exportability field is Optional.

6 2000-000x (2.0a) – Released April 2024

6.1 Summary

This is a general release for all customers. This is 1.9b deployment version 1.13.3 with the addition of 2 significant new features (Settings per LMK and Remote syslog), a number of other new features and bug fixes.

6.2 Version Details

Base Release: 2.0a

Revision: 2000-0000

Deployment Version: 1.14.2 Feature Release

Please note:

1. v1.9c and v1.9d are now also available but the contents of these releases are not included in 2.0a.
2. With the release of 2.0, the scheme for numbering the Revision has been updated as follows:

    Revision is in the format $M_3M_2M_1M_0 . N_3N_2N_1N_0$
    - M_3 and M_2 follow the base release, e.g.;
        - **20**00-1000 for base release 2.0a
        - **21**00-1000 for base release 2.1a
    - M_1 and M_0 are **00**
    - N_3 indicates whether the Security Settings are PCI HSM v3 compliant as with earlier releases:
        - **1** indicates the Security Settings compliant.
        - **0** indicates the Security Settings are not compliant.
    - N_2 is **0** to indicate the release is for payShield 10K as with earlier releases.
    - N_1 is incremented for releases that include enhancements that require PCI HSM v3 approval.
    - N_0 is incremented for releases that do not require additional separate PCI HSM v3 approval:
        - This is indicated by inclusion of 'x' as the last digit of the revision shown on the PCI website.

6.3 PCI HSM Compliance

It is important to note that a future release (2.0c) will now be submitted for PCI HSM approval in place of 2.0a and 2.0b. Therefore 2.0a **will not** be PCI HSM v3 approved.

6.4 Manuals

The following manuals have been updated for use with this release:

> 007-001512-020 Rev A payShield 10K Installation and User Guide
> 007-001518-020 Rev A payShield 10K Host Programmers Manual
> 007-001515-020 Rev A payShield 10K Core Host Commands
> 007-001516-020 Rev A payShield 10K Legacy Host Commands
> 007-001513-020 Rev A payShield 10K Security Operations Manual
> 007-001517-020 Rev A payShield 10K Applications Manual
> 007-000997-020 Rev A payShield 10K Console Guide
> 007-001443-020 Rev A payShield 10K Host Command Examples

6.5 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.

Please note that payShield Manager no longer supports Internet Explorer as this is no longer supported by Microsoft.

Operating System	Windows 10 64-bit			Linux Ubuntu 20 64-bit		macOS Monterey & Ventura
Browser	Chrome 64-bit	Firefox 64-bit	Edge 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K 2.0a	☑	☑	☑	☑	☑	☑

6.6   New functions

Deployment Version	Reference	Description

1.14.2	PA-15452
	PA-13583
		A new feature included in payShield 10K software release 2.0a and above allows certain settings to be configured for each LMK. In previous versions settings applied to all LMK installed on payShield 10K.
		
		By providing the ability to configure unique settings on a per LMK basis on a single payShield, payShield 10K customers can consolidate their payments workloads and use their payShield estate(s) more efficiently.
		
		For example, by using the new Settings per LMK feature allows PIN length of 4 for to be configured for "LMK ID 1" and a PIN length of 5 can be configured for "LMK ID 2". Previously separate payShield 10K would have had to be used for these separate settings.
		
		The following can now be selected per LMK:
		
		• Selected security settings to be set per LMK
		
		• Host Commands to be enabled and disabled per LMK
		    o Note that Console Commands are enabled or disabled on a per HSM basis as before.
		
		• PIN Block Formats to be enabled and disabled per LMK
		
		Some important restrictions to be aware of when using Settings per LMK:
		
		• The LMK ID to be used by the Host Commands is defined by the host port.
		    o The alternative methods, specifying the LMK at the end of the host command using a '%' delimiter, or specifying the LMK ID in the Thales Key Block are not supported when using settings per LMK.
		
		• A TCP or TLS connection is required
		    o UDP and FICON are not supported when using Settings per LMK
		
		• PCI HSM approval is assessed on an HSM basis
		    o The implies that for PCI HSM compliance, the Security Settings for all LMK ID must comply to PCI requirements.
		
		For further information please refer to Section 9.9 in the *payShield 10K Host Programmers Manual.*

	PA-74 PA-16178 PA-16234	A new "Remote syslog" feature is included in payShield 10K software release 2.0a and above. This facilitates the transmission of local error and audit logs to a remote syslog server. Users can configure up to two remote syslog servers and choose to use either the payShield 10K management or the auxiliary interface. Additionally, users have the option to utilize the default ports 601 or 514, or select non-default ports within the range of to 49300 through 49320 for remote syslog.

Deployment Version	Reference	Description
1.14.2		Configuration of the Feature is undertaken using either payShield Manager or the Console. For further information please refer to Chapter 15 in the *payShield 10K Host Programmers Manual*.
	PA-15861	Host Command 'KY' (Generate Secure Message) has been updated to support a new Scheme B which utilizes the relevant AES EMV Master Keys. Scheme 'B' is for Visa VIS 3.0 using EMV 4.4 Option 'C' ICC Master Key derivation and EMV Common Session Key Derivation. Please note that this is only supported for Mode Flag = '4' for integrity and PIN change.
	PA-16446	Host Command 'KW' (ARQC Verification and/or ARPC Generation) has been updated to provide support for Scheme ID 4 when using an AES EMV Master Key MK-AC. Support for a 3DES MK-AC is already provided. Scheme ID 4 is used for Visa Cloud-Based Payments using EMV Option 'A' Card Key Derivation and Limited Use Key. This is only valid if Mode Flag = '0' (perform ARQC verification only).
	PA-16552	Host Command 'CW' (Generate a Card Verification Code/Value**)** has been updated to support CVV generation on a 16 Byte CVV data instead of separate CVV generation fields - PAN, Expiry Date and Service Code. This is to match the support provided in Luna EFT.
	PA-1145	Host Command 'A2' (Print Component) has been updated with a "Print Option" parameter to allow components to be printed on multiple lines.
	PA-17245	New Host Command included to generate an ARQC. This has host command code 'K4'. Note that this command will be included in licences issued from now on but is only available in software release 2.0a and above.

6.7   Known Issues

Deployment Version	Reference	Description
1.14.2	PA-17575	If two Remote Syslog Servers have been configured, it is not possible to change the configuration to support only one Remote Syslog Server. If Remote Syslog Server is no longer required, it can be disabled instead.
	N/A	The SETTIME Console Command cannot be used in the payShield Manager Virtual Console. The payShield Manager user interface can be used to set the time instead.

6.8   Bugs and Errors Corrected

Deployment Version	Reference	Description
1.14.2	PA-6726 PA-16776	An issue previously reported using the Erase Button on the rear of payShield 10K has been fixed in this release: • In previous releases, if the Erase Button was used with payShield 10K powered off, there was a risk of payShield 10K entering High Tamper state, requiring the HSM to be replaced. In addition, another issue has been addressed which was causing a very small proportion of payShield 10K to enter High Tamper state: • The issue was caused by a problem accessing the temperature sensors and was resolved by resetting the connection allowing access to the temperature sensors to be reinstated. • In addition, if for any reason access to the temperature sensors is still not possible, then a Medium Tamper is entered instead of a High Tamper as the cause is due to a communication issue. • Note that this issue concerns access to the temperature sensors only and is not concerned with the actual temperature recorded.
	PA-16607	Key Encryption Keys with Thales Key Block Key Usage '24' (Key Encryption Key) can now be imported and exported using TR-31. The TR-31 Key Usage used in this case is 'K0'. This key is used in the following host commands: • 'IU' - Generate Remote Management Secure Message • 'IW' - Validate and Recover Remote Management Secure Message from the MPA • 'JW' – JWT Encode • 'JY' – JWT Decode
	PA-10414	A problem with installing and deleting TLS certificates has been fixed. The certificates were being installed and deleted from stores for both the Host Port and the Management Port instead of the selected port.

Deployment Version	Reference	Description
1.14.2	PA-12266	In some cases, the payShield Manager smart card serial number was not included in the audit log. This has been corrected.
	PA-13770	The Console Command 'CK' (Generate Key Check Value) now applies the following security setting: "Prevent single-DES keys masquerading as double or triple-length keys: Yes".
	PA-10676	The 'AQ' host command now supports the TPK when the security setting "Enforce key type 002 separation for PCI HSM compliance" = "Y" and using a Variant LMK. This command translates an RSA-encrypted PIN to a ZPK or TPK-encrypted PIN.
	PA-12436 PA-17867	A problem with the 'GK' host command (Export Key under an RSA Public Key) has been fixed. This command now correctly returns an IV of 32 H length for an AES Key.
	PA-12811	When using Console Commands 'CH', 'CM' & 'CA' to change the Host, Management & Auxiliary Port to an invalid address, the error "No such file or directory" was displayed. The error message has now been updated to provide the user the correct information.
	PA-13616	For host command 'A0' (Derive Key), an error is now given if an attempt is made to derive an AES iKey from a 3DES BDK.
	PA-14771	When using host command 'GI' (Import Key or data under an RSA Public Key) and referencing a key in user storage with Key Usage Indicator '06' an error was given. This has been corrected.
	PA-11830	To change the Fraud Settings using payShield Manager, Offline State is required in addition to Authorised State. This is now consistent with the 'A5' (Configure Fraud Detection) Console Command.
	PA-17206	The Host Programmer's Manual has been updated with additional information on supporting printing including a note regarding the support of "Parallel I/F bidirectional mode". See Section 1.2 and Appendix G.
	PA-18062	A cross reference has been corrected in the Security Operations Manual in the entry for Security Setting 'Use deprecated proprietary format (Tag J) when using PIN Blocks under Key Block LMK".

7 1500-0039 (v1.9b) – Released February 2024

7.1 Summary

This is a general release for all customers.

7.2 Version Details

Base Release: 1.9b
Revision: 1500-0039
Deployment Version: 1.13.3 Release February 2024 …   This is 1.13.1 with 4 features and bug fixes
                     1.13.1 Released October 2023 …   This is 1.13.0 with the addition of 3 fixes only
                     1.13.0 Released September 2023 …   Feature release

Note that Deployment Version 1.13.2 was not released.

7.3 PCI HSM Compliance

This software release is planned to undergo approval to 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

7.4 Manuals

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

> 007-001512-009 payShield 10K Installation and User Guide
> 007-001518-009 payShield 10K Host Programmers Manual
> 007-001515-009 payShield 10K Core Host Commands
> 007-001516-009 payShield 10K Legacy Host Commands
> 007-001513-009 payShield 10K Security Operations Manual
> 007-001517-009 payShield 10K Applications Manual
> 007-000997-009 payShield 10K Console Guide
> 007-001443-009 payShield 10K Host Command Examples

7.5   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.

Please note that payShield Manager no longer supports Internet Explorer as this is no longer supported by Microsoft.

Operating System	Windows 10 64-bit			Linux Ubuntu 20 64-bit		macOS Monterey & Ventura
Browser	Chrome 64-bit	Firefox 64-bit	Edge 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K v1.9b	☑	☑	☑	☑	☑	☑

7.6   New Functions

Deployment Version	Reference	Description
1.13.3	PA-15730	The 'FY' Host command (Generate ECC Keys Pair) has been updated with an option to support the EMV 4.4 requirements.
	PA-15723	Host commands and Console commands using EMV Keys have been updated to support Mode of Use 'X' as well as Mode of Use 'N' for use with a Thales Key Block LMK and TR-31. The Thales Key Block Key Usages that have been updated are as follows: ○ E0, E1, E2, E3, E4, E5, E6, E7, 32
	PA-15401	Host Command 'KI' (Derive Card Unique DES Keys) has been updated to support the encryption of the derived 3DES keys using an AES Key Encryption Key (KEK). This applies to the Key Derivation Methods noted in red in the table below.
	PA-15943	Host Command 'A6' (Import Key) has been updated to support the import of 3DES keys in CBC format when using a 3DES ZMK.

Key Derivation Method	Master Key, Card Key Algorithm	KEK Algorithm	Key Scheme (KEK)
'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', '2', '3'	3DES	3DES	'X' for a 112-bit key 'Y' for a 168-bit key (both ANSI X9.17)
'A', 'B', 'C', 'D', 'H'	**3DES**	**AES 256 bit only**	**'N' with AES-256 key (NIST SP800-38F Key Wrap)**
'I'	AES	AES	'N' for any AES key (NIST SP800-38F Key Wrap)

7.7   Known Issues

Deployment Version	Reference	Description
1.13.3, 1.13.1, 1.13.0	N/A	The SETTIME Console Command cannot be used in the payShield Manager Virtual Console. The payShield Manager user interface can be used to set the time instead.
	N/A	The 'NO' Host Command Response has been updated to respond with the 'Number of TCP Sockets' Field with a Length of 4N instead of 2N.
	PA-12436 PA-17867	A problem with the 'GK' host command (Export Key under an RSA Public Key) has been reported which does not return an IV of 32 H length for an AES Key correctly.

7.8   Bugs and Errors Corrected

Deployment Version	Reference	Description
1.13.3	PA-17368	The following problem that was introduced in 1.6a has been fixed in 1.9b. Note this problem does not occur if using an AES Key Block LMK.
		If a very large Excluded PIN Table is supplied with the following host commands when using a 3DES Variant or 3DES Key Block LMK, then HSM processing stops. For example, an Excluded PIN Table containing more than 44 excluded PINs with a PIN length of 4 is the maximum that can be used with host command EE when all the other fields are their maximum length. The other host commands require a longer table for the problem to occur – see below for the calculation details. To return to normal operation, the HSM is required to be powered off and then on. The host commands impacted are:
		• JA - Generate a Random PIN • GA - Derive a PIN Using the Diebold Method • EE - Derive a PIN and Optionally Generate Offset for New PVK Using the IBM Offset Method
		For this to occur, the Excluded PIN Table must be long. The exact number of bytes required for each host command can be calculated by adding up the number of bytes in the command message from the start of the PAN to the end of the message trailer – this must be greater than 255 in total for the problem to occur.
		The problem also occurs if significantly more data than specified in the Host Command Manual is supplied in the following host commands. This would not be expected to occur in normal operation. The commands are: BA, BG, CE, DE, DG, NG, PG and QK.
	PA-10527	Host Command 'KO' (Generate Card RSA Key Set and Public Key Certificate) has been updated to support a certificate length greater than 255.

Deployment Version	Reference	Description
	PA-15705 PA-16687 PA-12641 PA-16604	An issue was found with Host Command 'A6' (Import Key). This occurred when importing an AES Key in TR-31 Format with the Key Length padded to mask the true length of the key. The references to the standards that document the padding requirements are: • ASC X9 TR 31-2018 Section 5.2 • ANSI X9.143-2022 Section 5
	PA-16498	When converting a key usage from Thales Key Block to Verifone GISKE format, the key usage specified in the latest GISKE v2.3 specification was not being used. This has been corrected in Host Command 'A8' (Export Key).
	PA-15845	The 'B8' Host Command (Export Key) did not export the AES Ephemeral Key correctly when the 'Key Block Encryption Algorithm' Field is set to '01. This has been fixed

	PA-17364
	(Duplicate of PA-17208)
		To meet the requirements of GBIC in Germany, the following restrictions to Host Command 'A0' have been added when using an AES ZKA:
		
		• For the NSP:
		   ○ only ZKA options 7 and 8 are permitted.
		   ○ for ZKA option 8, the derivation of a PIN decryption key is not permitted.
		• For the Acquirer:
		   ○ only ZKA options 2 and 5 are permitted.
		   ○ for option 5, the derivation of a PIN encryption key is not permitted.

1.13.3	PA-15610	Host Command 'QE' (Generate Certificate Request) did not support a UTF8 based template (Tag 0x0C). To address this, the following tags for 'Subject Data Type' = 0 are supported:

Attribute	Tag (template)
countryName	Tag 13
State	Tag 0C
localityName	Tag 0C
organisationName	Tag 0C
organisationUnitName	Tag 0C
commonName	Tag 0C
Email	Tag 16

|
| | PA-11647 | Host Commands 'M0' (Encrypt Data) and 'M2' (Decrypt Data) have been updated to support a triple length DES BDK. |
| | PA-12578 | The 'TRACERT' Console Command (Trace TCP/IP route) gave an empty result – this has been corrected. |

Deployment Version	Reference	Description
1.13.3	PA-14947	On occasion while creating a TLS Connection, payShield 10K sends an 'Alert Fatal Bad Record, MAC' preventing the connection being established. The issue is in the handshake, so once a connection has been made, communication continues without issue. This has been corrected in this release.
	PA-15760	Core Host Command Manual – Correction included to Host Command 'C6' (Generate a Random Number) to confirm this command operates with a Key Block LMK as well as a Variant LMK.
	PA-17308	Core Host Command Manual – Correction to the Key Schemes supported in Host Command 'E8' (Generate a KCA and KMACH). This update addresses the fix included in 1.9a reference PA-14761.
		Additional miscellaneous Documentation updates to the following manuals: o Programmer's Guide o Security Manual o Core Host Command Manual

>

8   1500-0038 (v1.9a) – Released September 2023

8.1   Summary

This is a general release for all customers.

8.2   Version Details

Base Release: 1.9a
Revision: 1500-0038
Deployment Version: 1.13.1 Released October 2023 …   This is 1.13.0 with the addition of 3 fixes only
                       1.13.0 Released September 2023 …   Feature release

8.3   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

8.4   Manuals

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

> 007-001512-009 payShield 10K Installation and User Guide
> 007-001518-009 payShield 10K Host Programmers Manual
> 007-001515-009 payShield 10K Core Host Commands
> 007-001516-009 payShield 10K Legacy Host Commands
> 007-001513-009 payShield 10K Security Operations Manual
> 007-001517-009 payShield 10K Applications Manual
> 007-000997-009 payShield 10K Console Guide
> 007-001443-009 payShield 10K Host Command Examples

8.5   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.

Please note that payShield Manager no longer supports Internet Explorer as this is no longer supported by Microsoft.

Operating System	Windows 10 64-bit			Linux Ubuntu 20 64-bit		macOS Monterey & Ventura
Browser	Chrome 64-bit	Firefox 64-bit	Edge 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K v1.9a	☑	☑	☑	☑	☑	☑

8.6   New Functions

Deployment Version	Reference	Description
1.13.1 & 1.13.0	PA-13893 PA-13145	Support for Network Time Protocol (NTP) has been added in this release. This allows the payShield 10K clock to synchronize to an NTP Server rather than using the internal clock which is subject to drift. Up to four NTP Servers are supported. Each NTP Server must be located in the DMZ – connection to an external NTP Server is not supported. An option for symmetric authentication to the NTP Server is provided if authentication is required. The network address of the NTP server must be provided as an IP address – support for domain names is not provided. When using an NTP server, the time on payShield 10K uses UTC – Universal Time. Local times are not supported.
	PA-12510	The Security Settings are now available via SNMP. A reference number to each security setting is given together with the text of the settings. The settings are read only and cannot be changed via SNMP. Authentication and encryption are required to be set in order to obtain the settings.
	PA-14538	When using the following Console Commands for key management using TR-31 Key Block Format Key Block Version IDs B, C and D are now supported as well as A: • KG – Generate and optionally Export Key • KE – Export Key • IK – Import Key
	PA-14568	The following restrictions are no longer applied to the selection of cipher suites and certificates when using Secure Host Communications (i.e. TLS) on the Host Ports. This is to adhere to the latest standards as RFC 8422 has replaced RFC 4492: • An ECC key can be included in a certificate signed by an RSA CA • An RSA key can be included in a certificate signed by an ECC CA • Client and Server ECC keys no longer need to be the same length • Client and Server keys no longer need to be the same type, i.e. the Client can be RSA and the Server ECC and vice versa Note that only ECC key curves and lengths of P256, P-384 and P-521 are supported.
	PA-9037	The IP address of the client server attempting to logon to payShield Manager is now recorded in the Audit Log.

Deployment Version	Reference	Description
1.13.1 & 1.13.0	PA-13727 PA-13893	Support for the key management of the Pin Verification Key (PVK) using a Key Block LMK is included in this release. The PVK is then used with the standard host commands supporting the IBM 3624 PIN Offset method.
		Host Command 'A0' (Derive Key) now allows derivation of a Session PIN Key Card key (SPKC) from the Master PIN Key Card key (MPKC) using the Italian Standard Key Derivation Method.
		The PVK is then imported or exported encrypted under an SPKC in ANSI X9.17 format using Host Command 'A6' (Import Key) and 'A8' (Export Key).
		The MPKC is imported or exported encrypted under an RSA key using Host Commands 'GI' (Import Key under an RSA Key) and 'GK' (Export Key under an RSA Key).
		Further information is given in the Host Programmer's manual, Section 4.5 and in the Section describing Host Command 'A0' (Derive Key) in the Core Host Commands Manual
		The SPKC is The SPKC is also used to encrypt the PVK for export using ANSI X9.17 format and Host Command A8 (Export Key).
		payShield Manager has now been tested on Linux Ubuntu 20 and MacOS Monterey and Ventura.

8.7   Known Issues

Deployment Version	Reference	Description
1.13.1 & 1.13.0		The SETTIME Console Command cannot be used in the payShield Manager Virtual Console. The payShield Manager user interface can be used to set the time instead.
		The 'NO' Host Command Response has been updated to respond with the 'Number of TCP Sockets' Field with a Length of 4N instead of 2N.

8.7   Known Issues

8.8   Bugs and Errors Corrected

Please note that all bugs and fixes in releases made before this release are included – this includes those in v1.8b.

Deployment Version	Reference	Description
1.13.1	PA-16427	The Australian Standard host command 'I0' (Encrypt a Terminal Key under the LMK) has a bug in the support provided for both Data Block Format 03 and 04. The fix to support random padding in PA-15443 was not implemented correctly for Format 03 and also caused an error when Format 04 is used. This is fixed in this release.
	PA-14188	When using Host Command 'A8' (Export Key), export of a TMK with Thales Key Block Usage '51' was prevented when the Security setting "Enable export of a ZMK" set to NO. The Security Setting is only intended to affect the ZMK (with Thales Key Block usage 'K0' and '52'). This has been corrected in this release
	PA-15559	A problem has been found with the Optional Block Data returned in TR-31 format in one situation when using host command 'A0' (Generate and Export Key). The problem occurred when the length of the 'KS' (Key Set Identifier) Optional Block was set to 'FF'. In this case a truncated (KS) optional Block was returned and the informational 'KV' (Key Version) optional block is omitted. This has been corrected in this release.
1.13.0	PA-14897	OpenSSL has been upgraded to v1.1.1t.
	PA-12461	A problem was found when retrieving the Security Settings from smart card in releases from v1.1a. If Console Command 'QMAC' (MAC addresses of all network interfaces) is disabled and 'QM' (View Management Port Configuration) is enabled, then after retrieving the Security Settings 'QM' is disabled. This is fixed in this release.
	PA-9122	A problem has been fixed in Host Command 'EY' (Verify Signature) where Error 'A8' (Invalid Mode of Use) is returned when using Mode of Use 'V' (Verification Operations)
	PA-13706	The support provided for connection to the German Payment Network using AES has been corrected to allow the AES Master Key (ZKA) to be imported. The AES Master Key provided by the German Payment Network in TR-31 Key Block format includes a Key Set Identifier (KS) Optional Block. This optional block includes printable ASCII characters which are not supported by TR-31 and payShield 10K.

Deployment Version	Reference	Description
		To allow this key to be imported successfully, with this release the contents of this optional block are not imported into Thales Key Block format and the key is imported successfully.
		This change has been made when importing a TR-31 Key Block with Key Usage '11' (ZKA). This key usage is used only for the German GBIC scheme.
		This change is only applicable when the key usage is '11' and for all other key usages, the existing functionality remains unchanged.
	PA-14099	Host Command 'GI' (Import Key Under an RSA Public Key) returns a key block with an incorrect length when used with Optional Blocks. This has been corrected in this release.
	PA-14755	Host Command 'QE' (Generate a Certificate Request) generates a certificate response with OID ECDSA_P256 when key lengths 384 and 512 are used. This has now been fixed.
	PA-14934	A problem has been fixed with the generation a remote Master ZMK (MZMK) for exchange with the Trusted Management Device (TMD) using payShield Manager. It was found that when selecting the TDES algorithm, the parity of the TDES key was not being set correctly.
	PA-13580 PA-15491	A problem with the Host Command 'NI' (Return Network Information) caused the Response Message to report that connections were closed where in fact they were open. This is now fixed.

1.13.0	PA-14761 PA-10899 PA-15482 PA-16230 PA14993 PA-15920 PA-15819 PA-15769	payShield 10K Manuals have been updated for this release to include information on the new features as well as updates as required for the bug fixes listed above. They have also been updated to include several corrections as follows. In summary:
		
		• Core Host Commands Manual:
		   ○ Updated to include information on new features as well as to address several corrections and clarifications
		• Host Programmer's Manual:
		   ○ Section 4.5 Italian Key Derivation updated.
		   ○ Section 15.5.13, Security Settings updated and Appendix J, SNMP Security Setting Reference Numbers added, beginning on page 362
		• Security Operations:
		   ○ Update to Section 12.1.3 Cipher Suite Support
		   ○ Update to Section: 13 Appendix D – Audit Log Messages – to include the client's IP address when login is attempted to payShield Manager - see pages: 100 and 103.
		• Console Manual:
		   ○ SETTIME and GETIME Console Commands updated to include information on the new NTP functionality.

Deployment Version	Reference	Description
1.13.0		○ GK and KE Console Commands updated to include details on selecting the Key Block Version ID when exporting in TR-31 format. ○ Also included are a number of corrections and clarifications. - Installation and User Guide ○ Updates for NTP: Section 9.10.6.4, "General - Date and Time", on page 188 and addition of new chapter: Chapter 17, "Network Time Protocol (NTP)" - Applications Manual: ○ Includes new Section 8 providing Use Cases for the Italian commands and a cross reference between standard and the original custom commands.

9   1500-0037 (v1.8b) – Released July 2023

9.1   Summary

This is a restricted maintenance release for customers who <u>do not</u> require a PCI HSM approved release.

9.2   Version Details

Base Release: 1.8b
Revision: 1500-0037
Deployment Version: 1.12.2 Released July 2023

9.3   PCI HSM Compliance

This software release is an interim maintenance release <u>is not</u> planned to undergo compliance to PCI HSM V3. Customers requiring the fixes included in this release in a PCI HSM approved version should use the next base release planned which is currently v1.9a.

9.4   Manuals

The following payShield 10K manuals should be used with this release:
> 007-001512-008 payShield 10K Installation and User Guide
> 007-001518-008 payShield 10K Host Programmers Manual
> 007-001515-008 payShield 10K Core Host Commands
> 007-001516-008 payShield 10K Legacy Host Commands
> 007-001513-008 payShield 10K Security Operations Manual
> 007-001517-008 payShield 10K Applications Manual
> 007-000997-008 payShield 10K Console Guide
> 007-001443-008 payShield 10K Host Command Examples

9.5   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.

Please note that payShield Manager no longer supports Internet Explorer as this is no longer supported by Microsoft.

Operating System	Windows 10 64-bit			Linux Ubuntu 18 64-bit		macOS Big Sur
Browser	Chrome 64-bit	Firefox 64-bit	Edge 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K v1.8b	☑	☑	☑	☑	☑	☑

9.6   New Functions

None

9.7   Known Issues

Deployment Version	Reference	Description
1.12.1	PA-236	When using payShield Manager to view the Error Log and selecting the "Get More" button in the Status Tab all the information is displayed, but no message is displayed when you have reached the end of the Error Log.
	PA-13706	The support provided for connection to the German Payment Network using AES does not allow the AES Master Key (ZKA) to be imported. The AES Master Key provided by the German Payment Network in TR-31 Key Block format includes a Key Set Identifier (KS) Optional Block. This optional block includes printable ASCII characters which are not supported by TR-31 and payShield 10K. This issue is planned to be fixed in v1.7b. It is not fixed in v1.8a. The fix is also planned to be included in v1.9a.

9.8   Bugs and Errors Corrected

Deployment Version	Reference	Description
1.12.2	PA-15598	When using payShield Manager with Chrome, some GUI elements are not displayed correctly when using the latest Chrome release 114.x.x.x. This has been corrected in this release.
	PA-15454	After a significant number of calls to the following host commands using the ECC algorithm only, a payShield 10K reboot occurred which was recorded in the Audit Log. The reboot took approximately 2-3 minutes and normal service resumes after this completes. The issue occurred after approximately 650 K calls to the FY, EW and EY commands and 250 K calls to the IG host command. This issue was apparent in versions from v1.2a to v1.8a. The host commands impacted are: • FY – Generate ECC Key Pair • IG – Key Derivation using ECC • EW – Generate ECC Signature • EY – Verify ECC Signature The workaround was to schedule a periodic reboot. This is fixed in this release.
	PA-10438	Exporting a TMK in Key Block Format encrypted with a TMK also in Key Block Format is supported in Host Command 'A0' (Generate and Export Key) but gave an error in Host Command 'A8' (Export Key). This has been fixed in this release.
	PA-14459	Host Command 'A0' (Generate and Export Key) gave an error when an attempt is made to export a TAK with key usage M6 encrypted under a TMK in Key Block Format. This is fixed in this release.
	PA-14694	Host Command 'JG' (Translate a PIN from LMK to ZPK Encryption) now supports EBCDIC mode.
	PA-14761	Host Command 'E8' (Generate a KCA and KMACH) which supports the Australian AS2805 standard now correctly supports key schemes K and L.
	PA-15443	Host Command 'I0' (Encrypt a Terminal Key under the LMK) which supports the Australian AS2805 standard now correctly supports random padding.
	PA-15633	The Host Command Examples documentation has been updated to correct a typo in the reference to the IBM 3624 method.

10   1500-0036 (v1.8a) – Released May 2023

10.1   Summary

This is a general release for all customers.

10.2   Version Details

Base Release: 1.8a
Revision: 1500-0036
Deployment Version: 1.12.1 Released May 2023

10.3   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

10.4   Manuals

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

> 007-001512-008 payShield 10K Installation and User Guide
> 007-001518-008 payShield 10K Host Programmers Manual
> 007-001515-008 payShield 10K Core Host Commands
> 007-001516-008 payShield 10K Legacy Host Commands
> 007-001513-008 payShield 10K Security Operations Manual
> 007-001517-008 payShield 10K Applications Manual
> 007-000997-008 payShield 10K Console Guide
> 007-001443-008 payShield 10K Host Command Examples

10.5   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.

Please note that payShield Manager no longer supports Internet Explorer as this is no longer supported by Microsoft.

Operating System	Windows 10 64-bit			Linux Ubuntu 18 64-bit		macOS Big Sur
Browser	Chrome 64-bit	Firefox 64-bit	Edge 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K v1.8a	☑	☑	☑	☑	☑	☑

Note that the version of the payShield Manager Smart Card Bridge Chrome Extension was updated from 1.0.1 to 1.0.6 in the Chrome Store during May 2023. The new version includes support for "Manifest 3" as required by Google, and also updates to the text. There are no changes to the functionality and the new version is compatible with all versions of payShield Manager released for payShield 9000 and payShield 10K.

10.6 New Functions

Deployment Version	Reference	Description
1.12.1	PA-10354	The number of TCP and UDP sessions supported for each host ports has been increased from 64 to 128. Therefore, the total number of TCP and UDP sessions supported by payShield 10K for the two host ports has increased from 128 to 256.
	PA-1493	Host Commands 'LU' (Import an HMAC under a ZMK) and 'LW' (Export an HMAC under a ZMK) have been updated to include the following enhancements: - Support for encrypting an HMAC under an AES ZMK is now included. - The HMAC Key can now be imported and exported in TR-31 format. Please note that only TR-31 format is supported in this release – ISO-20038 specifies a slightly different format and so is not supported.
	PA-14659	An update has been included in Host Command 'B8' (TR-34 Export). When host command 'B8' is Authorised, it now allows export of a 128-bit AES key encrypted using a 2048-bit RSA key when the security setting 'Enforce PCI HSMv3 Key Equivalence for Key Wrapping' is set to YES. NIST determines that 128-bit AES key is stronger than a 2048-bit RSA key and so usually this combination of keys cannot be used when the above security setting is set to YES. However, PCI PIN (and PCI HSM) provide an exception to this restriction for remote distribution using asymmetric techniques.
	PA-12567	Host Command 'CY' (Verify a Card Verification Code/Value) has been enhanced to support CVV validation based on a 16-byte CVV data field instead of providing separate CVV generation fields - PAN, Expiry Date and Service Code. This format was supported in Luna EFT and is included to assist customers migrating to payShield 10K.
	PA-14085	Host Command 'EE' (Derive a PIN Using the IBM Offset Method) has been enhanced to optionally generate an offset using a new PVK. This functionality was supported in Luna EFT and is included to assist customers migrating to payShield 10K.
	PA-14025	PIN Block Tag 'J' Support for Encryption Under an AES LMK. Support for the encryption of PIN Blocks under an AES Key Block LMK for Issuers is provided using an AES Key Block LMK in v1.6a and above. The tag 'M' is used to indicate the PIN Block is encrypted under an AES Key Block LMK using ISO PIN Block Format 4 (Thales PIN Block Format 48). In payShield 9000 and payShield 10K, releases up to and including v1.5a, support was provided for encryption of a PIN Block under an AES Key Block LMK using tag 'J' which indicates the PIN Block is encrypted under a proprietary format. Support for this format was withdrawn in v1.6a. However, to allow customers more time to migrate to the format indicated by tag 'M', tag 'J'

Deployment Version	Reference	Description
1.12.1		is supported as well tag 'M' in v1.8a and a limited number of releases following v1.8a. The re-introduction of support for tag 'J' is designed to allow applications still using this format to continue without changing the application. This also allows the relevant host commands to support both Tag 'J' and tag 'M' to simplify the migration process to tag 'M'. The only exceptions are host commands JC (Translate a PIN from TPK to LMK Encryption) and JE (Translate a PIN from ZPK to LMK Encryption) where the format used is determined from a new Security Setting. There are two differences in the support provided using Tag 'J' when compared to the earlier releases and these are as follows. These both impact host commands JC (Translate a PIN from TPK to LMK Encryption) and JE (Translate a PIN from ZPK to LMK Encryption) only: • A new Security Setting is included to determine whether Tag J'' is used with host commands JC and JE (the other host commands are not affected by this setting): o "Use deprecated proprietary format (Tag J) when using PIN Blocks under AES Key Block LMK" o The default setting is NO, and this indicates Tag 'M' is used. Translation of a PIN Blocks from ISO Formats 0, 1, 3 and 4 (Thales PIN block formats 01, 05, 47 and 48 respectively) to encryption under an AES Key Block LMK using Tag 'J' are no longer allowed if the security setting "Restrict PIN Block Usage for PCI Compliance" is set to YES. Further information is given in the Programmers Manual Section 16.4 where all the details of the host command updates are given. Note that Tag 'J' is NOT described in the Core Host Command Manual as it was felt it was clearer to keep this documented separately.

10.7   Known Issues

Deployment Version	Reference	Description
1.12.1	PA-236	When using payShield Manager to view the Error Log and selecting the "Get More" button in the Status Tab all the information is displayed, but no message is displayed when you have reached the end of the Error Log.
	PA-13706	The support provided for connection to the German Payment Network using AES does not allow the AES Master Key (ZKA) to be imported. The AES Master Key provided by the German Payment Network in TR-31 Key Block format includes a Key Set Identifier (KS) Optional Block. This optional block includes printable ASCII characters which are not supported by TR-31 and payShield 10K. This issue is planned to be fixed in v1.7b. It is not fixed in v1.8a. The fix is also planned to be included in v1.9a.
		After a significant number of calls to the following host commands using the ECC algorithm only, a payShield 10K reboot occurs which is recorded in the Audit Log. The reboot takes approximately 2-3 minutes and normal service resumes after this completes. The issue occurs after approximately 650 K calls to the FY, EW and EY commands and 250 K calls to the IG host command. This issue is apparent in versions from v1.2a to v1.7a deployment version 1.11.2 inclusive. The host commands impacted are: - FY – Generate ECC Key Pair - IG – Key Derivation using ECC - EW – Generate ECC Signature - EY – Verify ECC Signature The workaround is to schedule a periodic reboot.

10.8   Bugs and Errors Corrected

Deployment Version	Reference	Description
1.12.1	PA-12946	Host Command 'BC' (Verify a Terminal PIN Using the Comparison Method) has now been updated to support encryption of a PIN Block under an AES Key Block LMK using Tag 'M'.
	PA-12962	Host Command 'GQ' (Verify a PIN Using the ABA PVV Method) has been updated to address an issue when using PIN Block Formats '4' (PLUS Network) and '48' (ISO PIN Block Format 4). When using these formats error codes 15 and 22 were returned respectively.
	PA-14443	When host commands are supplied using the same TCP/UDP session, an occasional intermittent error is given when using host commands that require the PAN to be supplied in nN format with the ";" delimiter. This is fixed in this release.
	PA-13136	A problem has been fixed with Host Commands 'M6' (Generate MAC) and 'M8' (Verify MAC) host commands. When using AES CMAC, the size of the MAC supplied / returned was restricted to 8 bytes (16 hex digits) whereas the standards place no restrictions on the MAC size. To address this, a new MAC size without a size restriction has been added as follows: • '2': MAC size of 32 hex digits (only valid for MAC Algorithm '6' CMAC) When using the above 'MAC Size' and Mode '0' or '3': • For Host Command 'M6', the MAC returned is 32 H in size • For Host Command 'M8', the MAC supplied is 32 H in size
	PA-13511	Host Command 'GW' (Generate/Verify a MAC) has been updated to support a full-size MAC. A new MAC Mode has been added to support this as follows: • '5': CMAC - 16 bytes (for an AES BDK only)
	PA-13655	Import and export of a key with key usage '25' (Counter Data Encryption Key, CTRDEK) is now supported when using TR-31 in the following host commands: 'A0' (Generate Key), 'A6' (Import Key and 'A8' (Export Key).
	PA-12982	Host Command 'CS' (modify Key Block Header) has been updated to support key usage 'M6' (CMAC).
	PA-8802	Host Command 'EM' (Translate a Private Key) did not allow the exportability field to be changed to 'S' when translating a private key from encryption under a key block LMK to another key block LMK. The exportability field was always set to 'N' irrespective of the input provided in the 'Exportability' Field in the Host Command. This has been fixed in this release.

Deployment Version	Reference	Description
1.12.1	PA-11335	Host Command 'EM' (Translate a Private Key) and Host Command 'EU' (Translate a Public Key) failed when translating Private or Public Key from encryption under a 3DES Double Length LMK to an AES Key Block LMK. This has been resolved in this release.
	PA-13461	The 'BW' Host Command (Translate Keys from Old LMK to New LMK and Migrate to New Key Type) fails after a period of time in some circumstances with Error Code '45' (Invalid key migration destination key type). This has been corrected in this release.
	PA-13020	Host Command 'NI' (Return Network Information) has been updated to return the correct error when one of the following ports is not configured: Host 1, Host 2, or Management. Previous error: 1: Nov 23 13:41:55 2022 ERROR: [Failed to query interface 3] **(Severity: 3**, Code = 0x00000001, Sub-Code = 0x00000001) Corrected error: 1: Jan 19 09:20:42 2023 ERROR: [Failed to query interface 3] (**Severity: 0**, Code = 0x00000001, Sub-Code = 0x00000001)
	PA-13551 PA-14161	A very small number of payShield 10K start to report a "Fan x too fast" error when running the self-diagnostics. Once this error is reported, it is then seen each time the self-diagnostics are run (typically each day). This issue has mainly been seen on PS10-D payShield 10K 10Gb and PS10-F payShield 10K FICON hardware platforms. It is important to note that in this case the error does not impact the operation of the HSM other than generating the error message. The Fan Tray is not faulty and replacing the fan tray does not solve the issue. This issue has been fixed in software in this release. After upgrading to this release, payShield 10K should not start reporting this issue unless there is a genuine fan failure. Any payShield 10K already reporting this issue should no longer report this issue after upgrading.
	PA-13239 (PA-14575)	The following issue occurs when using payShield 10K FICON with Brocade 16G and 32G switches. The issue addressed is that port was assigned as 'G' (General Port) rather than 'F' (FICON Port) after a power-on reset of payShield 10K FICON. This issue was consistently seen with Brocade 16G and 32G switch configurations. This issue could not be reproduced with Cisco 16G or 32G switches. This issue has been fixed in this release.

Deployment Version	Reference	Description
	PA-13954	A problem was found with the FICON interface when rebooting using payShield Manager. The FICON interface was not placed offline during this process. This issue has been fixed in this release.
	PA-12829	A problem has been fixed in payShield Manager whereby in a certain scenario it is not possible to go into Secure Mode without logging out and logging back in again. This occurred if the user logs on, selects the tabs in order from the right-hand tab (i.e., the Virtual Console) to the left-hand tab (i.e., the Summary) and then a second user enters their card to go into Secure Mode.
1.12.1	PA-10233 PA-11766 PA-12645 PA-13024 PA-13957 PA-14042 PA-14084 PA-14549	payShield 10K Manuals have been updated for this release to include information on the new features as well as updates as required for the bug fixes listed above. They have also been updated to include several corrections as follows. In summary: - Core Host Commands Manual: - Updated to include information on new features as well as to address several corrections and clarifications - Host Programmer's Manual: - Update to the description of the Thales Key Block Scheme in Chapter 8 - Section 11 updated to include support for import and export of HMAC keys using TR-31 - New Section 16.4 describing the updates included to support the deprecated legacy PIN Block Format Tag 'J' - Printer and SNMP MIB information updated in Appendices F and H. - Authorised Activities listed in Appendix G now include ECC - Section 2.1 updated to reflect the increase in the number of sessions supported from 64 o 128 - Security Operations: - Update to Cipher Suite Tables in Section 4.3.4 and 11.1.3 - New Section 2 and updates to sections 5.1, 10.4 and 10.5 regarding deployment and use of ACLs - New security parameter added "Use deprecated proprietary format (Tag J) when using PIN Blocks under AES Key Block LMK: Yes or No" - A broken link to the PCI site has been corrected. - Console Manual: - Clarification added that the key management commands do not support HMAC keys - AUDITOPTIONS information corrected. - Information regarding the Error Light removed. - Installation and User Guide - Firewall table added

11   1500-0034 (v1.7b) – Released June 2023

11.1   Summary

This is a general release for all customers.

11.2   Version Details

Base Release: 1.7b
Revision: 1500-0034
Deployment Version: 1.11.4 Released Dec 2023 …   This is 1.11.3 with the addition of 2 fixes only
                         1.11.3 Released June 2023 …   This is base release 1.7a deployment version 1.11.1
                                                       with the addition of 2 fixes only

11.3   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

Note that deployment version 1.11.4 listed above includes specific fixes only to meet the GBIC requirements in Germany and so will be covered by the PCI HSM Certification for v1.7b.

11.4   Manuals

The following payShield 10K manuals should be used with this release:
> 007-001512-007 payShield 10K Installation and User Guide
> 007-001518-007 payShield 10K Host Programmers Manual
> 007-001515-007 payShield 10K Core Host Commands
> 007-001516-007 payShield 10K Legacy Host Commands
> 007-001513-007 payShield 10K Security Operations Manual
> 007-001517-007 payShield 10K Applications Manual
> 007-000997-007 payShield 10K Console Guide
> 007-001443-007 payShield 10K Host Command Examples

11.5   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.

Please note that payShield Manager no longer supports Internet Explorer as this is no longer supported by Microsoft.

Operating System	Windows 10 64-bit			Linux Ubuntu 18 64-bit		macOS Big Sur
Browser	Chrome 64-bit	Firefox 64-bit	Edge 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K v1.7a	☑	☑	☑	☑	☑	☑

11.6   New Functions

None

11.7   Known Issues

Deployment Version	Reference	Description
1.11.3	PA-236	When using payShield Manager to view the Error Log and selecting the "Get More" button in the Status Tab all the information is displayed, but no message is displayed when you have reached the end of the Error Log.

11.8   Bugs and Errors Corrected

Deployment Version	Reference	Description

1.11.4	PA-17208	Host Command 'A0' (Derive and Optionally Export Key) has been updated as follows.
		
		The updates to the command address the feedback provided during approval by GBIC in Germany when using an AES Master Key (i.e. an AES ZKA):
		
		• For the NSP:
		  ○ the NSP is restricted to supporting "send request" messages and "receive response" messages only.
		  ○ derivation of a PIN decryption key is NOT permitted for "receive response" messages.
		  ○ the Network Operator ID_{NO} is NOT required to be supplied for these options.
		
		• For the Acquirer (which requires the Network Operator ID_{NO} to be provided):
		  ○ the Acquirer is restricted to supporting "receive request" messages and "send response" messages only.
		  ○ for the "send response" message, derivation of a PIN Encryption Key is NOT permitted.
		  ○ the Network Operator ID_{NO} is required to be supplied for these options.
		
		To meet the requirements referenced above, the following updates to Host Command 'A0' have been made when using an AES ZKA:
		
		• For the NSP:
		  ○ only ZKA options 7 and 8 are permitted.
		  ○ for ZKA option 8, the derivation of a PIN decryption key is not permitted.
		
		• For the Acquirer:
		  ○ only ZKA options 2 and 5 are permitted.
		  ○ for option 5, the derivation of a PIN encryption key is not permitted.
		
		Please note this update is only planned to be included in the following versions:
		
		• 1.7b (as documented here), 1.9b, 2.0a and releases after 2.0a.
		
		This update is NOT included in:
		
		1.8a, 1.8b or 1.9a.

	PA-15598	When using payShield Manager with Chrome, some GUI elements are not displayed correctly when using the latest Chrome release 114.x.x.x. This has been corrected in this release.

Deployment Version	Reference	Description
1.11.3	PA-13706	The support provided for connection to the German Payment Network using AES has been corrected to allow the AES Master Key (ZKA) to be imported. The AES Master Key provided by the German Payment Network in TR-31 Key Block format includes a Key Set Identifier (KS) Optional Block. This optional block includes printable ASCII characters which are not supported by TR-31 and payShield 10K. To allow this key to be imported successfully, with this release the contents of this optional block are not imported into Thales Key Block format and the key is imported successfully. This change has been made when importing a TR-31 Key Block with Key Usage '11' (ZKA). This key usage is used only for the German GBIC scheme. This change is only applicable when the key usage is '11' and for all other key usages, the existing functionality remains unchanged.
	PA-13461	The 'BW' Host Command (Translate Keys from Old LMK to New LMK and Migrate to New Key Type) fails after a period of time in some circumstances with Error Code '45' (Invalid key migration destination key type). This has been corrected in this release.

12   1500-0033 (v1.7a) – Released November 2022

12.1   Summary

This is a general release for all customers.

12.2   Version Details

Base Release: 1.7a
Revision: 1500-0033
Deployment Version: 1.11.1 Released April 2023 …   This is 1.11.0 with the addition of 1 fix only
                       1.11.0 Released November 2022 …   Feature Release

12.3   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

12.4   Manuals

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

> 007-001512-007 payShield 10K Installation and User Guide
> 007-001518-007 payShield 10K Host Programmers Manual
> 007-001515-007 payShield 10K Core Host Commands
> 007-001516-007 payShield 10K Legacy Host Commands
> 007-001513-007 payShield 10K Security Operations Manual
> 007-001517-007 payShield 10K Applications Manual
> 007-000997-007 payShield 10K Console Guide
> 007-001443-007 payShield 10K Host Command Examples

12.5 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.

Please note that payShield Manager no longer supports Internet Explorer as this is no longer supported by Microsoft.

Operating System	Windows 10 64-bit			Linux Ubuntu 18 64-bit		macOS Big Sur
Browser	Chrome 64-bit	Firefox 64-bit	Edge 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K v1.7a	☑	☑	☑	☑	☑	☑

12.6   New Functions

Deployment Version	Reference	Description

1.11.0	PA-10475
	PA-1569
	PA-11544
		The support provided for the TR-31 Optional Blocks has been enhanced in this release. Now supported are:
		
		• TR-31 Optional Key Block IDs:
		   o IK - Initial Key Identifier for the Initial DUKPT Key
		   o KC - Key Check Value of wrapped key
		   o KP - Key Check Value of the wrapping key
		   o TS - Time Stamp
		• TR-31 Numeric Optional Block IDs
		• TR-31 Extended Numeric Optional Blocks (for host command A8 only)
		
		For further information, please refer to:
		
		• Host Programmer's Manual, Section 11.3
		• Core Host Commands Manual, Host Commands, A0, A8, K8
		• Console Guide, Console Commands KG, KE

	PA-12463 PA-12613	The host command that exports symmetric keys according to the TR-34 standard (B8) has been enhanced as follows: • An AES ephemeral key is now supported (128 bit) • An option to use a Time Stamp to protect against replay attack has been added which can be used instead of using a Random Nonce. Please note that currently the maximum RSA key length supported for the KRD Public Key with Host Command B8 is 2048 bits. This key is used to wrap the AES ephemeral key and therefore the security setting 'Enforce PCI HSMv3 Key Equivalence for Key Wrapping' must be set to No to export an AES Key.
	PA-6725	This release also supports the 10,000 cps performance licence. This gives an approximate number of calls per second for the host commands listed below: • CA - Translate a PIN from TPK to ZPK/BDK (3DES DUKPT) Encryption • CC - Translate a PIN from One ZPK to Another The performance of the other host commands (excluding those listed below) are between 2,500 cps and 10,000 cps. The performance achieved in practice will depend on environment in which the payShield 10K is operating, including network configuration, network traffic, the Host Application and the Host Platform. In particular, the following aspects should be considered to achieve maximum performance: • Sufficient multiple threads should be used • The host interface should have no other traffic • Command/response processing at the host should not introduce any delays • The gathering of Utilization Statistics should be tuned OFF to achieve maximum performance.

Deployment Version	Reference	Description
1.11.0		The following Host Commands are excluded from the performance ratings: • Host Commands generating RSA Keys • Host Commands processing a large amount of data, e.g. commands performing Message Authentication, Message Encryption, Message Hashing Note that 10,000 cps is only available for the Premium package and that payShield 10K FICON Hardware Platform does not support 10,000 cps.
	PA-7363	Support is now provided for connection to the German Payment Network using AES. For AES only, this functionality is provided for customers operating as either a "Network Operator" (NSP) or an "Acquirer" in the GBIC scheme. The Host Commands supporting the scheme are as follows: • 'A0' (Derive Key) – to derive the AES PIN Encryption, Message Authentication and Data Encryption keys from the AES Master Key • 'A0' (Generate Key) – to generate a random AES ZKA Key • 'A6' (Import Key) – to import the AES Master Key in TR-31 format • 'A8' (Export Key) – to export the AES Master Key in TR-31 format • 'BW' (Translate Keys) – to translate the AES Master Key when the LMK is changed • 'BU' – (Generate Key Check Value) – to generate a KCV for the AES ZKA Master Key For further information, please refer to: • Host Programmer's Manual, Section 4.4 • Core Host Commands Manual, for the above Host Commands Please note there is an issue with the support provided with the import of the key provided by the German Payment Network in TR-31 format – see Known issue P-13706. This is planned to be fixed in v1.7b. This fix is not included in v1.8a but will be included in v1.9a.
	PA-12552	Host Command A8 (Export Key) has been enhanced to support the export of AES keys in CBC Format. This requires Authorisation and also the security setting "Key export and import in trusted format only" to be set to No.

12.7   Known Issues

Deployment Version	Reference	Description
1.11.1 & 1.11.0	PA-236	When using payShield Manager to view the Error Log and selecting the "Get More" button in the Status Tab all the information is displayed, but no message is displayed when you have reached the end of the Error Log.
	PA-13551	A very small number of payShield 10K start to report a "Fan x too fast" error when running the self-diagnostics. Once this error is reported, it is then seen each time the self-diagnostics are run (typically each day). This issue has mainly been seen on PS10-D payShield 10K 10Gb and PS10-F payShield 10K FICON hardware platforms. It is important to note that in this case the error does not impact the operation of the HSM other than generating the error message. The Fan Tray is not faulty and replacing the fan tray does not solve the issue. This issue has been fixed in v1.6a deployment version 1.10.4 and v1.8.
	PA-14443	When host commands are supplied using the same TCP/UDP session, an occasional intermittent error is given when using host commands that require the PAN to be supplied in nN format with the ";" delimiter. This issue has been fixed in v1.6a deployment version 1.10.4 and v1.8.
	PA-14575	The following issue occurs when using payShield 10K FICON with Brocade 16G and 32G switches. The issue addressed is that port was assigned as 'G' (General Port) rather than 'F' (FICON Port) after a power-on reset of payShield 10K FICON. This issue was consistently seen with Brocade 16G and 32G switch configurations. This issue could not be reproduced with Cisco 16G or 32G switches. This issue has been fixed in v1.6a deployment version 1.10.3 and v1.8a.
	PA-13954	A problem was found with the FICON interface when rebooting using payShield Manager. The FICON interface was not placed offline during this process. This issue has been fixed in v1.6a deployment version 1.10.2 and v1.8a.
	PA-13706	The support provided for connection to the German Payment Network using AES does not allow the AES Master Key (ZKA) to be imported. The AES Master Key provided by the German Payment Network in TR-31 Key Block format includes a Key Set Identifier (KS) Optional Block. This optional block includes printable ASCII characters which are not supported by TR-31 and payShield 10K. This issue is planned to be fixed in v1.7b. It is not fixed in v1.8a. The fix is planned to be included in v1.9a.

12.8 Bugs and Errors Corrected

Deployment Version	Reference	Description
1.11.1	PA-13136	A problem has been fixed with Host Commands 'M6' (Generate MAC) and 'M8' (Verify MAC) host commands. When using AES CMAC, the size of the MAC supplied / returned was restricted to 8 bytes (16 hex digits) whereas the standards place no restrictions on the MAC size. In order to address this, a new 'MAC size' option without a size restriction has been added as follows: • '2': MAC size of 32 hex digits (only valid for MAC Algorithm '6' CMAC) When using the above 'MAC Size' and Mode '0' or '3': • For Host Command 'M6', the MAC returned is 32 H in size • For Host Command 'M8', the MAC supplied is 32 H in size
1.11.0	PA-12620 PA-12853	The following Host Commands have been updated to address an issue with the functionality to encrypt a PIN Block encrypted under an AES Key Block LMK. The commands now support the input and output of a PIN Block encrypted under a 3DES ZPK/TPK/BDK as follows: PIN Verification: • BE - Verify an Interchange PIN Using the Comparison Method • GU - Verify a PIN using the Encrypted PIN method. PIN Translation: • JC - Translate a PIN from TPK to LMK Encryption • JE - Translate a PIN from ZPK to LMK Encryption • JG - Translate a PIN from LMK to ZPK Encryption
	PA-10415 PA-12446	For customers using the Australian Standard functions (AS2805), Host Command 'RK' (Generate Transaction Response, with Auth Para Generated by Acquirer) has been updated as follows: • This command now supports an option to generate the MAC to the AS2805 standard. The standard specifies the amount(AT) field is right justified and left zero-filled. In previous releases it was only possible to left-justify and right zero-fill this field. • The command now also supports an option not to force odd parity on the 'TK' key as required by the AS2805 standard. In previous releases it was only possible to force odd parity.
	PA-11191	An issue found with Host Command 'G0' (Translate a PIN from BDK to BDK or ZPK Encryption (3DES & AES DUKPT)) has been fixed when using a Destination KSN of '000' with BDK 2.

Deployment Version	Reference	Description
1.11.0	PA-11656	Host Command 'EM' (Translate a Private Key) now supports translation of an RSA Private Key from a Variant LMK to a Key Block LMK in the following situation: • Variant LMK: RSA Private Key with Key Type Indicator '4' (Data encryption/decryption (e.g. TLS/SSL premaster secret) • Key Block LMK: RSA Private Key with Key Usage '06' (Data encryption/decryption (e.g. TLS/SSL premaster secret)
	PA-12433	Host Command 'GI' (Import Key or data under an RSA Public Key) returned error code 'A5' when using stored private key and enabling the security setting "Enforce minimum key strength of 2048-bits for RSA". This has been fixed in this release.
	PA-12860 PA-12865 PA-12937	A number of Host Commands were not operating correctly in EBCDIC mode when using an AES Key Block LMK. These have been fixed in this release: • BA, BG, CE, DE, DG, EE, GA, JA, NG, PE, PG and QK

	PA-3232
	PA-12972
	PA-12591
		payShield 10K Manuals have been updated for this release to include information on the new features as well as updates as required for the bug fixes listed above. They have also been updated to include a number of corrections as follows::
		• Core Host Commands Manual:
		   o Host Command 'PM' (Verify a Dynamic CVV/CVC) to clarify the format of the 'Unpredictable Number' Field.
		   o For Host Commands 'M6', 'M8' and 'MY' an update is included to confirm that if Padding Method = '3', then Mode Flag must be set to '0'
		   o The notes provided with Host Command 'BU' (Generate Key Check Value) have been updated to provide further information on how the key check values are calculated.
		   o Host Command 'KU' (Generate Secure Message (EMV 3.1.1)) has been updated to clarify when the Plain Text Message Data is required.
		In addition, the Installation and User Guide now includes information on the new 'Power Supply Type 2'.

13 1500-0032 (v1.6a) – Released July 2022

13.1 Summary

This is a general release for all customers.

13.2 Version Details

Base Release:	1.6a		
Revision:	1500-0032		
Deployment Version:	1.10.4 Released March 2023 …	This is 1.10.3 with the addition of 2 fixes only
	1.10.3 Released March 2023 …	This is 1.10.2 with the addition of 1 fix only
	1.10.2 Released December 2022 …	This is 1.10.1 with the addition of 2 fixes only
	1.10.1 Released September 2022 …	This is 1.10.0 with the addition of 1 fix only
	1.10.0 Released July 2022 …	Feature Release

13.3 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

Note that all deployment versions listed above include specific bug fixes only and so will be covered by the PCI HSM Certification for v1.6a.

13.4 Manuals

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

> 007-001512-006 payShield 10K Installation and User Guide
> 007-001518-006 payShield 10K Host Programmers Manual
> 007-001515-006 payShield 10K Core Host Commands
> 007-001516-006 payShield 10K Legacy Host Commands
> 007-001513-006 payShield 10K Security Operations Manual
> 007-001517-006 payShield 10K Applications Manual
> 007-000997-006 payShield 10K Console Guide
> 007-001443-006 payShield 10K Host Command Examples

13.5   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.

Please note that payShield Manager no longer supports Internet Explorer as this is no longer supported by Microsoft.

Operating System	Windows 10 64-bit			Linux Ubuntu 18 64-bit		macOS Big Sur
Browser	Chrome 64-bit	Firefox 64-bit	Edge 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K v1.6a	☑	☑	☑	☑	☑	☑

Please note PA-12519 regarding a temporary issue with the availability of the smart card bridge from the Chrome Store has been fixed.

13.6   New Functions

Deployment Version	Reference	Description
1.10.0	PA-7362	For Issuers, support for the encryption of PIN Blocks under an AES Key Block LMK is provided in this release. Please note: • PIN Blocks are encrypted under an AES Key Block LMK in ISO PIN Block Format 4 (Thales PIN Block Format 48) • The tag 'M' is used to indicate the PIN Block is encrypted under an AES Key Block LMK. The following Host Commands are updated: • PIN & Offset Generation: EE, GA, JA, DE, CE, DG • PIN Mailer Printing: PE, PG • Clear PIN: BA, NG • PIN Verification: BC, BE, GU • PIN Translation: JE, JC, JG, QK • LMK Translation: BG Note that the following Host Commands for PIN Solicitation do **NOT** support an AES Key Block LMK as we understand these are no longer used: • PIN Solicitation: OA, RC, QA, QC
	PA-9788	For Issuers, support is provided for the encryption of PIN Blocks under an AES TPK, ZPK or when using a BDK. The following Host Commands are updated: • PIN Generation Host Commands: BK FW • PIN Change Host commands: DU, CU • PIN Verification Host Commands (Standard): BC, BE,DA, EA, CG, EG, DC, EC • PIN Verification Host Commands (DUKPT): GO, GQ, GS, GU • PIN Translation: JE, JC, JG • Host Commands Used For Updating PIN on EMV Card: KU, KY • Host Command Used For Generation of Digitized Single Use Keys (SUKs) for Cloud Based Payments: IY
	PA-11740	payShield Manager now supports Microsoft Edge. Please note: • The latest version of Microsoft Edge based on Chromium only is supported • Support is provided when using Edge on Windows 10 only • The Thales Bridge extension is installed from the Chrome store and not the Microsoft store • Please note there is a temporary issue with the Bridge in the Chrome Store – see Known Issues.

Deployment Version	Reference	Description
1.10.0	PA-10596	SNMP Enhancements for payShield Monitor. Enhancement in payShield 10K MIB to allow customers to obtain the following additional information: 1. MIB for maximum limit of error and audit logs. 2. MIB for monitoring host machines and their respective load. 3. MIB for hash for following configurations of HSM. • Security Settings • General Settings • Configure Commands • Audit Settings • LMK
	PA-10517	Secure Host Communications using TLS. The SHA-1 cipher suites have been removed and so can no longer be used.
	PA-9938	Two new Security Settings have been added in this release order to comply with the GBIC requirements in Germany. These are: **Return PIN Length in PIN Translation Response: Yes or No** This setting should be set to YES for backward compatibility. If set to YES, the PIN length will be returned in the Host Commands AQ, CC, CA and G0. This setting should be set to NO if the PIN Length returned in the Host Commands below is not required, or to comply with the requirements of the German Banking Industry (GBIC). **Enable PIN Translation to BDK Encryption: Yes or No** This setting should be set to YES for backward compatibility. If set to YES, translation to BDK encryption is enabled for Host Commands CA and G0. This setting should be set to NO if translation to BDK encryption is not required, or to comply with the requirements of the German Banking Industry (GBIC). Please note that in addition meet the requirements of the German Certification Scheme (GBIC), Host Command 'A0' has been updated to restrict the mode of use that can be specified for the keys that are derived from the ZKA Master Key. This update is also included in v1.5a deployment version 1.9.0. The change ensures: • The sender must use ZKA Option 1 to generate a random RNDI and can only use the derived keys for encryption and MAC generation operations as appropriate for the key type specified. • The receiver must use ZKA Option 0 with the RNDI supplied by the sender and can only use the derived keys for decryption and MAC verification operations as appropriate for the key type specified. The restrictions imposed for ZKA Option '1' and '0' are given below and are detailed in the payShield 10K Core Host Commands Manual for Host

Deployment Version	Reference	Description
1.10.0		Command 'A0'. Please also see below for a temporary removal of some of these restrictions in deployment version 1.9.2. '0': Derive one of the following "receive" keys using supplied RNDI: • PIN Decryption Key (Key Usage="72", Mode Of Use="D") • Data Decryption Key (Key Usage="22", Mode Of Use="D") • MAC Verification Key (Key Usage="M3", Mode Of Use="V") '1': Derive one of the following "send" keys using new RNDI: • PIN Encryption Key (Key Usage="72", Mode Of Use="E") • Data Encryption Key (Key Usage="22", Mode Of Use="E") • MAC Generation Key (Key Usage="M3", Mode Of Use="G")
	PA-1377	Derivation of data encryption keys from the Master Key to the Italian Standard. Host Command A0 now support the derivation of a Terminal Encryption Key (TEK) from the Master MKPOS/MKSER to the Italian Standard. Please note that generation, import and export of the Master MKPOS/MKSER (key usage 57) is only supported in the following host commands: • A0 (Generate Key) • GK (Export Key under an RSA Public Key) • A6 (Import Key) • A8 (Export Key) • BW (Translate Key from Old LMK to New LMK). Note that for host command BW, only translation from Key Block LMK to Key Block LMK is supported for this key – as this key is not supported in base when using a variant LMK, translation using a Variant LMK is not supported.
	PA-8358	Canadian Interac Debit Card ARQC verification and ARPC generation is supported in this version, as specified for the Canadian domestic Interac debit card. This is implemented in the KW Host Command (ARQC Verification and/or ARPC Generation).

13.7   Known Issues

Deployment Version	Reference	Description
1.10.4, 1.10.3, 1.10.2, 1.10.1, 1.10.0	PA-236	When using payShield Manager to view the Error Log and selecting the "Get More" button in the Status Tab all the information is displayed, but no message is displayed when you have reached the end of the Error Log.

13.8   Bugs and Errors Corrected

Deployment Version	Reference	Description
1.10.4	PA-13551	A very small number of payShield 10K start to report a "Fan x too fast" error when running the self-diagnostics. Once this error is reported, it is then seen each time the self-diagnostics are run (typically each day). This issue has mainly been seen on PS10-D payShield 10K 10Gb and PS10-F payShield 10K FICON hardware platforms. It is important to note that in this case the error does not impact the operation of the HSM other than generating the error message. The Fan Tray is not faulty and replacing the fan tray does not solve the issue. This issue has been fixed in software in this release. After upgrading to this release, payShield 10K should not start reporting this issue unless there is a genuine fan failure. Any payShield 10K already reporting this issue should no longer report this issue after upgrading.
	PA-14443	When host commands are supplied using the same TCP/UDP session, an occasional intermittent error is given when using host commands that require the PAN to be supplied in nN format with the ";" delimiter. This is fixed in this release.
1.10.3	PA-14575	The following issue has been addressed when using payShield 10K FICON with Brocade 16G and 32G switches. The issue addressed is that port was assigned as 'G' (General Port) rather than 'F' (FICON Port) after a power-on reset of payShield 10K FICON. This issue was consistently seen with Brocade 16G and 32G switch configurations. This issue could not be reproduced with Cisco 16G or 32G switches.
1.10.2	PA-13136	A problem has been fixed with Host Commands 'M6' (Generate MAC) and 'M8' (Verify MAC) host commands. When using AES CMAC, the size of the MAC supplied / returned was restricted to 8 bytes (16 hex digits) whereas the standards place no restrictions on the MAC size. In order to address this, a new MAC size without a size restriction has been added as follows:

Deployment Version	Reference	Description
		• '2': MAC size of 32 hex digits (only valid for MAC Algorithm '6' CMAC) When using the above 'MAC Size' and Mode '0' or '3': • For Host Command 'M6', the MAC returned is 32 H in size • For Host Command 'M8', the MAC supplied is 32 H in size
	PA-13954	A problem was found with the FICON interface when rebooting using payShield Manager. The FICON interface was not placed offline during this process. This has been fixed in this release so the FICON card is placed offline when rebooting and is placed back online when the interface is available. Please also see known issue above.
1.10.1	PA-12858	When using a printer with the "Delay" parameter configured using payShield Manager or the Console to a time longer than 100 ms, an error was given in earlier releases. This has been fixed in this release.
1.10.0	PA-7699	An issue with the removal of SNMP users when upgrading software using DHCP has been resolved.
	PA-11553	Host Command 'GW' (Generate / Verify a MAC) has been updated to correct the key derivation algorithm used for AES DUKPT when using bi-directional keys (i.e. BDK-2 and BDK-4).
	PA-8102	Host Command 'KU' (Generate a Secure Message) now correctly changes the PIN when using ISO PIN Block Format 4 (Thales PIN Block Format 48) with Mode 4 and Scheme 1.
	PA-10626	Host Command 'KY' (Generate Secure Message) now supports the correct key derivation algorithm when using Scheme ID 9 (Visa VIS CVN 22)
	PA-10358	The 'IE' Host Command (Prepare Secure Message for Chip Card) now supports DGI length of 3 bytes as required by VISA v2.8.1.
	PA-9891	Host Command 'QE' (Generate Certificate Signing Request) now correctly sets the CSR version to 1 instead of 2.
	PA-10440	Host Command 'B8' (TR-34 Key Export) now correctly now supports EBCDIC.
	PA-10513	Host Command 'B8' (TR-34 Export) now supports Key Block Version ID 'D' (Key block protected using the AES Key Derivation Binding Method) as documented in the Host Command Reference Manual.

Deployment Version	Reference	Description
1.10.0	PA-9925	Host Command 'IG' (Key Derivation using Elliptic Curve Key Agreement) now corrects DES keys for odd parity.
	PA-8485	For customers using the Australian Standard functions (AS2805), an update is included to support the Alternate Variant 'Hb' with Host Command 'PI' (Generate a Set of Terminal Keys) – see the Core Host Commands Manual for further details.
	PA-8786	For customers using the Australian Standard functions (AS2805), Console Command 'EA' (Convert (KEK) ZMK into a KEKr or KWK) is now available.
	PA-10439	Host Command 'A0' now gives Error 17 when attempting to export a ZMK in Key Block Format when the Security setting 'Enable export of a ZMK' is set to NO.
	PA-8080	The following key block keys can now be authorized individually: • K0 (KEK Generic) • 53 (ZKA Master Key) • E7 (EMV/Master Personalization Key) • K1 (KEK Generic)
	PA-8823	For a customer with custom software, key type 604 can now be authorized individually when using the Console or Host Commands.
	PA-12261	When using the Hosted HSM functionality, when calling the OOB performance endpoint with LMK=1, a combination of 1 Key Block LMK and 1 Variant LMK is now allowed instead of 1 x Key block or 1 x Variant LMK.

	PA-9002
	PA-10394
	PA-11422
	PA-11010
	PA-11132
	PA-11500
	PA-11609
	PA-4754
	PA-11397
		payShield 10K Manuals have been updated for this release as follows:
		
		• Security Operations:
		   o Further information on the Audit Trail has been added.
		   o Error Log information has been moved to the Installation and User Guide.
		   o The certification section has been updated.
		   o Two new Security Settings have been added that are required for GBIC in Germany.
		• Host Command Examples:
		   o This is now added to the manual set, using the same examples as provided with payShield 9000
		
		All other manuals include a number of updates, corrections and clarifications.

14   1500-0031 (v1.5a) – Released March 2022

14.1   Summary

This is a general release for all customers.

14.2   Version Details

Base Release:	1.5a		
Revision:	1500-0031		
Deployment Version:	1.9.2 Released May 2022	…	This is 1.9.0 with the addition of 9 fixes only (5 customer related fixes and 4 internal fixes)
	1.9.0 Released March 2022	…	Feature Release

14.3   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

Note that deployment version 1.9.2 listed above includes specific bug fixes only and so will be covered by the PCI HSM Certification for v1.5a.

Also note that a later deployment release (1.9.7) has been made but this is a restricted release specific customers only – it is not for general release.

14.4   Manuals

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

> 007-001512-005 payShield 10K Installation and User Guide
> 007-001518-005 payShield 10K Host Programmers Manual
> 007-001515-005 payShield 10K Core Host Commands
> 007-001516-005 payShield 10K Legacy Host Commands
> 007-001513-005 payShield 10K Security Operations Manual
> 007-001517-005 payShield 10K Applications Manual
> 007-000997-005 payShield 10K Console Guide

14.5   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.

Please note that payShield Manager no longer supports Internet Explorer as this is no longer supported by Microsoft.

Operating System	Windows 10 64-bit		Linux Ubuntu 18 64-bit		macOS Big Sur
Browser	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit
payShield 10K v1.5a	☑	☑	☑	☑	☑

14.6   New Functions

Deployment Version	Reference	Description
1.9.0	PA-1633	Remote configuration of the Trusted Management Device (TMD) using payShield Manager. The Trusted Management Device (TMD) is a separate product provided by Thales for use together with payShield 10K. The TMD is used to securely manage key components to meet the latest requirements from PCI. In this release of payShield 10K Software, a new method of setting up the initial key (MZMK) is provided in payShield Manager. This is provided to share the MZMK between payShield 10K and the TMD. This allows the TMD to be used entirely remotely from payShield 10K. In previous releases, a visit to the datacentre was required to store the MZMK in components on smart card using payShield 10K to share with the TMD. The new method to exchange the MZMK uses the Elliptic Curve Key Agreement Algorithm (ECKA) and is carried out as follows: • Use the TMD to generate an ECC key pair and export the Public Key • Use payShield Manager to import the TMD Public Key, to generate the MZMK and to export the MZMK derivation data • Use the TMD to import the MZMK derivation data and derive the MZMK The new feature is provided in the "Manage MZMK" option in the "Configuration Tab" in payShield Manager. Further information is given in the Install and User Guide Sections 1.11 and 9.10.11. Some background information on ECKA is also provided together with the 'IG' Host Command in the Core Host Commands manual. Please note that to use this feature also requires the next release of the TMD software which will be available soon.

Deployment Version	Reference	Description
1.9.0	PA-9811 PA-7950	Support for a new payShield Manager smart card is included in this release. The is smart card will be available later in 2022 and provides the same functionality as the existing payShield Manager smart cards except that it can only used with payShield 10K software v1.5a and above. The smart card can be identified easily as new graphics are used as follows: The new smart card will be available later using the following part numbers: • 971-000176-001 - PS10-RMGT-PM6 - payShield Manager Smart Cards x 6 for Software v1.5a and above • 971-000177-001 - PS10-RMGT-PM30 – payShield Manager Smart Cards x 30 for Software v1.5a and above
1.9.0	PA-9303	To meet the requirements of the German Certification Scheme (GBIC), Host Command 'A0' has been updated to restrict the mode of use that can be specified for the keys that are derived from the ZKA Master Key. The change ensures: • The sender must use ZKA Option 1 to generate a random RNDI and can only use the derived keys for encryption and MAC generation operations as appropriate for the key type specified. • The receiver must use ZKA Option 0 with the RNDI supplied by the sender and can only use the derived keys for decryption and MAC verification operations as appropriate for the key type specified. The restrictions imposed for ZKA Option '1' and '0' are given below and are detailed in the payShield 10K Core Host Commands Manual for Host Command 'A0'. Please also see below for a temporary removal of some of these restrictions in deployment version 1.9.2. '0': Derive one of the following "receive" keys using supplied RNDI: • PIN Decryption Key (Key Usage="72", Mode Of Use="D") • Data Decryption Key (Key Usage="22", Mode Of Use="D") • MAC Verification Key (Key Usage="M3", Mode Of Use="V") '1': Derive one of the following "send" keys using new RNDI: • PIN Encryption Key (Key Usage="72", Mode Of Use="E") • Data Encryption Key (Key Usage="22", Mode Of Use="E") • MAC Generation Key (Key Usage="M3", Mode Of Use="G")
1.9.2	PA-11686	Following customer feedback, to allow customers further time to update their applications to meet the restrictions noted above, some restrictions have been removed in deployment version 1.9.2. This is a temporary measure and the restrictions imposed in PA-9303 above will be reinstated in v1.6a. '0': Derive one of the following "receive" keys using supplied RNDI: • PIN Decryption Key (Key Usage="72", Mode Of Use="D" or "N") • Data Decryption Key (Key Usage="22", Mode Of Use="D" or "N") • MAC Verification Key (Key Usage="M3", Mode Of Use="V", "G" or "N") '1': Derive one of the following "send" keys using new RNDI:

Deployment Version	Reference	Description
		• PIN Encryption Key (Key Usage="72", Mode Of Use="E" or "N") • Data Encryption Key (Key Usage="22", Mode Of Use="E" or "N") • MAC Generation Key (Key Usage="M3", Mode Of Use="G" or "N")
1.9.0	PA-8174	The two cipher suites below are available for use with TLS when using the Ethernet Host Port: • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
1.9.0	PA-536	The version of AngularJS used with payShield Manager has been updated to the latest version - v1.8.2.

14.7   Known Issues

Deployment Version	Reference	Description
1.9.0 & 1.9.2	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.
1.9.0 & 1.9.2	PA-11609	The manual for Host Command 'M6' (Generate MAC) does not specify the message length should be a multiple of 16 when using Input Format Flag '1' (Hex-encoded binary), MAC Algorithm '3' (ISO 9797 MAC Algorithm 3) and Padding Method '0' (No padding).

14.8   Bugs and Errors Corrected

Deployment Version	Reference	Description
1.9.2	PA-10999	After a significant number of SNMP requests are made to payShield 10K, a payShield 10K reboot occurs. Typically an SNMP request every 5 minutes causes a reboot after approximately 5 months. The reboot takes approximately 1 minute and normal service resumes after this completes. This issue is apparent in versions from v1.2a to v1.5a deployment version 1.9.0 inclusive. To reduce the occurrence of this issue, the number of SNMP requests should be reduced. This issue has been fixed in this release (i.e. v1.5a deployment version 1.9.2).

Deployment Version	Reference	Description
	PA-7583	Host Command 'M6' (Generate MAC) occasionally failed with an error when using Input Format Flag '1' (Hex-encoded binary), MAC Algorithm '3' (ISO 9797 MAC Algorithm 3) and Padding Method '0' (No padding) when the message length is not a multiple of 16 as required. This has been fixed in this release.
	PA-8224	When using Custom Software, the SNMP GET request "payShieldEnabledHostCommandsList.0" is now correctly showing custom commands which were missing in earlier releases.
	PA-10505	With Host Command 'A8', when exporting in TR-31 format with optional header block ID's KS and KV, an error was given when exporting in EBCDIC format. This is corrected in this release.
	PA-11686	See entry in the 'New Functions' section above. This specifies the temporary changes to the restrictions imposed to the mode of use that can be specified for the keys that are derived from the ZKA Master Key in Host Command 'A0'.
	PA-10458	A significant issue is addressed when using Host Command 'QY' (Generate a Dynamic CVV) with a Key Block LMK. Customers using this command are advised to use v1.5a or a later release when using a Key Block LMK. In previous releases, multiple uses of this Host command causes all host commands using a Key Block LMK to respond with Error Code 'AC'. For payShield Manager users, the 'Reboot' option in the 'Status' Tab in the 'Device Information' option can be used to resolve the issue for a short while. For Console Users, a power cycle can be used instead. Customers using a Variant LMK are unaffected by this issue.
	PA-8896	Host Command 'A0' (Generate Key) has been updated to correct an issue when used as follows: - Exporting the key generated in TR-31 format - Using EBCDIC format (instead of ASCII) - Using Optional Header Block IDs 'KS' (Key Set Identifier) and/or 'KV' (Key Block Values) In previous releases, the 'KS' and 'KV' Optional Header Blocks were in ASCII format instead of EBCDIC format.
	PA-10413 PA-8323	Host Command 'B8' (TR-34 Key Export) now correctly supports the Optional Key Usage 'K0' or 'K1'.
1.9.0	PA-10703	For Host Command 'B8' (TR-34 Export), a new Scheme has been added. This supports the update included in the ASC X9 TR 34-2019 Draft Errata (ASC X9 TR 34-2019 Corrigendum).

Deployment Version	Reference	Description
		When Scheme = '2', this is identical to Scheme 1 but in the Response Message, the ASN.1 encoded `EncryptedContent` element is a sibling of the `ContentEncryptionAlgorithm` element instead of a child of the element.
	PA-4369	An update is included with Host Command 'BA' (Generate an IBM PIN Offset (of a customer selected PIN)) to correct the mode of use supported from 'V' to 'G'. This command now supports mode of use 'C', 'G', and 'N' instead of 'C', 'V' and 'N'
	PA-8834	Host Command 'BU' (Generate a Key Check Value) now correctly returns a key check value for an HMAC when using a key block LMK. In previous releases, error A7 was given.
	PA-8924	Host Command 'BW' (Translate Keys from Old LMK to New LMK and Migrate to New Key Type) now prevents translation of a key from encryption under a Variant LMK to encryption under a Key Block LMK with an Optional Header Block Key Status of 'T' (Test).
	PA-8635	For Host Command 'EI' (Generate RSA Key Pair, the activities 'generate.05.host' and 'generate.06.host' can now be authorized in the same way as 'generate.03.host' when using a key block LMK.
	PA-9674 PA-9784	Host Command 'EK' now correctly loads the following RSA Private Keys into key change storage. In previous releases Error Code '03' was given: • RSA Key pair generated using host command 'EI' with Key Type Indicator '1' (key pair used for key management only) • RSA key pair generated with Key Type Indicator '5' (key pair used for PIN encryption/decryption).
	PA-5048	When using Host Command 'IC' (Establish Secure Session with Chip Card), with an AES Key Block LMK and Secure Channel Method 1, Error 26 was returned. This is now fixed in this release.
	PA-1566	An issue when using a Key Block LMK has been fixed with Host Command 'K2' (Verify Truncated Application Cryptogram (Mastercard CAP))
	PA-10396	An issue with Host Command 'KO' (Generate Card RSA Key Set and Public Key Certificate) has been resolved where very infrequently an erroneous response is given.
1.9.0	PA-10309 PA-10312	An issue with the key derivation method used when using BDK-2 and BDK-4 has been fixed with Host Command 'M0' (Encrypt Data Block), 'M2' (Decrypt Data Block), 'M4' (Translate Data Block), 'MY' (Verify and Translate a MAC) and 'GW' (Generate/Verify a MAC).

Deployment Version	Reference	Description
	PA-7444	When using the Console Command 'VR' (View Revision), the Elliptic Curve Algorithm (ECC) is now listed.
	PA-4347	When using a printer connected to payShield 10K, the printer settings now do not need to be re-entered when the printer is rebooted.
	Various	payShield 10K Manuals have been updated for this release as follows: • The Core Host Commands Manual includes a number of updates, corrections and clarifications in particular: o An update for Host Command A0 regarding the ZKA Option o An update to Host Command B8 which now includes Scheme 2 and improved descriptions of Scheme 0 and 1. o An AES DUKPT Key Usage Indicator table added in Section 5.6 • All other manuals include a number of updates, corrections and clarifications.

15   1500-0030 (v1.4a) – Released Sept 2021

15.1   Summary

This is a general release for all customers.

15.2   Version Details

Base Release: 1.4a

Revision: 1500-0030

Deployment Version: 1.8.3 Released December 2021 ….   This is 1.8.2 with the addition of 3 fixes only

1.8.2 Released November 2021 ….   This is 1.8.1 with the addition of 2 fixes only

1.8.1 Released October 2021   ….   This is 1.8.0 with the addition of 2 fixes only

1.8.0 Released September 2021 …   Feature Release

15.3   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

Note that all deployment versions listed above include specific bug fixes only and so will be covered by the PCI HSM Certification for v1.4a.

15.4   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

15.5   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	☑	☑	☑	☑	☑	☑

15.6   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.

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

Deployment Version	Reference	Description
		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.

15.7 Known Issues

Deployment Version	Reference	Description
1.8.0, 1.8.1 & 1.8.2	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.

15.8 Bugs and Errors Corrected

Deployment Version	Reference	Description
1.8.3	PA-6865 PA-8400 PA-10487	An issue has been fixed in payShield Manager when using the Thales (Gemalto) IDBridge CT700 Smartcard Reader with PIN Pad. This smart card reader will soon be available in the payShield Manager Starter Pack and also be available to be purchased separately and will replace the existing reader. For further information on this smart card reader please see: https://cpl.thalesgroup.com/resources/access-management/idbridge-ct700-product-brief The driver for the IDBridge CT700 Smartcard Reader for Windows is available using the following link: https://supportportal.gemalto.com/csm?sys_kb_id=68db1c5edb9bbe40d298728dae9619e9&id=kb_article_view&sysparm_rank=1&sysparm_tsqueryId=794215c6db544110f0e32208059619cd&sysparm_article=KB0015847 The driver for Linux and MacOS are included with the operating systems.

Deployment Version	Reference	Description
1.8.2	PA-8956	Digital signatures were occasionally generated and verified incorrectly when using the Elliptic Curve Cryptographic (ECC) algorithm. This has been fixed in this release. *Customers using ECC should upgrade to this or a later release.* This issue impacts the following functionality: • Host Commands supporting the ECC algorithm. • TLS connections when using an ECC cipher suite. The impact seen here is that the payShield 10K response is occasionally rejected by the TLS client and vice versa in v1.2a and above.
	PA-10257	The following problem has been fixed in this release. This only occurs on the PS10-D payShield 10K 10Gb Ethernet Hardware Platform: • Occasionally the payShield 10K 10Gb Ethernet link goes down and requires the unit to be rebooted to recover. • This has been seen occasionally when the 10Gb Transceivers have been swapped and also when the network switch has been powered off and then on.
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.
	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.

Deployment Version	Reference	Description
		• QE Generate a Certificate Request • 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:
		   ○ AES PIN encryption keys can only be used with PIN Block ISO Format 4.
		   ○ 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.

16   1500-0029 (v1.3d) – Released August 2021

16.1   Summary

This is a general release for all customers.

16.2   Version Details

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

16.3   PCI HSM Compliance

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

16.4   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

16.5   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	☑	☑	☑	☑	☑	☑

16.6   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.

16.7   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.

16.8   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.

17   1500-0026 (v1.3b) – Released June 2021

17.1   Summary

This is a general release for all customers.

17.2   PCI HSM Compliance

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

17.3   Version Details

Base Release: 1.3b
Revision: 1500-0026
Deployment Versions: 1.6.2 Released July 2021   ….   This is 1.6.1 with the addition of 3 fixes only
                       1.6.1 Released June 2021   ….   Feature Release

17.4   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

17.5   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	☑	☑	☑	☑	☑	☑

17.6   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.

17.7   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.

17.8   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

18   1500-0025 (v1.3a) – Released for Restricted Distribution April 2021

18.1   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.

18.2   Version Details

Base Release: 1.3a
Revision: 1500-0025
Deployment Version: 1.6.0 Released April 2021   ….   Maintenance Release - Restricted

18.3   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

18.4   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	☑	☑	☑	☑	☑	☑

18.5   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:
		   ○ payShield 10K should first be upgraded to v1.3a using payShield Manager or the Console in the usual way.
		   ○ a Factory Reset should then be undertaken with v1.3a loaded.
		   ○ 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:
		   ○ 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
		   ○ a Factory Reset should then be undertaken with v1.3a loaded.
		   ○ 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.

18.6   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.

19   1500-0024 (v1.2a) – Released Feb 2021

19.1   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

19.2   Version Details

Base Release: 1.2a
Revision: 1500-0024
Deployment Versions: 1.5.3 Released June 2021   ….   This is 1.5.2 with the addition of 1 fix only

                       1.5.2 Released April 2021 ….   This is 1.5.1 with the addition of 1 fix only
                                                       (For restricted distribution)

                       1.5.1 Released Feb 2021   ….   This is 1.5.0 with the addition of 1 fix only
                                                       (For custom software only)

                       1.5.0 Released Feb 2021   ….   Feature Release

19.3   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

19.4   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	☑	☑	☑	☑	☑	☑

19.5   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.

19.6   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.

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

20   1500-0023 (v1.1a) – Released August 2020

20.1   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

20.2   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

20.3   Manuals

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

20.4   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.

20.5   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.

20.6 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.

21   1500-0022 (v1.0f) – Released April 2020

21.1   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

21.2   Version Details

Base Release: 1.0f

Revision: 1500-0022

Deployment Version: 1.3.2 Released April 2020   ….   This is 1.3.0 with the addition of 1 fix only

21.3   Manuals

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

21.4   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".

22   1500-0021 (v1.0e) – Released March 2020

22.1   PCI HSM Compliance

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

22.2   Version Details

Base Release: 1.0e

Revision: 1500-0021

Deployment Versions: 1.3.0 Released March 2020   ….   Maintenance Release

22.3   Manuals

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

22.4   New Functions

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

22.5   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

23   1500-0020 (v1.0d) – Released Dec 2019

23.1   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

23.2   Version Details

Base Release: 1.0d

Revision: 1500-0026

Deployment Version: 1.2.5 Released December 2019   ….   Feature Release

23.3   Manuals

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

23.4   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

23.5   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.

24 1500-0010 (v1.0c) – Released April 2019

24.1 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

24.2 Manuals

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

24.3 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

24.4 Bug Fixes and Errors

Reference	Description
PA-799	Fixed error log entries from factory

25 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)
Auxiliary 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	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
Maximum performance	1500 tps	2500 cps (calls per second)
PCI HSM certification	Yes PCI HSM Version 1.0 (selected hardware &	Yes PCI HSM Version 3.0

Function/Feature	payShield 9000	payShield 10K
	software versions) Expires end of April 2019	(Selected software versions)
FIPS Certification	FIPS 140-2, Level 3	FIPS 140-2, Level 3

Function/Feature	payShield 9000	payShield 10K

26   Technical Support Contacts

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

https://supportportal.thalesgroup.com/csm

THALES