THALES

cpl.thalesgroup.com

payShield 9000 Release Note Base Software Version 3.5b

PPRN0523-079

24 February 2021

Contents

Notice

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

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

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

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

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

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

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

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

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

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

Follow this link to find the End User Licensing Agreement:

https://cpl.thalesgroup.com/legal/eula

Introduction

This payShield 9000 release note contains details of the following subjects:

- Enhancements and bug fixes
- Known significant issues in base software
- Compatibility information
- Manuals version to be used.
- Other useful information

Latest Software Numbers

Version 3.5 Development Stream	**1407-x925 (v3.5b)**
Version 3.4 Development Stream	**1407-x917 (v3.4c)**
Version 3.3 Development Stream	**1407-x911 (v3.3b)**
Version 3.2 Development Stream	**1407-x908 (v3.2c)**
Version 3.1 Development Stream	**1407-x905 (v3.1d)**
Version 3.0 Development Stream	**1407-x901 (v3.0b)**
Version 2.4 Development Stream	**1346-x922 (v2.4c)**
Version 2.3 Development Stream	**1346-x917 (v2.3f)**
Version 2.2 Development Stream	**1346-x911 (v2.2b)**
Version 2.1 Development Stream:	**1346-x907 (v2.1d)**
Version 2.0 Development Stream:	**1346-x904 (v2.0c)**
Version 1.4 Development Stream:	**1317-x922 (v1.4g)**
Version 1.3 Development Stream:	**1317-x915 (v1.3e)**
Version 1.2 Development Stream:	**1317-x900 (v1.2a)**
Version 1.1 Development Stream:	**1110-0921 (v1.1b)**
Version 1.0 Development Stream:	**1110-0914 (v1.0f)**

Important Notes

1. See the table in the section "payShield Manager Compatibility Information" later in this document for an overview of compatibility between payShield Manager environments (operating systems, browsers, etc.) and payShield 9000 software (v3.x only).
2. See the table in the section "Local & Remote HSM Manager Compatibility Information" later in this document for an overview of compatibility between HSM Manager software and payShield 9000 software (v1.x and v2.x only).

3. Because different software versions (e.g. v1.0 and v1.1) 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. The entries below now provide information for this situation to be understood.
4. Within a software version (e.g. v1.1) there may be some instances where changes in one release are not included in a later release. This is explained in the entries for the relevant releases.
5. The term "Limited release only" below means that the software release was a maintenance release which was not generally distributed but was available to customers who experienced any issues that the release addressed and required an urgent resolution. Such releases may have had limited system testing.
6. The term "Special request only" below identifies versions which relate to published Security Advisories. These versions are available if a request is made to users' Thales account managers or resellers, or (in the case of a software download) to Thales Support.

PCI HSM Compliance

Selected versions of payShield 9000 from v1.2a will be certified to the PCI HSM requirements. Please note the following:

1. The information below for each release indicates which versions of payShield 9000 software are certified to PCI HSM. For handy reference, a table of the compliances is included in the sub-section "PCI HSM Certified versions of payShield 9000 base software" towards the end of this document.
2. 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 given compliant values.
3. PCI HSM compliance requires that the HSM is delivered in a compliant method. Any order for a payShield 9000 that is required to be PCI HSM compliant must specify that PCI HSM compliance is required.
4. As an indicator that the software is certified and all the settings are compliant, the software revision number (accessible using, for example, the VR Console command) changes from format nnnn-09nn to format nnnn-19nn. If VR shows a software revision in the format nnnn-09nn then that version of payShield 9000 software is not PCI HSM certified and/or some settings are not compliant.
5. Information about PCI HSM is included with the manuals for payShield 9000 v1.2a onwards – for example, see Chapter 10 of the *payShield 9000 General Information Manual*. You can also find information in the Chapter 18 of the *payShield 9000 Host Programmer's Manual*.
6. Where Local or HSM Manager is to be used with a payShield 9000 that is required to be PCI HSM compliant then the appropriate version of HSM Manager (as defined in the section on *Local & Remote HSM Manager Compatibility Information*) must be used.

Upgrading software on existing payShield 9000 units

Where it is required to update the software on a payShield 9000 which is already in use, users with appropriate support contracts with Thales may be able to acquire the new software at no cost.

Different classes of Thales support contracts are available. All entitle the user to both minor release updates (e.g. from v**1**.0a to **1**.0b or from v**1**.0a to v**1**.3f), and major release updates (e.g. from v**1**.3f to v**2**.0a).

Users who do not have an appropriate support contract can purchase a license for the updated software by ordering:

- HSM9-LIC001 where the new software is in the v1 range, or
- HSM9-LIC001Vx (x = 2 or more) where the new software is in the vx range or
- HSM9-PAC30x (x = 1, 2 or 3) where the new software v3 or above

The normal delivery method is by download from the Thales Support site.

Enhancements and Bug Fixes

Version 3.5 Development Stream

Note: When Thales ships a payShield 9000 HSM pre-loaded with v3.X software, a certificate will be installed inside the HSM (known as a 'warrant') to enable remote commissioning of the HSM using payShield Manager. However, remote commissioning is not permitted when an LMK is already installed in the HSM. Therefore, prior to shipping, Thales will not pre-install the Test LMK into any HSM which is loaded with v3.X software.

Relationship to v3.4

All fixes and enhancements in the v3.4 stream up to and including 1407-0917 (v3.4c) are included in v3.5a and v3.5b. Changes in later versions in the v3.4 stream are not included in the v3.5 stream unless these Release Notes explicitly say that they have been included.

1407-0925 (v3.5b) – Released February 2021

PCI HSM Compliant?

This release is not currently planned to be submitted for PCI HSM v1 or AusPayNet certification. Please contact support for further information

payShield Manager Compatibility

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 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 9000 v3.5b	☑	☑	☑	☑	☑	☑

Notes:

- When using MacOS Catalina and Big Sur, there are a few additional steps to be carried out before the landing page can be accessed. Please refer to the Knowledge Base on the support portal for further information.

- A summary of browser compatibility with payShield Manager for each release of payShield 9000 software is given towards the end of this document.
- This version of HSM software is not compatible with HSM Manager. All management activities can be performed using payShield Manager, which is accessed using a regular web browser.

Manuals

- ➢ Issue 38 of the payShield 9000 manuals dated on or after February 2021 should be used with this release.

Enhancements

Ref.	Description
PA-6075	Host Command 'KY' (Generate Secure Message (EMV 4.x)) now supports Destination PIN Block Format Codes '05' (ISO 9564-1 Format 1) and '47' (ISO 9564-1) when a PIN Change is required. Note this update was also included in v3.5a.
PA-7274	Host Command 'QE' has been updated to support a Mode of Use for the Private Key of 'D' (decrypt operations).
PA-4820	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 Australian Standards Reference Manual for further details.
PA-5949 PA-6774	For Card Issuance, Host Command 'IE' has been updated to support longer command lengths. Please refer to the description of the 'Command Length' parameter in the Card & Mobile Issuance Reference Manual. Included in the update is a fix to an issue reported in an earlier v3.5a hot fix which failed to create a single APDU with 1 Byte Length as specified.

Major Bugs and Errors Corrected

Ref.	Description
PA-3165	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: • 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 console manual.

Bugs and Errors Corrected

Ref.	Description
PA-6580 PA-5005	The following 2 issues have 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 PIN Block Format 48. • Issue when translating a PIN Plock from encryption under a TDES key to encryption under and AES key.
PA-5590 PA-2490	The following 2 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 using Host Command 'CC' now gives error 23 if the ZPK in not an AES key.
PA-5712 PA-5978	Host Command 'G0' (Translate a PIN from BDK to BDK or ZPK Encryption) now translates a PIN Block from ISO Format 4 to ISO Format 0.
PA-5620	The Host Command 'KU' (Generate Secure Message) has been updated to fix an issue when using a PIN Block in PIN Block Format 48 (ISO 9564-1 format 4).
PA-6167 PA-6982	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).
PA-4778	An issue with the key derivation method used when using the ASA2805 method to verify a MAC has also been fixed. This is occurred when using BDK-2 and BDK-4 with Host Command 'GW' (Generate/Verify a MAC).
PA-3790	Host Command 'BW' (Translate Keys from Old LMK to New LMK and Migrate to New Key Type) has been updated to support translation of a single length DES CVK which is still used in some legacy systems.
PA-4541	Host Command 'A8' (Export a Key) now allows a TMK to be exported when encrypted under another TMK when using a Key Block LMK (as well as a Variant LMK).
PA-4964	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-5416	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 Host Command Reference Manual.

PA-6564	A fix has been added to host command ‘A0’ (Generate Key) to prevent export of a ZMK when the ‘Enable export of a ZMK’ security setting is set to ‘No’ when exporting to Thales and TR-31 key block.
PA-6581 PA-5974	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 previously in the Host Command Reference Manual. The manual has also been updated to show support for Scheme ‘1’ (X9 TR-34:2019) is provided.
PA-4350	Host Command ‘I8’ (MULTOS ALU Generator) has been updated to correct a padding issue. This occurred if Application Unit size Modulo 8 = 7 and ‘0x80’ is now correctly added as specified in EMV 4.2 and EMV 4.3.
PA-3967	payShield Manager is now prevented from loading settings from smart card when payShield 9000 is in PCI compliant mode.
PA-4112 PA-4824	The following issues reported with the import of a TLS certificate have been resolved when using Console Command ‘SI’ (Import Certificate): • The first issue was that the command was reporting the certificate was imported successfully. However when viewing the certificate using Console Command SV (View Installed Certificates) the certificate was not shown. • The second issue was that the command was reporting the certificate was imported successfully and then the Console became unresponsive requiring a reboot to obtain Console access again.
PA-7131	payShield 9000 Manuals have been updated for this release as follows: • 1270A546-038 Host Command Reference Manual: ○ Support for storage of PINs encrypted under an AES Key Block LMK has been removed in this release. This functionality will now only be provided in payShield 10K in a later release. ○ Updates to Host Commands: ‘A0’, A8’, ‘B8’, ‘EI’, ‘KY, ‘QE’. ○ Corrections to host commands: ‘BY’, N0. ○ Key Usages Indicators used for AES DUKPT added. • 1270A548-038 Card & Mobile Issuance Reference Manual ○ Update to Host Command ‘IE’ • 1270A547-038 Australian Standards ○ Update to Host Command ‘PI’ • 1270A544-038 Console v3.5 ○ Update to Console Command ‘XA’ • 1270A593-038 General Information v3.5

	○ Information on the Trusted Management Device (TMD) has been added.

1407-0921 (v3.5a) – Released May 2020

PCI HSM Compliant?

This software has completed certification to the PCI HSM standard.

HSM Manager Compatibility

This version of HSM software is not compatible with HSM Manager. All management activities can be performed using payShield Manager, which is accessed using a regular web browser.

Manuals

- Issue 38 of the payShield 9000 manuals should be used with this release.

New Functions

Ref.	Description
PA-187	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.
PA-468	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. A 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-2292 PA-1124 PA-3092	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-3193	payShield Manager now also supports Chrome 80. This required the Thales smart card bridge to support the Chrome 'SameSite' feature.
PA-2379	To support customers migrating to an AES Key Block LMK, Host command to Translate Keys from Old LMK to New LMK and Migrate to New Key Type (BW) has been enhanced to allow translation single length PIN Verification Key (PVK) with key type code 002 from 2DES LMK to AES LMK
PA-160	A new license to control FF1 functionality is included in this release.

Significant Corrections to Functionality

Ref.	Description
PA-2675 PA-3223	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) 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.
PA-322	The Korean SEED related host and console commands have been updated to correct an issue found in the implementation of the algorithm.

Bugs and Errors Corrected

Ref.	Description
PA-323	Fix to Console Command RS 'Retrieve HSM Settings from a Smartcard' regarding PCI settings
PA-1333	Host command K2 'Verify Truncated Application Cryptogram (Mastercard CAP)' now returns K305
PA-1374	Fixed issue with Host command I8 'MULTOS ALU Generator' which was returning error 50 - Invalid CRT component length byte contents
PA-3568	Corrected issue with TLS CSRs to fully adhere to PKCS#10 Standard
PA-158 PA-2705	Added support for private key ModeOfUse E in Host Command QE 'Generate a Certificate Request' Also fixed an issue in the user manual with placement of the delimiter in the host command
PA-301	Fixed issue where security scan produces an error
PA-324	Fixed issue with AES keys with host command CS 'Modify Key Block Header'.
PA-516	Manual updated for host command GK regarding MAC verification failure when using LMK Identifier.
PA-756	Fixed issue with generation of IPEK and export in TR-31 format encrypted under a TMK
PA-845	Fixed issue whereby users could change PCI compliant settings while in PCI compliant mode when loading security settings from a smart card
PA-863	A0 host command failing on AES key generation and export fixed
PA-907	ACL list can now be disabled only in secure mode
PA-974	Fixed issue for Key Usage E2 & AES with console command FK
PA-1027	Fixed issue with host command KG with AES LMK
PA-1038	Addressed problem whereby payShield Manager negatively impacts host command processing performance
PA-1127	Bug fixed with host command M0 fixed when generating a key with algorithm 1.
PA-1129	Bug fixed for host command EY which failed to verify a No Hash Signature created with EW
PA-1537	Weak pin checking in user manual removed for host commands DE, CE, and DG as no longer required
PA-1662	Secure Host Communications uses SHA-2 in place of SHA-1
PA-2026	Bug with A6 host command where key 22 was not available for authorisation is fixed.
PA-2564	Intermittent failures to host command PM which verifies a dynamic CVV/CVC fixed
PA-2706	Fixed issue with Translate encrypted PIN to encrypted alphanumeric PIN (ZK) for WEBPIN which returned error 14
PA-3143	Added support for K1 for TR-31 format with host command A0
PA-3217	Fixed issue with BW host command which was returning error BXBD - Incompatible key types
PA-3512	Fixed AES DUKPT MAC Padding Issue
PA-848	Bug fixed where import key fails with error code 17 with single authorisation import.51.host

Ref.	Description
PA-976	A problem with payShield Manager has been fixed where when configuring the host port in payShield manager, if Host port 2 is disabled, validation is still active on the fields, making it impossible to update the host configuration.
PA-1040	Minor memory leak fixed with console commands IK and EA.
PA-1117	Problem with importing AES keys using 05 Optional Header fixed
PA-2363	Host command A6 now supports key blocks with unusually large amounts of padding in the encrypted key section when using AES key
PA-2911	Fixed issue where payShield Manager was not displaying payShield 9000 information correctly on landing page
PA-3288	Authorization of key 103 in both export and generate does not remain after rebooting the HSM, despite persistent setting - Fixed.
PA-3357	Memory issue during stability testing
PA-850	Security Settings Popup warns about erasing KTKs (but doesn't erase KTKs) - Fixed

Known Significant Base Software Issues

The following table lists significant issues which are known to exist in payShield 9000 software and which are not yet resolved. The evaluation of an item as "significant" may change, resulting in items being added to or removed from the list. Items will be removed from the list as they are resolved, and the resolution will be reported in the appropriate Release Note:

Ref.	Description
PA-4715	Software updates require to have enough free memory to load the new firmware file. Should software update fail due to not enough memory it is recommended to clear the system logs: errorlog, auditlog and utilization and reboot the unit.
PA-4450	A reboot is required when returning the network configuration for the host interfaces back from a static ip address to DHCP. This issue was also present in v3.4c. Note that payShield 9000 is initially delivered with DHCP enabled.
PA-2192	The clear button provided for the Virtual Console on payShield Manager does not always clear the contents correctly. The screen is only cleared from the last command up to when a small number of console commands were last used.
PA-4622	payShield Manager very occasionally displays a grey screen for a short while instead of the login page. This also occurred in v3.4c.

Version 3.4 Development Stream

Note: When Thales ships a payShield 9000 HSM pre-loaded with v3.X software, a certificate will be installed inside the HSM (known as a 'warrant') to enable remote commissioning of the HSM using payShield Manager. However, remote commissioning is not permitted when an LMK is already installed in the HSM. Therefore, prior to shipping, Thales will not pre-install the Test LMK into any HSM which is loaded with v3.X software.

Relationship to v3.3

All fixes and enhancements in the v3.3 stream up to and including 1407-0911 (v3.3b) are included in v3.4a. Changes in later versions in the v3.3 stream are not included in the v3.4 stream unless these Release Notes explicitly say that they have been included.

1407-0917 (v3.4c) - Released November 2018

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is not compatible with HSM Manager. All management activities can be performed using payShield Manager, which is accessed using a regular web browser.

Manuals

- Issue 37 of the payShield 9000 manuals should be used with this release.

New Functions

Ref.	Description
PK-2996	Enhanced the host command PM, to support Gemalto dCV dynamic CVV.
PK-3308 PK-3362 PK-3363	Enhanced console commands IK & KE and host commands A6 & A8 to allow import & export of a ZMK under a ZMK.
PK-1187	Enhanced host commands GI & GK to allow import & export of a ZMK under an RSA key.
PK-3299	Enhanced host command L6 to support key usage values 03, 04, 05 & 06.
PK-2834	Enhanced host command IE to also support lengths in TLV format.

Bugs and Errors Corrected

Ref.	Description
PK-776	Fixed issues in console commands KG, IK, KE and host commands A0, A6, A8 in their support of TR-31:2018 with AES transport keys.
PK-3386	Fixed host command A8, which was failing to export an IPEK (when using a Variant LMK).
PK-3357	Fixed console command LK, which was rejecting the standard Thales 3DES triple-length Test LMK when the "Enforce multiple key components" security setting is set to YES.
PK-3301	Fixed host command L6, which was failing to import an RSA private key whose corresponding public key was provided in 2's compliment format.
PK-3438	Fixed host command JG, so that it is no longer dependent on the "Restrict PIN block usage for PCI compliance" setting. (JG should only be dependent on the output PIN block format being PCI approved.)
PK-3380 PK-3419	Fixed an issue when applying security settings, to erase any installed KTKs when the HSM switches to PCI compliant mode.
PK-585	Fixed host commands M6, M8 and MY which were incorrectly returning an 8 byte IV when using AES keys.
PK-3256	Fixed host command IE to accept the SK-DEK key block with a Mode of Use = 'B' or 'E', in order to accept the SK-DEK key block output by host command IC.
PK-3133	Fixed host command CS, which was failing to operate on key blocks with Key Usage = 47, 48 or 49.
PK-3261	Fixed display of FIPS validated algorithms in payShield Manager by removing FF1 and BSP algorithms.
PK-3454	Fixed host command M0, which was causing stability issues with certain payloads.
PK-3350	Fixed the SNMP module, so that changes to the "Enable Single DES" security setting will always send an SNMP Trap.
PK-3410	Modified text in console commands CS/QS, from "Authorized state required when importing DES key under RSA key" to "Authorized state required when importing a key under RSA key" since this setting applies to DES, AES and HMAC keys.
PK-3424	Fixed host command L6, so that the delimiter '~' and its associated fields are optional.
PK-3355 PK-3395	Non-specific code security & stability improvements.

1407-0916 (v3.4b) - Released July 2018

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is not compatible with HSM Manager. All management activities can be performed using payShield Manager, which is accessed using a regular web browser.

Manals

- Issue 36 of the payShield 9000 manuals should be used with this release.

Bugs and Errors Corrected

Ref.	Description
PK-3306	Removed incorrect reference to ECC functionality in console command VR, and in payShield Manager.
PK-3285	Fixed console command SV, so that it now displays all currently installed certificates for securing the management interface using TLS.
PK-3286	Fixed console command SD, so that it is now possible to delete both management and host TLS certificates.
PK-3073	Fixed console command RZ, which was failing with the message 'Card is either not formatted or does not contain CA components'.
PK-3288	Fixed host command GI, which failed when using an RSA private key in key block format with Mode of Use = 'T'.
PK-3292	Fixed issue with payShield 9000 SNMP MIB, which was missing the trap which is sent when the state of the box changes.

1407-0915 (v3.4a) - Released July 2018

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is not compatible with HSM Manager. All management activities can be performed using payShield Manager, which is accessed using a regular web browser.

Manuals

- Issue 36 of the payShield 9000 manuals should be used with this release.

Note: If LIC002 (RSA algorithm) is present, this version of software will report that the RSA and ECC algorithms are both supported. This is incorrect: the ECC algorithm is not supported in this version of software.

New Functions

Ref.	Description
PK-951	Enhanced the host commands A0, G0, GQ, GS, GU, GW, M0, M2, M4 and MY to support for ANSI X9.24-3:2017 AES DUKPT
PK-776	Enhanced the host commands A0, A6, A8 and console commands KG, IK, KE to support X9 TR-31:2018 key block (Key Block Version ID = 'D').
PK-2938	Added new host commands P6 and P8 to support MyPINPad OPIN functionality (PIN on glass).
PK-1007	Enhanced the host command B8 (TR34 Key Export) to support keyblock, 192 bit 3DES key and Version 'D' of TR31.
PK-2837	Enhanced the host commands M0, M2 and M4 to support NIST SP800-38G FF1 Format Preserving Encryption.
PK-802	Enhanced the host command KU to support JCB (CVN 04) and Union Pay.
PK-800	Enhanced the host command KY to support EMV 4.3 AES card and session key derivation and Visa CVN18.
PK-2994	Added a new host command QE to support generation of a CSR of a supplied RSA public key.
PK-2995	Enhanced the host commands EW and EY to support RSA-PSS.
PK-2992	Enhanced the host commands JW and JY to support RSA-PSS.
PK-689	Enhanced the host command BW to optionally return the key check value.
PK-1099	Enhanced the host command NC to return the check value of either the current LMK or the LMK in key change storage.
PK-3027	Enhanced the console command CH to disallow a host connection if there is no LMK installed.
PK-3190	Enhanced the host command QY to support Visa dCVV2 time based dynamic CVV.
PK-1078	Added the ability to generate test LMK cards at the console (via new console command GT) and via payShield Manager.
PK-2937 PK-800 PK-2921	Enhanced the host command KY to support EMV 4.3 Option 'C' (AES keys) and EMV scripting with cards that use EMV Option ‘B’ for DK generation and Visa Proprietary XOR for SK generation (CVN18).
PK-2877	Improve implementation of RSA private keys for TLS pre-master secret decryption.
PK-3110	Any installed KTKs are no longer erased when changing the security related settings or restoring HSM settings.
PK-3119	Restoring security related settings via payShield Manager will now cause installed LMKs to be erased (similar to the console behaviour).
PK-2886	Error log entry date now displays value for the year.

Ref.	Description
PK-2896	Added SNMP Trap for HSM State Change Event (Online/Offline/Secure). Note: CipherTrust Monitor v1.5.1 (or higher) will respond to these traps. Earlier versions will ignore the trap.

Security Enhancements and Fixes

Ref.	Description
PK-2527	Fixed console command SS to save security parameters.
PK-3030 PK-3031	payShield Manager will now prompt for LMK deletion if alarm settings are changed from high to low.
PK-871	FTP service is no longer started when the HSM is put into Secure state via payShield Manager.
PK-3199	Upgraded OpenSSL to 1.0.2o.
PK-3238	Removed "Ingenico BPS Algorithm" from under the list of FIPS validated algorithms (since it is not a FIPS validated algorithm).

Bugs and Errors Corrected

Ref.	Description
PK-774	Fixed an issue in host commands A0/A2/A4/A6/A8 so that Key Usage 23 can be used.
PK-2188 PK-2915	Fixed an issue that was preventing users from being able to cancel HSM authorization via payShield Manager.
PK-3024 PK-2409	Fixed an issue that was causing certain option blocks to fail when importing keys in TR-31 format.
PK-3049	Fixed an issue with host command EM that was causing it to return error code 15.
PK-3115	Fixed an issue with host command KI which was returning errors when using an AES KEK with Mode 'G'.
PK-2984	Fixed collection of health statistics so that the "command chaining" command and all the sub-commands will log as separate commands in the utilization statistics.
PK-120	Fixed issues during saving and restoring configuration data from smart card.
PK-2875	Fixed an issue with the Audit log which was causing the payShield Manager Virtual Console to lock up when 'Continue' was pressed.
PK-3029	Fixed an issue during the saving and retrieving Alarm settings from smartcard.
PK-2431	Fixed an issue in console command VR, which was displaying an incorrect list of licenses.
PK-2983	Fixed an issue where UDP port in netstat reverts to default port 1500 even though host port is set to a different port.
PK-2936	Fixed an issue in payShield Manager which was causing problems when using Windows 10 with IE.
PK-3189	Fixed an issue in console command VC so that it can successfully verify LMKs stored on all types of regular HSM cards.
PK-3036	Enhanced the management port configuration utilities such that any modification to the settings no longer requires the HSM to restart.
PK-3051	Fixed an issue with host command EY which was causing the TCP server to lock up.

Version 3.3 Development Stream

Note: When Thales ships a payShield 9000 HSM pre-loaded with v3.X software, a certificate will be installed inside the HSM (known as a 'warrant') to enable remote commissioning of the HSM using payShield Manager. However, remote commissioning is not permitted when an LMK is already installed in the HSM. Therefore, prior to shipping, Thales will not pre-install the Test LMK into any HSM which is loaded with v3.X software.

Relationship to v3.2

All fixes and enhancements in the v3.2 stream up to and including 1407-0908 (v3.2c) are included in v3.3a. Changes in later versions in the v3.2 stream are not included in the v3.3 stream unless these Release Notes explicitly say that they have been included.

1407-0911 / 1407-1911 (v3.3b) - Released February 2018

PCI HSM Compliant?

- ***This software has been certified for PCI HSM compliance.*** PCI HSM compliance of the payShield 9000 is subject to appropriate user settings having compliant values – see manuals.
- Software number 1407-0911 applies if some security settings are not PCI HSM compliant. Software number 1407-1911 applies if all security settings are PCI HSM compliant: only this software number appears on the PCI certificate. (See manuals)

HSM Manager Compatibility

This version of HSM software is not compatible with HSM Manager. All management activities can be performed using payShield Manager, which is accessed using a regular web browser.

Manuals

- Issue 35 of the payShield 9000 manuals should be used with this release.

Security Enhancements and Fixes

Ref.	Description
PK-2776	Fixed issue in payShield Manager relating to TESA 2017-013.

Bugs and Errors Corrected

Ref.	Description
PK-3059	Fixed issue which (positively) affected the HSM's performance.
PK-2914	Fixed compatibility issue with payShield Manager & Chrome v65.

1407-0910 (v3.3a) - Released December 2017

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is not compatible with HSM Manager. All management activities can be performed using payShield Manager, which is accessed using a regular web browser.

Manuals

- Issue 35 of the payShield 9000 manuals should be used with this release.

New Functions

Ref.	Description
PK-2242 PK-326	Introduce support for "weak PINs" to be identified by a number of rules, rather than an explicit (global or local) list.
PK-229 PK-2026	Extend host command A6 and console command IK to allow a ZEK to be imported using a Key Block LMK.
PK-234 PK-798 PK-799 PK-1116	Extend host commands KW and KI to support AES EMV Master Keys.
PK-238	Extend host command GW to allow an AS2805.4.1 MAC to be generated/verified.
PK-239	Extended AS2805 command set (H8, I0, E8) to support data block format 4 (in H8 and I0), and new key schemes K (in E8 & H8) and L (in E8 only).
PK-247	Introduced support for VISA DSP, including support for VISA Format Preserving Encryption. (This functionality requires its own license, HSM9-LIC039.)
PK-1068 PK-328 PK-759	Modified the list of security settings so that the switch to enable the use of single-DES is included in list of PCI-HSM compliant settings.
PK-760	Extended existing commands for Visa cards to allow for up to 19 digit PANs.
PK-794 PK-1185	Extended host command PM to support Visa LUC with host provided value.
PK-795	Extended host command QY to support Visa Authentication Value (AV).

Ref.	Description
PK-797	Introduce new host commands JW and JY to provide JWT (JSON Web Token) Encode/Decode, supporting GCM encryption and key wrapping.
PK-806	Extended console command ConfigCmds and its equivalent payShield Manager screen to allow all host and all console commands (except ConfigCmds) to be enabled/disabled.
PK-819	Modified security options for Secure Host Comms to only support TLS v1.2.
PK-823 PK-2756	Modified all existing host commands that allow RSA private keys in key block format to allow for Mode Of Use = 'N'.
PK-849	Extended existing host commands to allow the use of AES TPKs.
PK-856	Extended host command IY to support the inclusion of PINs as part of the Key Generation process.
PK-859 PK-2622	Modified host command K8 to allow a ZAK to have Key Usages M1, M2 and M3.
PK-756 PK-1242	Modified host commands A0 and A8, to allow the export of a DUKPT initial key (IKEY) under a Terminal Master Key (TMK).
PK-801	Extended host command KU and PM to support JCB acquiring functionality.
PK-2916	Extended host command EM, to allow the translated key's Exportability field to be specified when translating from Variant LMK to Key Block LMK.

Bugs and Errors Corrected

Ref.	Description
PK-1626	Fixed an issue that was causing console command CONFIGPB to incorrectly display custom PIN block formats.
PK-1897	Fixed an issue with the key type table, where key types 40D and 50D previously had permission "U__" instead of "UAU".
PK-792 PK-2485	Fixed an issue that caused payShield Manager to become unresponsive when viewing an empty audit log.
PK-761 PK-2540	Fixed an issue that was causing console command VC to incorrectly reject a Test LMK smart card due to invalid format.
PK-2708 PK-818	Fixed an issue in host command EI when using a Key Block LMK. When called with Key Type Indicator = 4, this command now returns a Key Block with Key Usage = '06', and Mode of Use = 'D'.
PK-405	Remove CBC ciphersuite support from the TLS, as CBC ciphers are prone to vulnerabilities in TLS. Also restricted connections on the management port (for payShield Manager) to TLS v1.2 only.
PK-464	Added additional security checks to ensure that component cards #1 and #2 are always used when installing an LMK.

Ref.	Description
PK-514	Fixed an issue so that invalid (unprintable) command codes do not appear in the audit log when logging commands; instead, the hex value of the command code will appear in a new audit message.
PK-738	Fixed a usability issue in payShield Manager, whereby one system running payShield Manager could be impacted by another system attempting to connect to the HSM using payShield Manager.
PK-752	Fixed an issue with host command IU, which was permitting the export of keys marked as non-portable.
PK-755 PK-824 PK-1741 PK-2634	Fixed an issue with host commands M6, M8 and MY, to allow single, double and triple-length DES keys to be used to calculate/verify MACs using MAC Algorithm 1 and 3, using Variant LMKs and Key Block LMKs.
PK-808	Fixed an issue with host command EE which was incorrectly requiring the PIN length to be equal to 'Check Length'.
PK-2109	Fixed an issue which caused an error ('Failed to get host config') to appear in the error log when upgrading from v2.x to v3.x.
PK-2167	Fixed an issue with Secure Host Comms, to allow TLS session reuse.
PK-2202	Updated documentation for host commands M6, M8 and MY, to clarify use of key blocks with Key Usage = 'M5' and 'M6'.
PK-2323	Fixed an issue with host command PM, which was incorrectly imposing a limit for the TWU parameter.
PK-2367 PK-2770 PK-2901	Fixed an issue with host commands EO, EQ and EU, which were rejecting key blocks with Mode Of Use = 'V'.
PK-2658	Updated documentation for host command K8, to clarify usage when using a Key Block LMK.
PK-2709	Fixed an issue with Secure Host Comms, which caused performance to degrade while sessions are established.
PK-518 PK-2762	Fixed an issue with host command QY, which was failing when used with a Key Block LMK.
PK-2796	Updated documentation for host command IE, which was missing the APDU Message Count field for when Output Mode = 2 or 3.
PK-2839	Fixed an issue with host command NE, which was failing with AES key components.
PK-2809	Fixed an issue with host command GI, which was failing to import AES keys.
PK-2784	Fixed an issue with host command BW, which was failing to translate keys with Key Type Code = 107 to keys with Key Usage = 54.
PK-2808	Fixed an issue with host command Q2, to prevent it being added to the audit log.
PK-2810	Fixed an issue with payShield Manager, which was failing on some browsers to upload the TLS certificate.

Ref.	Description
PK-2878	Fixed an issue with payShield Manger, which now has improved accuracy with its inactivity timer.
PK-2879	Fixed an issue in the documentation for command GK, to clarify that Key Check Values for AES keys are always 6 digits.
PK-2887	Fixed an issue with payShield Manager, which was not applying changes to console settings until the HSM was restarted.
PK-2909	Fixed an issue with host command KE, which was failing to accept a plain ASN.1 DER encoded public key for Mode Flag = '1'.
PK-2912	Fixed an issue with payShield Manager, which now forces the HSM to restart after a successful reset to factory settings.
PK-315 PK-317 PK-335 PK-462 PK-575 PK-581 PK-684 PK-727 PK-735 PK-746 PK-754 PK-763 PK-780 PK-783 PK-787 PK-793 PK-840 PK-853 PK-854 PK-1162 PK-1677 PK-2359 PK-2509 PK-2865 PK-2874 PK-2880	Non-specific code security & stability improvements.

Version 3.2 Development Stream

Note: When Thales ships a payShield 9000 HSM pre-loaded with v3.X software, a certificate will be installed inside the HSM (known as a 'warrant') to enable remote commissioning of the HSM using payShield Manager. However, remote commissioning is not permitted when an LMK is already installed in the HSM. Therefore, prior to shipping, Thales will not pre-install the Test LMK into any HSM which is loaded with v3.X software.

Relationship to v3.1

All fixes and enhancements in the v3.1 stream up to and including 1407-0905 (v3.1d) are included in v3.2a. Changes in later versions in the v3.1 stream are not included in the v3.2 stream unless these Release Notes explicitly say that they have been included.

1407-0908 / 1407-1908 (v3.2c) - Released September 2017

PCI HSM Compliant?

- ***This software has been certified for PCI HSM compliance.*** PCI HSM compliance of the payShield 9000 is subject to appropriate user settings having compliant values – see manuals.
- Software number 1407-0908 applies if some security settings are not PCI HSM compliant. Software number 1407-1908 applies if all security settings are PCI HSM compliant: only this software number appears on the PCI certificate. (See manuals)

HSM Manager Compatibility

This version of HSM software is not compatible with HSM Manager. All management activities can be performed using payShield Manager, which is accessed using a regular web browser.

Manuals

- Issue 34 of the payShield 9000 manuals should be used with this release.

Bugs and Errors Corrected

Ref.	Description
PK-2776	Fixed issue in payShield Manager relating to TESA 2017-013.

1407-0907 (v3.2b) - Released August 2017

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is not compatible HSM Manager. All management activities can be performed using payShield Manager, which is accessed using a regular web browser.

Manals

- Issue 34 of the payShield 9000 manuals should be used with this release.

Bugs and Errors Corrected

Ref.	Description
ST-6561	Fixed an internal processing issue which caused the HSM's host Ethernet ports to hang under certain circumstances.
ST-6505	Fixed issue with host command LI which was incorrectly returning error code 16.
ST-6526	Fixed issue with host command PM which was incorrectly returning error code 15 when using Scheme ID = 2 (American Express).
ST-6451	Fixed issue with host command NE which failed (error code A7) when printing an AES-128 key component.
ST-6539	Fixed issue with host command NY to allow use of MK-CVC3 with key usage '32'.
ST-6434	Fixed issue with console command CONFIGPB which was badly formatting custom PIN block formats.
ST-6574	Fixed an internal processing issue which could potentially cause memory overrun issues.

1407-0906 (v3.2a) - Released June 2017

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is not compatible with HSM Manager. All management activities can be performed using payShield Manager, which is accessed using a regular web browser.

Manuals

- Issue 34 of the payShield 9000 manuals should be used with this release.

New Functions

Ref.	Description
ST-6219	Enhanced payShield Manager to support TLS certificate installation.
CIL-560 CIL-635	Added new host command B8 to support export of keys in TR-34 format.
CIL-339	Added new host command IK to perform EMV Sign Data operation.
CIL-340	Added new host command IM to perform EMV Recover Data operation.
ST-5149	Added new host command AQ to support translation from RSA-encrypted PIN to ZPK/TPK encrypted PIN.
CIL-345 CIL-500 CIL-577 CIL-661 PK-6461	Added new host commands L6 & L8 to support import/export of RSA private keys. Added new security setting to control the import/export of RSA private keys.
ST-5947	Removed requirement for AES license (HSM9-LIC007) for generating/installing an AES Key Block LMK. Note: An AES license is still required in order to use AES working keys.
ST-5681	Allowed key scheme 'X' to be used for LMK encrypted keys.
ST-6311	Enhanced host command PM to support Oberthur & Visa time-based dCVV functionality.
ST-6575	Enhanced host commands KI & KW to support VISA QR code functionality.
ST-6576	Enhanced host commands KI, PM, KW & CY to include updates for Discover's card applications.
HCE-155	Enhanced host command GK to support export of AES keys under RSA public key.
HCE-349	Enhanced host commands GI & GK to allow DES/AES keys to be imported/exported using block type 4 (previously restricted to HMAC keys).
CIL-253 CIL-341 CIL-342 CIL-343 CIL-344	Enhanced host command KK, KG, KE, KO to support Union Pay, JCB & Discover certificates.
HCE-333	Enhanced host command IU to allow data encryption key to be loaded once and reused for multiple data items.
HCE-191	Enhanced host command IY to allow 24 and 32 byte session keys with block type 3.

Ref.	Description
HCE-331	Enhanced host commands CC, JE & JG to support PIN Block format 48 (ISO 9564-1 PIN Block format 4 – for use with AES keys).
HCE-366	Enhanced host command PM (Scheme 1, Version 4) to allow key usage E0 for MK-DCVV.
HCE-107	Enhanced host command IY to add support for interfacing to MDES.
CIL-254	Enhanced host command KO to support Thales Key Blocks.
CIL-348	Enhanced host command KO to output AES keys under the KEK.
CIL-253	Enhanced host command KK to support Thales Key Blocks.
CIL-634	Modified host command KO when using Thales Key Blocks and Mode Flag 1, the Card Public Key must now be supplied DER encoded (unsigned) in ASN.1 format.
CIL-633	Modified host command NY to support MK-CVC with key usage E6 or E0.
CIL-595	Modified host command KO when using AES KEK and Pad Mode 1, allowable pad lengths are now 4, 8, 12 and 16 bytes.
CIL-255	Enhanced host command K8 to support Thales Key Blocks.
ST-6241	Enhanced host command A0 to allow a derived IPEK to be exported in TR-31 format under a TMK (key block).
ST-6391	Enhanced host command A0 to support derivation of IPEK from BDK3 and BDK4.
ST-5726	Modified host command EI so that authorized state is no longer required when generating RSA keys with key type 3 (ICC key pairs).
ST-6381	Modified host command A0 to allow generation of MK-AC with a key usage of 'A0'.
ST-6148	Added new security setting to allow LMK ID in header of Thales Key Block to be ignored.
ST-5624	Modified the behaviour of the security setting "Enable Weak PIN Checking" so that it controls the use of the global and local weak PIN tables.
ST-5875	Clarified the security setting "Enforce host port override for LMK use" by renaming it to "Ensure LMK Identifier in command corresponds with host port".
ST-6577	Upgraded OpenSSL to 1.0.2j.

Bugs and Errors Corrected

Ref.	Description
ST-6303	Fixed host command GI to support 16-byte IV when importing AES keys.
ST-6250	Fixed Virtual Console in payShield Manager to allow execution of custom console commands.
HCE-359	Modified host command IU to change Session ID from binary to ASCII hex.

Ref.	Description
HCE-362	Fixed host command IY which was failing to output multiple SUK blocks.
ST-6324	Fixed host command A6 to remove restrictions on key usage when importing from key block (under ZMK) to key block (under LMK).
ST-6392	Fixed issue with host command HY and console command KK, which was failing when used with Thales Key Blocks.
ST-6394 ST-6578 ST-6579	Fixed issue in multi-part MACing commands, re: TESA-2017-005. Also limited the use of multi-part MACing options to use minimum of 3 blocks per part.
ST-6402	Fixed issue with EBCDIC and PINs encrypted under an AES LMK.
ST-6165	Fixed issue in software upgrade process, which was creating a file unnecessarily.
ST-6359	Fixed issue with authorized activities, to allow component.{key}.console to operate with all valid key types/usages.
ST-6409	Fixed issue which prevented import/export of BDK2/3/4 in TR-31 format.
ST-6340	Fixed issue which prevented authorizing export of key usages 41, 42 or 43.
ST-6419	Fixed issue with host command RY, Mode 4, Flag 3, which was not returning
ST-6437 PK-692	Fixed issue with host command EI, which now returns error code 48 when the LMK is determined to be too weak to adequately protect the RSA private key being generated.
ST-6463	Fixed issue with host command KI, which was failing when the serial number ended with the digits '3B'.
PK-701	Fixed issue with Ethernet host connection management which caused the HSM to become unresponsive – requiring a power cycle to restore normal operation.
ST-6415	Fixed issue which caused internal netstat operation to fail, resulting in creation of a new error log entry.
ST-6473	Fixed issue in payShield Manager smart card bridge which caused the Reiner (Secoder) smart card reader to display error messages.
ST-6461	Fixed issue with host command EI, which was failing when specifying Key Type 3 using an AES LMK.
ST-6475	Fixed issue with host command BW, which was failing to translate AES working keys.

Ref.	Description
PK-303 PK-319 PK-458 PK-461 PK-463 PK-595 PK-601 PK-660 PK-663 PK-677 PK-678 PK-700 PK-714 PK-721	Non-specific code stability improvements.

Version 3.1 Development Stream

Note: When Thales ships a payShield 9000 HSM pre-loaded with v3.X software, a certificate will be installed inside the HSM (known as a 'warrant') to enable remote commissioning of the HSM using payShield Manager. However, remote commissioning is not permitted when an LMK is already installed in the HSM. Therefore, prior to shipping, Thales will not pre-install the Test LMK into any HSM which is loaded with v3.X software.

Relationship to v3.0

All fixes and enhancements in the v3.0 stream up to and including 1407-0901 (v3.0b) are included in v3.1a. Changes in later versions in the v3.0 stream are not included in the v3.1 stream unless these Release Notes explicitly say that they have been included.

1407-0905 / 1407-1905 (v3.1d) - Released March 2017

PCI HSM Compliant?

- ***This software has been certified for PCI HSM compliance.*** PCI HSM compliance of the payShield 9000 is subject to appropriate user settings having compliant values – see manuals.

- Software number 1407-0905 applies if some security settings are not PCI HSM compliant. Software number 1407-1905 applies if all security settings are PCI HSM compliant: only this software number appears on the PCI certificate. (See manuals)

HSM Manager Compatibility

This version of HSM software is not compatible with HSM Manager. All management activities can be performed using payShield Manager, which is accessed using a regular web browser.

Manuals

- Issue 33 of the payShield 9000 manuals should be used with this release.

Bugs and Errors Corrected

Ref.	Description
ST-6394	Multi-block MAC operations now encrypt intermediate IVs

1407-0904 (v3.1c) - Released January 2017

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is not compatible with HSM Manager. All management activities can be performed using payShield Manager, which is accessed using a regular web browser.

Manuals

- Issue 32 of the payShield 9000 manuals should be used with this release.

New Functions

Ref.	Description of Enhancement
PK-58 PK-407 PK-408 PK-275	Enhanced browser support: • Chrome on Windows, Linux & MAC • Firefox on Windows & Linux • Internet Explorer on Windows

Bugs and Errors Corrected

Ref.	Description of Error
ST-6271	Resolved issues with User Storage, using variable size & EBCDIC.
ST-6358	Fixed host command A0 which was failing in PCI mode when generating/exporting a TPK.
ST-6344	Fixed host command QK which could cause issues on FICON units.
ST-6350	Fixed console command KK & host command HY to allow import of ZMK, DEK and ZEK.
PK-420	Fixed issue in payShield Manager where the QuickLinks menu was occasionally failing.
PK-355	Fixed issue in payShield Manager where authorized activities marked as persistent still retained a time value.
PK-443	Fixed issue in payShield Manager which prevented authorization of newly installed LMK.
PK-480	Fixed issue in payShield Manager on Internet Explorer (Windows), where smartcard readers with Secure PIN Entry (SPE) were not being detected.
PK-456	Improved online help in payShield Manager (license summary).
PK-494	Fixed issue in payShield Manager which was incorrectly clearing the ACL settings when invalid ACL settings were applied.
PK-490	Improved error handling in payShield Manager on Firefox (Linux) when the browser extension and bridge were not installed.
PK-532	Improved error handling in payShield Manager when entering an invalid IP/mask ACL.

1407-0903 (v3.1b) - Released December 2016

(Limited release only)

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is not compatible with HSM Manager. All management activities can be performed using payShield Manager, which is accessed using a regular web browser.

Manuals

- Issue 31 of the payShield 9000 manuals should be used with this release.

New Functions

Ref.	Description of Enhancement
PK-460 PK-171	Enhanced browser support: • Chrome on MAC

Bugs and Errors Corrected

Ref.	Description of Error
PK-392	Fixed issue when authorizing the LMK ID 19 when 20 LMKs are installed.
PK-354	Fixed issue where some authorized activities appeared to remain after clearing all authorizations. (This was a UI error; no activities remained authorized.)
PK-438	Fixed issue which could cause the payShield Manager Virtual Console to shut down unexpectedly, when the HSM operated in PCI mode.

1407-0902 / 1407-1902 (v3.1a) - Released September 2016

PCI HSM Compliant?

- ***This software has been certified for PCI HSM compliance.*** PCI HSM compliance of the payShield 9000 is subject to appropriate user settings having compliant values – see manuals.

- Software number 1407-0902 applies if some security settings are not PCI HSM compliant. Software number 1407-1902 applies if all security settings are PCI HSM compliant: only this software number appears on the PCI certificate. (See manuals)

HSM Manager Compatibility

This version of HSM software is not compatible with HSM Manager. All management activities can be performed using payShield Manager, which is accessed using a regular web browser.

Manuals

- Issue 31 of the payShield 9000 manuals should be used with this release.

New Functions

Ref.	Description of Enhancement
ST-6270	Add support for new KMD V1.1 functionality at the console & host
ST-6214	Add support for DUKPT-to-DUKPT translations using BDK4
ST-6213	Add support for Ingenico BPS Format Preserving Encryption algorithm
ST-6141	Enhancements to SNMP MIB & support for SNMP Traps
ST-5875	Optionally prevent LMK Id specified in a host command overriding the LMK Id implied by the TCP port number.
ST-5795	Add support for the AES PIN Block (ISO 9564-1 format 4) – only for use with AES PIN encryption keys.
ST-5791	Optionally clear front panel Error LED after viewing error log.
ST-5168	Improve the process of migrating from an 'old' LMK to a 'new' LMK.
ST-3246	Extend RSA commands by supporting up to 4096-bit keys.

Bugs and Errors Corrected

Ref.	Description of Error
ST-6279	Authorization requirements for HCE key types fixed.
ST-6272	SNMP process now returns correct data & time.
ST-6263	Fixed issue which was causing transparent async comms to fail.
ST-6257	Fixed GI host command which was occasionally incorrectly returning error 15.

Ref.	Description of Error
ST-6232/ ST-6187	Resolved potential memory leak during TLS/SSL negotiation.
ST-6224/ ST-6044	Fixed issue where commands disabled by CONFIGCMDS were re-enabled after a license update.
ST-6221	Console 'Reset' command now resets host Ethernet i/f to use DHCP
ST-6206	Resolved issue that was causing an error when migrating from v2.x to v3.x software.
ST-6195	Triple-Length Variant LMK no longer requires multi LMK license
ST-6186	Fixed issue causing loss of chain of trust after migration from Remote HSM Manager to payShield Manager.
ST-6180	Fixed NI host command which was not populating Ethernet statistics
ST-6171	Corrections to Name & Description fields in payShield Manager
ST-6164	Resolved potential memory corruption in software update process
ST-6160	Resolved potential memory leak in the CLEARAUDIT command.
ST-6153	Fixed RESET console command so that it doesn’t reboot unless requested.
ST-6151	Fixed RESET console command so that it doesn’t cause "Unable to create file" to appear in the error log.
ST-6146	HSM incorrectly derives encryption/authentication keys when importing and exporting using a 128-bit or 192-bit AES ZMK.
ST-6088	Fixed BY host command which was failing to import an AES ZMK
ST-6071	Fixed GETCMDS console command which was incorrectly calculating the hash over enabled and licensed commands (-h switch).
ST-6025	Resolved problem preventing Authorizing Officer smartcards working (relating to a 3DES Keyblock LMK).
ST-6282/ ST-6294/ ST-6300/ ST-6302	Non-specific code stability improvements.

Version 3.0 Development Stream

Note: When Thales ships a payShield 9000 HSM pre-loaded with v3.X software, a certificate will be installed inside the HSM (known as a 'warrant') to enable remote commissioning of the HSM using payShield Manager. However, remote commissioning is not permitted when an LMK is already installed in the HSM. Therefore, prior to shipping, Thales will not pre-install the Test LMK into any HSM which is loaded with v3.X software.

Relationship to v2.4

All fixes and enhancements in the v2.4 stream up to and including 1346-0919 (v2.4a) are included in v3.0b. Changes in later versions in the v2.4 stream are not included in the v3.0 stream unless these Release Notes explicitly say that they have been included.

1407-0901 (v3.0b) - Released December 2015

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is not compatible with HSM Manager, but introduces support for payShield Manager, which is accessed using a regular web browser.

Manials

- Issue 30 of the payShield 9000 manuals should be used with this release.

New functions

Ref.	Description of Enhancement
	Introduce support for payShield Manager.

Version 2.4 Development Stream

Relationship to v2.3

All fixes and enhancements in the v2.3 stream up to and including 1346-0917 (v2.3f) are included in v2.4a. Changes in later versions in the v2.3 stream are not included in the v2.4 stream unless these Release Notes explicitly say that they have been included.

1346-0922 (v2.4c) - Released January 2018

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 5.1.7

Manuals

- Issue 20 of the payShield 9000 manuals should be used with this release.

Bugs and Errors Corrected

Ref.	Description
PK-726 PK-2856 PK-2857 PK-2861 PK-2997 PK-3004 PK-3012 PK-3013 PK-3014	Non-specific code security & stability improvements.

1346-0921 (v2.4b) - Released April 2017

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 5.1.7

Manuals

- Issue 20 of the payShield 9000 manuals should be used with this release.

Bugs and Errors Corrected

Ref.	Description
PK-337	Upgraded OpenSSL to 1.0.2j
ST-6373	Removed ZKA Master Key from LMK pair 06-07/0 and 14-15/0
ST-6394	Multi-block MAC operations now encrypt intermediate IVs
ST-6300 ST-6307 ST-6344	Non-specific code stability improvements.

1346-0919 (v2.4a) – Released May 2016.

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 5.1.7

Manuals

- Issue 19 of the payShield 9000 manuals should be used with this release.

New functions

Ref.	Description of Enhancement
CR 13361	Add functionality introduced via early-release software 1401-09xx: • Host Card Emulation support in host commands KW, KI, PM, IO, IQ, IU, IW, IY, GI. • PAN Tokenization support in host commands EC, CM, GQ, CC, CI, G0. • X9 TR-31:2010 support in host commands A0, A6, A8. • New/modified settings in console commands CS, QS, RS, SS.
CR 13361	HSM now issues gratuitous ARP at start up.

Ref.	Description of Enhancement
CR 13450	Upgraded OpenSSL to 1.01q
CR 13261	Allow export of ZKA Master Key type (requires Authorized state).
CR 12726	Add functionality to support triple-length Variant LMKs.

Bugs and Errors Corrected

Ref.	Description of Error
CR 13419	GETCMDS console command has memory allocation problem.
CR 13406	M0 host command incorrectly returning error 06.
CR 13371	HSM Manager connection failing intermittently.
CR 13359	HSM Manager connection failing after reading full audit log.
CR 13330	HSM failing to release TCP sessions on host i/f.
CR 13300	JG host command – incorrectly returning error code 14 instead of 15.
CR 13282	NO & commands supporting Weak PIN functionality were occasionally performing slowly, as data was written to Flash memory.
CR 13239	Host Ethernet interface not properly handling 10/100MBps connections to managed switches
CR 13215	XC console command doesn't appear in commands auth category until after the HSM is restarted.
CR 13211	ROUTE console command may cause lockup.
CR 13163	KI host command fails when using method C and derivation data contains 0x19.
CR 13158	A4 host command isn't permitted although authorized.
CR 13120	Loading LMK into HSM now enforces unique components.
CR 12953	IE host command incorrectly outputs DGI value and length fields when using non-STORE DATA APDUs.
ST-6242	In the event that the HSM becomes disconnected from the Remote HSM Manager application, the HSM now always returns to Online state.
ST-6195	Triple Length Variant LMK can't be loaded without a multi-LMK license.
ST-6083	Audit log disconnects from HSM Remote Manager and has a performance issue.
ST-6180	NI host command response doesn't populate Ethernet stats.
HSMMAN-2643	IU host command mode 1 allows a Message Data Item Type of other than '5'.
HSMMAN-2656	Commands IO, IQ, IU, IW, IY return incorrect error code when license is not present.

Version 2.3 Development Stream

Relationship to v2.2

All fixes and enhancements in the v2.2 stream up to and including 1346-0910 (v2.2b) are included in v2.3a. Changes in later versions in the v2.2 stream are not included in the v2.3 stream unless these Release Notes explicitly say that they have been included.

1346-0917 / 1346-1917 (v2.3f) – Released June 2015

PCI HSM Compliant?

- ***This software has been certified for PCI HSM compliance.*** PCI HSM compliance of the payShield 9000 is subject to appropriate user settings having compliant values – see manuals.
  - Software number 1346-0917 applies if some security settings are not PCI HSM compliant. Software number 1346-1917 applies if all security settings are PCI HSM compliant: only this software number appears on the PCI certificate. (See manuals)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 5.1.7

Manuals

- Issue 18 of the payShield 9000 manuals should be used with this release.

Security Enhancements and Fixes

Ref.	Description of Error
CR 13277	Addresses vulnerability outlined in Security Advisory TESA-2015-004.

Bugs and Errors Corrected

Ref.	Description of Error
CR 13284	Improved TCP & UDP performance.
CR 13271	Modified SG console command in its use of the hardware RNG.

1346-0916 (v2.3e) – Released March 2015

(Special request only)

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 5.1.7

Manuals

- Issue 18 of the payShield 9000 manuals should be used with this release.

Bugs and Errors Corrected

Ref.	Description of Error
CR 13240	Upgrading from pre-v2.2a to any version from 2.2a-2.3d can result in the loss of the private key for remote access.
CR 13118	NO host command can cause timeout errors
CR 13113	HSM may fail to resend a command when requested
CR 12872	Command processing latency is sometimes higher than expected

1346-0915 (v2.3d) – Released January 2015

(Special request only)

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 5.1.7

Manuals

- Issue 17 of the payShield 9000 manuals should be used with this release.

Bugs and Errors Corrected

Ref.	Description of Error
CR 12872	Performance of command processing improved to minimize latency.
CR 13113	Fix to ensure lost response messages are always resent.

1346-0914 / 1346-1914 (v2.3c) – Released November 2014

(Special request only)

Special Notes

- ***It is recommended that existing users of v2.3a and v2.3b upgrade to v2.3c.***
- Remote HSM Manager does not currently support the use of AES LMKs. Local HSM Manager or the Console should be used where AES LMKs are to be deployed.
- An intermittent error has been reported where the console may become unresponsive if connected to the left-hand USB port on the front panel of the payShield 9000. This has been observed to happen after events such as a software load or a restart. If this error is encountered, it can be circumvented by connecting the console to a different USB port or re-starting the payShield 9000.

PCI HSM Compliant?

- ***This software has been certified for PCI HSM compliance.*** PCI HSM compliance of the payShield 9000 is subject to appropriate user settings having compliant values – see manuals.
- Software number 1346-0914 applies if some security settings are not PCI HSM compliant. Software number 1346-1914 applies if all security settings are PCI HSM compliant: only this software number appears on the PCI certificate. (See manuals)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 5.1.7

Manuals

- Issue 17 of the payShield 9000 manuals should be used with this release.

Security Enhancements and Fixes

Ref.	Description
CR 13099	Addresses POODLE vulnerability in OpenSSL libraries by implementing OpenSSL v1.0.1j
CR 13098	Addresses vulnerability outlined in Security Advisory TESA-2014-001.

Bugs and Errors Corrected

Ref.	Description of Error
CR 13037	A0 Host Command returns response code when generating and exporting an IKEY/IPEK after 100+ iterations when using Keyblock LMKs
CR 13000	JK Host Command (Get Instantaneous Health Check Status) returns incorrect value for "Ethernet Host link 1 state" in certain cases.

1346-0913 (v2.3b) – Released August 2014

(Special request only)

Special Notes

- ***It is recommended that existing users of v2.3a upgrade to v2.3b.***
- Remote HSM Manager does not currently support the use of AES LMKs. Local HSM Manager or the Console should be used where AES LMKs are to be deployed.
- An intermittent error has been reported where the console may become unresponsive if connected to the left-hand USB port on the front panel of the payShield 9000. This has been observed to happen after events such as a software load or a restart. If this error is encountered, it can be circumvented by connecting the console to a different USB port or re-starting the payShield 9000.

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 5.1.7

Manuals

- Issue 16 of the payShield 9000 manuals should be used with this release.

New functions

Ref.	Description of Enhancement
CR 11558	Secure Host Communications using TLS or SSL v3 is now available on general release. This feature requires the use of Optional License HSM9-LIC036. (*Note: USB memory sticks are used to transfer material such as certificates in and out of the payShield 9000. The Operating System used in the payShield 9000 supports most types of USB memory stick, but may not have the drivers for some of the newer types. If difficulties are experienced when trying to read from or write to a USB device, an alternative memory stick should be used.*)
CR 12686	QY Host Command to generate a dCVV
CR 12476	payShield 9000 IP address can now be obtained from a DHCP server or via a DNS name server.
CR 12194	Access Control Lists can now be applied to Ethernet host ports.
CR 11471	N0 Host Command introduced to generate and return a Random Number.
CR 10261	Support for native USB printers.

Enhancements to Existing Functions

Ref.	Description of Enhancement
CR 12890	OpenSSL upgraded to version 1.0.1h.
CR 12800 CR 12738	Upgrade OpenSSL Toolkit used for Secure Host Communications to v1.0.1g: this prevents the Heartbleed vulnerability.
CR 12719	Card Issuing Enhancements – support for Global Platform SCP02 (i=055 mode)
CR 12703	G0 Host Command extended to support any valid PIN Block format.
CR 12690	A0 Host Command extended to allow export of an IPEK under a TMK.
CR 12662	BU Host Command extended to generate a Key Check Value on an HMAC key.
CR 12627	Users can now specify which Ethernet port is to be used for SNMP
CR 12622	GETCMDS, CONFIGCMDS, and AUDITOPTIONS Console commands can now handle more than 120 commands.
CR 12596	When using the SI Console command, user is informed if no certificates are found on the USB memory device.
CR 12575	Users can now select whether to limit the authorization period for console commands. This limitation must be selected where PCI HSM compliance is required.
CR 12548	Users can now audit whenever an attempt to establish a Secure Host Sessions fails because the certificate has expired. The audit log entry identifies the certificate.
CR 12543	A0 Host command extended to provide GBIC/ZKA key derivation.
CR 12508	Internet network numbers are now displayed in standard CIDR format.
CR 12504	Major upgrade to user Storage capability. New "Variable" length setting allows longer data items including RSA keys and Keyblock LMK-encrypted keys to be held in the user Storage area inside the payShield 9000.
CR 12475	Software no longer reports whether it is PCI HSM certified or not. Instead it refers users to online certificate at PCI web site, in line with PCI wishes. Software just reports on status of security settings that affect PCI HSM compliance.
CR 12429	BU host command does not generate KCVs for AES keyblocks.
CR 12346	GQ, GS and GU Host commands enhanced so that they support Mode=2 (Verify PIN only using a unidirectional PIN key)
CR 12306	The use of multiple components can be enforced when forming keys or loading LMKs. This setting must be used for PCI HSM compliance.
CR 12235	A0 Host command now allows a TMK to be exported under a TMK.
CR 12217	Card Issuer Password can now be restored to its original value.
CR 12210 CR 12145	Management and Default LMKs can now be reassigned without having to delete LMKs.

Ref.	Description of Enhancement
CR 12144	When deleting the LMK that is the Management or Default LMK (when there is another LMK present), the user is prompted to re-assign Management and/or Default LMK first.
CR 12001	Auditing of Error responses now ignores response 43
CR 11953	Settings can now be saved in Online and Offline states
CR 11862	PIN translation *to* a BDK.
CR 10606	Improvements of display of utilisation data when using the UTILSTATS Console command.

Security Enhancements and Fixes

Ref.	Description
CR 12992	Enhancement to certain console commands following updated best practise review.
CR 12884	-P option removed from NETSTAT console command to (a) ensure compliance with security advisory related to the NetBSD implementation, and (b) to remove option deemed unnecessary for HSM operations. *[NOTE: the –p (lower case) option is still available.*]

Bugs and Errors Corrected

Ref.	Description of Error
CR 13002	Error code 28 returned when importing a PVK (key type 002) when security settings are PCI HSM-compliant.
CR 12926	Restore Settings, (RS console command) appears to restore PIN Block Formats correctly but after power cycle the settings are back to what they were before RS was run.
CR 12922	GK Console command prompt for TDES Keyblock LMKs corrected: "Enter value C:" changed to "Enter secret value C:"
CR 12917	After using facility to Return To Factory Settings, a manual restart may be required in addition to the automatic restart.
CR 12905	When authorizing activities using the A console command, if authorizations are made using both the menu and command line methods, the output from the A command may show multiple entries for time remaining for authorization with conflicting values.
CR 12866	Error code 17 incorrectly returned when host command A0 used to generate a TPK and export under a TMK when using a keyblock LMK.
CR 12816	Self test run time value not retrieved correctly from saved settings via RS command.
CR 12801	Changes made in CH and CM console commands now take effect on completion of the command.
CR 12755	Sometimes unable to load software using FTP

Ref.	Description of Error
CR 12752	G0 host command may fail with error response A3 instead of 23.
CR 12727	When importing a GISKE key using A8 host command, encrypted key is all zeroes.
CR 12691	If Security Setting "Enable weak PIN checking" is set to NO, weak PIN checking is not performed if a local Weak PIN table is included in a command.
CR 12671	ROUTE command not setting up persistent routes correctly
CR 12611 CR 12557 CR 12099 CR 11647 CR 11527	Corrections to display of installed optional licenses.
CR 12603	Message Trailers not being returned for J6 and JI Host commands
CR 12594	A0 Host command is not correctly exporting, for example, a ZPK under a ZMK with the AS2805 H key scheme applied.
CR 12565	BA Host command now checks that cleartext PINs are padded with F to the encrypted PIN length.
CR 12559	RG Console command (Generate RMK) command on an incorrectly formatted smartcard causes error then the smartcard cannot be formatted.
CR 12558	Under some circumstances there may be an inability to print and system logs may outgrow the file system.
CR 12514	Cannot read an AES decimalization table from user storage.
CR 12506	Console can crash if user input is too long to A6 and MI Console commands.
CR 12482	PE host command may fail and cause the HSM to become unresponsive if binary data is sent to the printer.
CR 12246	Invalid MAC calculated with intermediate to final block when verified with C4 command.
CR 12190	Remote HSM Manager lost connection to HSM and was not able to connect again until the HSM was rebooted.
CR 11183	I8 Host Command / Sub Command Code 04 (Load Cipher Data) fixed for Cipher Data Type 2 (Triple DES key encrypted under KEK)
CR 11510	BW host command returns error 33 when there is no old LMK loaded.
CR 10914	When auditing forming of keys from components while using HSM Manager, multiple audit log entries are made.
CR 10727	A8 Host command does not import a GISKE key correctly: it populates the encrypted key field with all 0's
CR 10607	Utilisation Stats are not being reset when new firmware loaded using USB stick.
CR 10398	Process for switching between Console management and HSM Manager management enhanced to prevent attempted Denial of Service attacks.

Ref.	Description of Error
CR 10311	Audit Log may be corrupted if user changes time or audit counter.
CR 10232	Save settings may not save host comms interface type correctly
CR 10027	If a port number is used in a test to specify an incorrect LMK, sometimes error code A1 returned instead of error code 13.
CR 9171	Single-character wildcards (e.g. "+CR?") not working for enabling commands in CONFIGCMDS Console command.

1346-0912 (v2.3a) – Released July 2014

(Withdrawn)

This software has been withdrawn and should not be used. It has been replaced by v2.3c.

Enhancements and error corrections that were made in v2.3a have been included in the lists provided above for v2.3b.

Version 2.2 Development Stream

Relationship to v2.0

All fixes and enhancements in the v2.0 stream up to and including 1346-0904 (v2.0c) are included in the v2.2 stream. Changes in later versions in the v2.0 stream are not included in the v2.2 stream unless these Release Notes explicitly say that they have been included.

1346-0911 (v2.2b) – Released April 2014

(Special request only)

Special Notes

- ***This release replaces v2.2a and is in response to the Heartbleed bug.***
- ***V2.2a contains software to provide a Secure Host Communications feature, which was to be enabled in the future using a new license. This feature makes use of OpenSSL.***
- ***Although v2.2a is not susceptible to the Heartbleed vulnerability because the license that activates Secure Host Communications was never made available, Thales recommends that users of v2.2a upgrade to v2.3c. This allows a clear statement to be made that the product does not contain the vulnerable version of OpenSSL. The only changes in this release compared with v2.2a are:***
    - ***the dormant OpenSSL component has been upgraded to a version not vulnerable to the Heartbleed bug, and***
    - ***the ability to activate the Secure Host Communications license has been removed.***

  payShield 9000 versions prior to v2.2a did not include OpenSSL, and therefore users of these versions do not need to take any action.

  Users who want to move from v2.1 or earlier to v2.2 software should move to v2.2b or later.
- See Special Notes for v2.2a.

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 5.1.4 (for v2.2a of the payShield 9000)

Manuals

- Issue 14.6 of the payShield 9000 manuals should be used with this release.

Enhancements to Existing Functions

Ref.	Description of Enhancement
CR 12806	OpenSSL 1.0.1f upgraded to OpenSSL 1.0.1g. Optional License to activate Secure Host Communications is not operational in this release.

1346-0910 (v2.2a) – Released July 2013

(Withdrawn)

Special Notes

- Remote HSM Manager does not currently support the use of AES LMKs. Local HSM Manager or the Console should be used where AES LMKs are to be deployed.
- An intermittent error has been reported where the console may become unresponsive if connected to the left-hand USB port on the front panel of the payShield 9000. This has been observed to happen after events such as a software load or a restart. If this error is encountered, it can be circumvented by connecting the console to a different USB port or re-starting the payShield 9000.

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 5.0.19

Manuals

- Issue 14 of the payShield 9000 manuals should be used with this release.

New functions

Ref.	Description of Enhancement
CR 11861	RSA Booster license (HSM9-LIC033) to increase performance of main RSA functions.
CR 11781	New host command (QK) introduced to enable the account number to be changed (without changing the PIN) in an LMK-encrypted PIN. This allows card issuers to issue replacement cards while retaining the old PIN.
CR 11558	Introduction of Secure Host Communications, using TLS or SSL. *Notes:* *1. This capability is undergoing customer trials, and the enabling licence will be made available when these trials have been completed.* *2. The default set of ciphers on the IBM z/OS platform do not support connections to the payShield 9000. Users affected by this should contact their IBM representative to obtain an updated set of ciphers.*

Ref.	Description of Enhancement
CR 11415	MACing of Issuer Discretionary Data.
CR 11285	Support for Discover ZIP contactless transactions.

Enhancements to Existing Functions

Ref.	Description of Enhancement
CR 12195	Reporting of Authorisation State identifies whether commands are Host, Console, or All
CR 12064	A5 console command now allows current fraud detection settings to be viewed while the payShield 9000 is in Online and unauthorized state.
CR 12063	HEALTHSTATS console command now allows health statistics settings to be viewed while the payShield 9000 is in Online and unauthorized state.
CR 11968	Users no longer need to specify an SNMP community write string.
CR 11935	HSM Manager user interface improved when asking whether configuration changes should be applied at next restart.
CR 11916	PSU failure (on dual-PSU models) now reported immediately instead of at next restart,
CR 11858	Improvements to way that battery life is reported.
CR 11857	Enhancements to card personalization and MULTOS capabilities.
CR 11741	VC console command now identifies the component type (i.e. Variant, 3DES-Keyblock or AES-Keyblock) on the card.
CR 11676	Audit log is now displayed with most recent entries first. On the console, audit log display can be terminated by using Ctrl-C. This supports the recent increase in Audit Log size to 50,000 records, which will take a long time to display on a serial console.
CR 11365	Console commands show the maximum permissible value of LMK ID.
CR 10937 CR 10793 CR 10758	Error messages enhanced.
CR 10907	Enforced audit log entries for key entry (“KE”) actions now identified as user actions to distinguish them for KE console command entries.
CR 10051	Support for 20 LMK option for Multiple LMK licenses - HSM9-LIC022.
CR 9112	When loading an LMK using the LK console command, if no management or default LMK already exists the user is asked whether they want to allocate the new LMK as management/default LMK.
CR 8817	Authorising activities by command line now notifies which activities will be authorized before requesting cards and PINs.

Bugs and Errors Corrected

Ref.	Description of Error
CR 12435	Incorrect reporting of voltages being out of range.
CR 12431 CR 12430 CR 11774 CR 11135 CR 11103	Corrections made to SNMP MIB.
CR 12404 CR 12403	Some optional licenses not being reported correctly with VR console command.
CR 12399	Use of Reset to Factory settings feature sets Ethernet port speeds to an invalid value.
CR 12385	HSM Manager Health Check data for fans and PSU status inconsistent with Console DT command.
CR 12254	Cannot authorise all required key types for BU host command and CK console command.
CR 12246	Invalid MAC calculated with intermediate to final block when verified with C4 command.
CR 12236	Error Message on VR Console command and no serial number shown after Return to factory Settings
CR 12183	After applying new Ethernet host settings to the payShield, the TCP and/or UDP server stop working.
CR 12166	Presence of LIC030 not being reported in HSM Manager
CR 12165	Console command "SNMP" to view the SNMP settings returns error “No such file or directory”, and not able to add an SNMP community.
CR 12109	HSM Manager Health Check data showing incorrect vales for numbers of tampers and reboots.
CR 12085	GW host command may incorrectly return error code 15.
CR 12040	C4 host command may incorrectly return error code 01.
CR 12032	Problems when configuring printer using HSM Manager
CR 12025	Generate Components function returning “Incompatible Key length” error.
CR 12012	SNMPADD console commands allows entry of zero-length community/user names, which prevents the SNMP agent from running after a reboot.
CR 11985	QH console command may show errors when displaying interface settings.
CR 11980	HC host command returns a corrupted header when the PCI HSM key separation setting is on.
CR 11960	VR command not reporting presence of LIC030
CR 11959	KK host command incorrectly returns error code 07.
CR 11956	Some saved audit settings are not restored when using HSM Manager.
CR 11952	KK host command returns error code 15

Ref.	Description of Error
CR 11548	Software update may result in error message 'Failed reading single item setting'
CR 11487	RI host command has the wrong Mode of Use used in the keyblock response of TPK.
CR 11309	Parity should not be set or checked in IKEY (a.k.a. IPEK) keys.
CR 11112	Async option may not appear when using CH console command.
CR 11013	Error in Fraud Detection Total PIN Attacks counter.
CR 10968	Certain RSA Key pairs sizes can be created using EI host command that fail to work in EW host command.
CR 10829	Activity terminated on incorrect PIN entry instead of allowing a retry.
CR 10807	Cannot establish SNMP v3 connection.
CR 10558	Changing SNMP configuration starts the SNMP service even if it is disabled (and can cause an error to be logged)
CR 10534	SNMPADD console command allows spaces to be included in usernames, but SNMP cannot connect when spaces are used.
CR 10302	If no Old Key is loaded in Key Storage, BS returns error code 13 instead of 00.
CR 10137	If you try to delete a route that isn't there the HSM still asks you if you want to delete the persistent route
CR 9895	FK console command should display KCV of component as entered by custodian and be given the opportunity to re-enter component.
CR 9881	EW host command fails with AF (invalid end date) instead of AE (Invalid start date)
CR 9434	Retrieve Setting command incorrectly deletes the LMKs - LMKs should only be deleted for Alarm and Security settings.
CR 7147	In the NY host cmd, it should be an error if the 5N ATC field is > 65535 or if the Unpredictable Number field is 10N and > 4294967295.

Version 2.1 Development Stream

Relationship to v2.0

All fixes and enhancements in the v2.0 stream up to and including 1346-0904 (v2.0c) are included in v2.1c. Changes in later versions in the v2.0 stream are not included in the v2.1 stream unless these Release Notes explicitly say that they have been included.

1346-0908 (v2.1e) – Released April 2015

(Special request only)

Special Notes

- Remote HSM Manager does not currently support the use of AES LMKs. Local HSM Manager or the Console should be used where AES LMKs are to be deployed.
- An intermittent error has been reported where the console may become unresponsive if connected to the left-hand USB port on the front panel of the payShield 9000. This has been observed to happen after events such as a software load or a restart. If this error is encountered, it can be circumvented by connecting the console to a different USB port or re-starting the payShield 9000.

PCI HSM Compliant?

- This software is not certified to the PCI HSM standard. (Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.)
- Software number 1346-0908 applies if some security settings are not PCI HSM compliant. Software number 1346-1908 applies if all security settings are PCI HSM compliant. (See manuals)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 4.1.7

Manuals

- Issue 13.5 of the payShield 9000 manuals should be used with this release.

Bugs and Errors Corrected

Ref.	Description of Error
CR 13275 CR 12872	Command processing latency is sometimes higher than expected

1346-0907 (v2.1d) – Released January 2015

Special Notes

- Remote HSM Manager does not currently support the use of AES LMKs. Local HSM Manager or the Console should be used where AES LMKs are to be deployed.

- An intermittent error has been reported where the console may become unresponsive if connected to the left-hand USB port on the front panel of the payShield 9000. This has been observed to happen after events such as a software load or a restart. If this error is encountered, it can be circumvented by connecting the console to a different USB port or re-starting the payShield 9000.

PCI HSM Compliant?

- This software is not certified to the PCI HSM standard, but it will be submitted for certification. (Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.)
- Software number 1346-0907 applies if some security settings are not PCI HSM compliant. Software number 1346-1907 applies if all security settings are PCI HSM compliant: only this software number will appear on the PCI certificate if the software is successfully certified. (See manuals)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 4.1.7

Manuals

- Issue 13.5 of the payShield 9000 manuals should be used with this release.

Bugs and Errors Corrected

Ref.	Description of Error
CR 13037	A0 host command fails to export an IPEK after a large number of iterations
CR 13032	Remote Manager disconnects when the Audit log becomes full (50,000 entries).
CR 12691	If Security Setting "Enable weak PIN checking" is set to NO, weak PIN checking is not performed if a local Weak PIN table is included in a command.
CR 12603	Message Trailers not being returned for J6 and JI Host commands
CR 12475	Software no longer reports whether it is PCI HSM certified or not. Instead it refers users to online certificate at PCI web site, in line with PCI wishes. Software just reports on status of security settings that affect PCI HSM compliance.
CR 12420	A0 host command returns Error Code A6 generating KB types K0 and 52
CR 12190	Remote HSM Manager lost connection to HSM and was not able to connect again until the HSM was rebooted.
CR 12085	GW host command returns Error Code 15
CR 12040	C4 host command returning C501 with Good Data
CR 11991	NG host command processing not checking for authorized state and clear PIN security setting. (Note: this affects only v2.0a software.)

Security Enhancements and Fixes

Ref.	Description
CR 13098	Addresses vulnerability outlined in Security Advisory TESA-2014-001.
CR 12992	Enhancement to certain console commands following updated best practise review.
CR 12884	-P option removed from NETSTAT console command to (a) ensure compliance with security advisory related to the NetBSD implementation, and (b) to remove option deemed unnecessary for HSM operations. *[NOTE: the –p (lower case) option is still available.*]
CR 11994	Temperature sensor/alarm is now permanently active.

1346-0905 / 1346-1905 (v2.1c) – Released April 2013

(Special request only)

Special Notes

- Remote HSM Manager does not currently support the use of AES LMKs. Local HSM Manager or the Console should be used where AES LMKs are to be deployed.
- An intermittent error has been reported where the console may become unresponsive if connected to the left-hand USB port on the front panel of the payShield 9000. This has been observed to happen after events such as a software load or a restart. If this error is encountered, it can be circumvented by connecting the console to a different USB port or re-starting the payShield 9000.

PCI HSM Compliant?

- ***This software has been certified for PCI HSM compliance.*** PCI HSM compliance of the payShield 9000 is subject to appropriate user settings having compliant values – see manuals.
- Software number 1346-0905 applies if some security settings are not PCI HSM compliant. Software number 1346-1905 applies if all security settings are PCI HSM compliant: only this software number appears on the PCI certificate. (See manuals)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 4.1.0 & 4.1.4

Manuals

- Issue 13 of the payShield 9000 manuals should be used with this release.

Version 2.0 Development Stream

Relationship to v1.4

All fixes and enhancements in the v1.4 stream up to and including 1317-0917 (v1.4b) are included in v2.0a. Changes in later versions in the v1.4 stream are not included in the v2.0 stream unless these Release Notes explicitly say that they have been included.

1346-0904 (v2.0c) – Released April 2013

(Special request only)

Special Notes

- Remote HSM Manager does not currently support the use of AES LMKs. Local HSM Manager or the Console should be used where AES LMKs are to be deployed.
- An intermittent error has been reported where the console may become unresponsive if connected to the left-hand USB port on the front panel of the payShield 9000. This has been observed to happen after events such as a software load or a restart. If this error is encountered, it can be circumvented by connecting the console to a different USB port or re-starting the payShield 9000.

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 4.0.12, 4.1.0, 4.1.4

Manuals

- Issue 13 of the payShield 9000 manuals should be used with this release.

Bugs and Errors Corrected

Ref.	Description of Error
CR 12165	"No such file or directory" when trying to view or add SNMP Community/User.
CR 12152	Cannot load AES LMK unless a multiple LMK license is installed.
CR 12150 CR 12073	Management port settings not applied correctly unless unit is restarted,
CR 12098	NC host command incorrectly returns Error Code 32 (LIC007 not present)
CR 12083	Upgrading to v2.0 software from some versions of earlier software could require Ethernet port speeds to be set before the ports could be used.

Ref.	Description of Error
CR 12072	Incorrect Microcontroller Version number reported when using HSM Manager.
CR 12043	payShield 9000 may become unresponsive, with Host 1 LED permanently illuminated.
CR 12011	FICON units experiencing a UE when a large number of blocks received without a rewind.
CR 12004	A Console command reports console authorization expires in 720 minutes even when a shorter timeout has been specified (e.g. for 120 minutes)
CR 11981 CR 11979	FG & OE Host commands return error code 15 when they should return 68
CR 11648	A0 Host command may incorrectly return error code 67 (command not licensed).

1346-0902 (v2.0b) – Released February 2013

(Special request only)

Special Notes

- **Upgrading to v2.0b**: an additional step is required when upgrading to v2.0b on a payShield 9000 which has never run software v1.4a or later (or where v1.4a or later has been run in the past but the *Reset to Factory Settings* utility has been used since then). In such cases, after the v2.0b software has been loaded the console commands CH and CM should be used to set the Host and Management Ethernet port speeds (see reference to CR 10788 below): if this step is omitted the Ethernet ports will be inactive.
- Remote HSM Manager does not currently support the use of AES LMKs. Local HSM Manager or the Console should be used where AES LMKs are to be deployed.
- An intermittent error has been reported where the console may become unresponsive if connected to the left-hand USB port on the front panel of the payShield 9000. This has been observed to happen after events such as a software load or a restart. If this error is encountered, it can be circumvented by connecting the console to a different USB port or re-starting the payShield 9000.

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 4.0.12, 4.1.0, 4.1.4

Manuals

- Issue 12 of the payShield 9000 manuals should be used with this release.

Enhancements to Existing Functions

Ref.	Description of Enhancement
CR 11965	CVC3 functionality now supports PINCVC3
CR 11799	It is now possible to use all the commands required by AS2805 (enabled with LIC003) and APACS. Previously, the commands RI, RK, RU, RW, RM, RO, RQ, RS were used in both AS2805 and APACS, and as a result only one "meaning" of the commands was available, depending on the security setting to choose the transaction key scheme. Now, the alternative meaning of the commands can be used by using aliases HI, HK, HU, …
CR 11777	It is now possible to audit commands where an error code is returned in the response. (Information and warning codes are not audited.)
CR 11474	GETCMDS modified to list commands that are (a) licensed, (b) not disabled by CONFIGCMDS, and (c) implemented in the installed software.
CR 10788	Host and Management port speeds and duplexity can now be set manually.
CR 10758	RR console command - error messages enhanced.
CR 9844	Audit log now has an entry when entries are erased.
CR 9374	HSM Manager can now cancel TRACERT
CR 9209	Retrieve settings function now does not ask you whether you want to load settings for a group when there are no saved settings.
CR 9112	If user is entering an LMK and the Default/Management LMKs are empty, user now asked if the new LMK should be the Default/Management LMK.

Bugs and Errors Corrected

Ref.	Description of Error
CR 12025	Component generation using HSM Manager may incorrectly return an "Incompatible Key Length" error
CR 12012	Zero-length communities and strings should not be allowed in the SNMPADD console command.
CR 12008 CR 12006	An error reporting "Not Enough Memory" is entered into the error log; the payShield 9000 becomes unresponsive when the error log is viewed and requires rebooting. (Note: this affects only software versions 1.4d, 1.4e, and 2.0a.)
CR 11991	NG host command processing not checking for authorized state and clear PIN security setting. (Note: this affects only v2.0a software.)
CR 11960	VR console command does not detect presence of LIC030.
CR 11959	KK host command may incorrectly return error code 07.
CR 11947	NY host command can result in an "Unprocessed Software" entry in the error log.

Ref.	Description of Error
CR 11945	IK console command reports a "key masquerading" error instead of "key all zeroes".
CR 11936	D6 host command - if the imported TMK1 is X variant and/or the KP is X variant the HSM returns the wrong encrypted response.
CR 11931	SNMP MIB file incorrectly references NuDesign.
CR 11930	UTILSTATS console command goes into a loop when displaying host command volumes when there is data for more than 256 different commands.
CR 11929	Display of saved motion sensor settings did not show sensitivity level.
CR 11928	If there is no saved setting for self-test time, a value of "00:00" is assumed instead of "09:00".
CR 11924	IK Console command allows import of key type 000 (ZMK)
CR 11912	If incorrect time is entered in console SETTIME command, the message "The system time has been modified" is displayed. (The time has ***not*** been modified.)
CR 11905	Console command RY does not correctly display the RMK KCV.
CR 11865	Security setting prompt for the "Enable ZEK/TEK …" item is sometimes truncated.
CR 11860	DU Command; when the security parameter "Variable length PIN offset" is set to YES the new length of the offset is being taken from the length of the old PIN, not the new one contained in the New PIN Block.
CR 11854	"RSA Not Licensed" is unnecessarily reported in the error log.
CR 11836	The HSM can become unresponsive when there is a high rate of host commands using too many connections.
CR 11813	Print function "Reverse CR/LF" not working.
CR 11798	Some commands running slower than expected
CR 11790	A0 command failing with Mode set to 'B'
CR 11762	Save settings function not handling the new security setting to Enable ZEK/TEK binary encryption.
CR 11729	MY host command: Padding mode 1 implemented incorrectly for MACing mode 3.
CR 11700	It is possible to change the IP address of a host port that will not work with the current default gateway.
CR 11683	In AUDITOPTIONS, the current value of the counter is displayed as 0.
CR 11665	Key types missing when trying to authorize FK console command.
CR 11604	Keyblock key usage for BDK Types 2 & 3 is not recognized in FK and KG console commands
CR 11568	KO host command can cause host comms port to become unresponsive.

Ref.	Description of Error
CR 11566	RSA key generation occasionally returns error code 15.
CR 11490	Sub-Category for 'genprint' and 'component' doesn't list key types supported.
CR 11481	License for FICON card is deleted when the payShield Return to Factory Settings facility is used.
CR 11464	On a unit power-cycle the audit counter does not initialize to the expected value.
CR 11437	Need to change TKB Key Usage values 'B1' and 'B2' into '41' and '42' respectively.
CR 11388	Console message changed to refer to "HSM Manager" instead of "Management GUI"
CR 11320	In prompts for TRACERT command, "TRACEROUTE" changed to "TRACERT".
CR 10889	KE and KO commands performance is incorrect for the payShield 9000 model they are running on.
CR 10874	The host command FE should fail with error code 68 when key separation is set to Yes
CR 10845	The VA console command does not work while Multiple authorization is Off.
CR 10559	Alarm settings not included when settings are saved.
CR 10558	Adding an SNMP community starts the SNMP service even if it is disabled (and can cause an error to be logged)
CR 10137	ROUTE console command - User still asked to delete a persistent route even if it doesn't exist

1346-0900 (v2.0a) – Released August 2012

(Special request only)

Special Notes

- payShield 9000 v2.0a software should not be used because of important changes made in v2.0b software. Users who have not yet deployed v2.0a software should go directly to v2.0b or later. Users who have already deployed v2.0a software should immediately upgrade to v2.0b or later.
- Remote HSM Manager does not currently support the use of AES LMKs. Local HSM Manager or the Console should be used where AES LMKs are to be deployed.

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 4.0.10

Manuals

- Issue 10.3 of the payShield 9000 manuals should be used with this release.

New functions

Description of Enhancement
Software v2.0 introduces support for the AES cryptographic algorithm. The functionality that can utilize AES includes: ➢ 256-bit AES LMKs ➢ 128/192/256-bit AES key management keys (e.g. ZMK, TMK) ➢ 128/192/256-bit AES data encryption keys (TEK, ZEK, DEK) ➢ 128/192/256-bit AES data authentication keys (TAK, ZAK) Note: the use of the AES algorithm requires the HSM9-LIC007 AES license.

Bugs and Errors Corrected

Ref.	Description of Error
CR 11744	Changing state rapidly can cause the management port to lock, and any process that accesses the management port's IP address to fail.
CR 11584	With asynchronous host comms., if a stream of EI host commands is sent (with no other host commands during this period) the performance will degrade, and then the HSM stops responding.

Version 1.4 Development Stream

Relationship to v1.3

All fixes and enhancements in the v1.3 stream up to and including 1317-0915 (v1.3e) are included in v1.4a. Changes in later versions in the v1.3 stream are not included in the v1.4 stream unless these Release Notes explicitly say that they have been included.

1317-0922 (v1.4g) – Released February 2015

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.8.2

Manuals

- Issue 8.3 of the payShield 9000 manuals should be used with this release.

Security Enhancements and Fixes

Ref.	Description
CR 13098	Addresses vulnerability outlined in Security Advisory TESA-2014-001.
CR 12992	Enhancement to certain console commands following updated best practise review.
CR 12884	-P option removed from NETSTAT console command to (a) ensure compliance with security advisory related to the NetBSD implementation, and (b) to remove option deemed unnecessary for HSM operations. *[NOTE: the –p (lower case) option is still available.*]
CR 12691	If Security Setting "Enable weak PIN checking" is set to NO, weak PIN checking is not performed if a local Weak PIN table is included in a command.
CR 11994	Temperature sensor/alarm is now permanently active.

Bugs and Errors Corrected

Ref.	Description of Error
CR 13130	SG console command may accept an invalid character

Ref.	Description of Error
CR 13037	A0 Host Command returns response code when generating and exporting an IKEY/IPEK after 100+ iterations when using Keyblock LMKs

1317-0920 (v1.4e) – Released January 2013

(Limited release & special request only)

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.8.1

Manuals

- Issue 8.2 of the payShield 9000 manuals should be used with this release.

Bugs and Errors Corrected

Ref.	Description of Error
CR 11947	NY host command can result in an "Unprocessed Software" entry in the error log.
CR 11936	D6 host command - if the imported TMK1 is X variant and/or the KP is X variant the HSM returns the wrong encrypted response.
CR 10874	The host command FE should fail with error code 68 when key separation is set to Yes
CR 10558	Adding an SNMP community starts the SNMP service even if it is disabled (and can cause an error to be logged)

1317-0919 (v1.4d) – Released November 2012

(Special request only)

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.8.1

Manuals

- Issue 8.2 of the payShield 9000 manuals should be used with this release.

Bugs and Errors Corrected

Ref.	Description of Error
CR 11931	Errors caused by SNMP MIB referencing NuDesign
CR 11924	IK Console command allows import of key type 000 (ZMK)
CR 11905	Console command RY does not correctly display the RMK KCV.
CR 11836	The HSM can become unresponsive when there is a high rate of host commands using too many connections.
CR 11813	Print function "Reverse CR/LF" not working.
CR 11798	Some commands running slower than expected
CR 11790	A0 command failing with Mode set to 'B'
CR 11681	User storage cannot be accessed at offset F00.
CR 11665	Key types missing when trying to authorize FK console command.
CR 11604	Keyblock key usage for BDK Types 2 & 3 is not recognized in FK and KG console commands
CR 11568	KO host command can cause host comms port to become unresponsive.
CR 11566	RSA key generation occasionally returns error code 15.
CR 11490	Key types missing when authorizing component and genprint
CR 11437	Need to change TKB Key Usage values 'B1' and 'B2' into '41' and '42' respectively.
CR 11320	In prompts for TRACERT command, "TRACEROUTE" changed to "TRACERT".

1317-0917 (v1.4b) – Released July 2012

(Special request only)

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future*.)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.8.1

Manuals

- Issue 8 of the payShield 9000 manuals should be used with this release.

Special Note

Please see the note against CRs 11340 and 11346 for v1.4a in the section on *Enhancements to Existing Functions* for information relating to the new Default Gateway function for users upgrading from earlier versions.

Bugs and Errors Corrected

Ref.	Description of Error
CR 11662	UDP host communications does not function if only one host Ethernet port is configured.
CR 11618	Cannot re-attach a payShield 9000 after detaching it from their host when using FICON and 3490 device emulation.

1317-0916 (v1.4a) – Released July 2012

(Special request only)

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future*.)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.8.1

Manuals

- Issue 8 of the payShield 9000 manuals should be used with this release.

New functions

Ref.	Description of Enhancement
CR 11555	Support for MU and MW Host commands (for compatibility with legacy applications only). Requires HSM9-LIC034. *(NOTE: the Release Notes issued with v1.3e incorrectly stated that this functionality was included in v1.3e.)*

Enhancements to Existing Functions

Ref.	Description of Enhancement
CR 11132	Allow console command AuditOptions to work (in read-only mode) in Online state.

Ref.	Description of Enhancement
CR 11340 CR 11346	Ethernet ports now support default gateways. Ethernet ports can now be on the same subnet as each other. (***IMPORTANT NOTE: when upgrading from earlier versions of software, all static routes will be deleted, as a default gateway is now available for each interface. If an interface's IP address is set to A.B.C.D, then the default gateway for that interface is initially set to A.B.C.1. The default gateway for each interface may be changed using the console CM or CH or HSM Manager equivalent commands.*** ***If necessary, static routes may be re-entered using the console ROUTE and HSM Manager equivalent commands.)***
CR 11341	KO Host command enhanced to also provide clear public key modulus and exponent.
CR 11432	Audit log size increased to 50,000 records.
CR 11591	BU command modified to support generating check value of IPEK keys.

Bugs and Errors Corrected

Ref.	Description of Error
CR 10930	Using a Remote Manager card with the RC console command causes the card to become un-ejectable.
CR 11102	Entering an incorrect PIN (e.g. RH Console command) causes a smartcard error response instead of asking to re-enter the PIN
CR 11106	When an asynchronous host connection is pulled from the USB socket on the payShield 9000, and put back again, the Host connection becomes blocked.
CR 11111	Incorrect PIN entry in HSM Manager - error message just says 'Card Error'
CR 11117	LW host commands sometimes returns keyblocks with an incorrect Exportability value
CR 11373 CR 11396	Inconsistencies in performance between different host interfaces.
CR 11395	Sending an Async host command with zero length command causes HSM's Host Async port to hang until HSM is rebooted or changed to offline and then back to online.
CR 11425	Unable to authorise the import of a ZMK on the Console command line
CR 11502	KO Host command returns encrypted public key exponent and modulus instead of encrypted private key exponent and modulus.
CR 11510	BW Host command returns BX33 when there is no old LMK loaded.
CR 11549	Changing state returns errlog entry with 'Failed to get host IP address, using any'.

Ref.	Description of Error
CR 11565	ES Host command sometimes incorrectly returns error code 41.
CR 11588	Management Ethernet port might not function if Host 1 Ethernet port is not in use.

Version 1.3 Development Stream

Relationship to v1.2

All fixes and enhancements in the v1.2 stream up to and including 1317-0900 (v1.2a) are included in v1.3a. Changes in later versions in the v1.2 stream are not included in the v1.3 stream unless these Release Notes explicitly say that they have been included.

1317-0915 (v1.3e) – Released March 2012

(Special request only)

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.7.2

Manuals

- Issue 7.1 of the payShield 9000 manuals should be used with this release.

Enhancements to Existing Functions

Ref.	Description of Enhancement
CR 10965	Prompt to enter a new card in RX Console command has been improved
CR 11193	TEK encrypted under a TMK can now be exported.
CR 11242	Diagnostics now report separately on temperature and fan speed. Fans are no longer stopped and re-started by the diagnostics.
CR 11253	New key scheme introduced for SEED (for HSM9-LIC020)
CR 11257	On-screen text for A Console command (multiple authorized activities state) improved to remind user that console authorizations are limited to 720 minutes.
CR 11259	When trying to disable a core command using CONFIGCMDS console command, feedback is now provided that the request has not been actioned.
CR 11260	On-screen text for A Console command (multiple authorized activities state) improved to remind user that persistence can only be applied to host command authorizations. (Persistence required the authorization to be permanent, and console commands cannot now be permanently authorized.)

Ref.	Description of Enhancement
CR 11275	On-screen text for A5 Console command changed to make it clear that limits apply to PIN verification failures.

Bugs and Errors Corrected

Ref.	Description of Error
CR 10548, CR 11139	LMK ID can be set higher than number of licensed LMKs
CR 11369, CR 11141	Import of binary keys allowed without authorization under some circumstances.
CR 11247	When using HSM9-LIC003 (AS2805), errors when importing/exporting keys in key scheme "H".
CR 11293	Requesting Health Check data using HSM Manager results in "Child not found: -1" error message.
CR 11298	With PCI HSM compliant key types implemented, BW Host commands returns error response 04.
CR 11306	DUKPT IPEK should not be parity-adjusted.
CR 11311	PE Host command may return error code 14 even with valid PIN
CR 11318	Diagnostic reporting temperature test failure because fans are turning at wrong speed, even if fan speed is within expected limits.
CR 11335	Corrected types of keyblock keys which can be exported using HSM Manager
CR 11342	Corrected on-screen text in CS & QS Console command relating to Minimum HMAC length.
CR 11368	RS Console command text may show irrelevant entries.

1317-0914 (v1.3d) – Released January 2012

(Special request only)

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. *(Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future*.)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.6.1

Manuals

- Issue 7 of the payShield 9000 manuals is appropriate to this release.

Enhancements to Existing Functions

Ref.	Description
CR 11283	Changes to on-screen messages concerning PCI HSM compliance
CR 11272	Added support for key type BDK-3.
CR 11249	Derivation of DUKPT IPEK keys is now supported by the A0 host command

Bugs and Errors Corrected

Ref.	Description
CR 11279	PIN with incorrect length causes corruption of printed output.

1317-0912 (v1.3b) – Released December 2011

(Special request only)

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future*.)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.5.3

Manuals

- Issue 6 of the payShield 9000 manuals is appropriate to this release.

Enhancements to Existing Functions

Ref.	Description
CR 11073	MAC padding method 3 added.

Bugs and Errors Corrected

Ref.	Description
CR 11225	In DT Console Command, fan speed tolerances changed when reporting on Temperature.
CR 11147	Performance shaping and utilization statistics not working for FICON interface.
CR 11131	I4 Host Command not returning the Hash Modulus Identifier in the response.
CR 11129	Prompt text for FICONTEST Console command made clearer.

Ref.	Description
CR 11074	Host connections may be closed or fail to open.
CR11016	Authorised commands may not be persistent across re-boot.
CR 10966	Remote Operator smart cards may not eject when being managed at the HSM.
CR 10939	If a large number of Remote HSM Manager Administrator and Operator cards are stored in the HSM, then the HSM Manager "Remove card from Security Croup" function does not work and may cause the link between the HSM and HSM Manager to terminate.

1317-0911 (v1.3a) – Released October 2011

(Special request only)

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future*.)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.5.3

Manuals

- Issue 6 of the payShield 9000 manuals is appropriate to this release.

New functions

Description
Support for FICON Host communications (preliminary release).

Enhancements to Existing Functions

Ref.	Description
CR 10336	Support for AmEx CSC v2 and AEVV.
CR 10155	Support for Discover D-PAS EMV chip-card transactions
	DUKPT data encryption (using PIN-variant of transaction key)
	Binary data encryption using any encryption key
CR 11001	FK modified to prompt user for correctness of key check value for component types X, E and S.
CR 9637	FK Console command now checks for authorization before components are entered.

Bugs and Errors Corrected

Ref.	Description
CR 10539	Card does not become active for 2-3 seconds after being inserted.
CR 10613	VR command incorrectly reporting presence of some optional licenses when custom firmware is installed.
CR 10790	GO command does not allow PIN verification using BDK-2.
CR 10790	M2 command uses wrong key variant to decrypt a message encoded using BDK-2.
CR 10799	AG command returns parity error when PCI HSM compliant key types are being used.
CR 10862	HSM can freeze, with error LED blinking red.
CR 10870	TCP/IP keep-alive not working properly
CR 10988	EW (RSA signing) enforces use of DER encoding.
CR 11108	Turning off Alarm settings using HSM Manager does not delete LMKs (in the way that CL Console command does).
CR 9638	When using CL Console command, LMKs should not be erased if alarms are turned on (only if they are turned off).
CR 10699	Difficulty in connecting Remote HSM Manager to low-speed HSMs.

Version 1.2 Development Stream

1317-0900 / 1317-1900 (v1.2a) – Released June 2011

(Special request only)

PCI HSM Compliant?

- ***This software has been certified for PCI HSM compliance.*** PCI HSM compliance of the payShield 9000 is subject to appropriate user settings having compliant values – see manuals.
- Software number 1317-0900 applies if some security settings are not PCI HSM compliant. Software number 1317-1900 applies if all security settings are PCI HSM compliant. (See manuals)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.4.7

Manuals

- Issue 5 of the payShield 9000 manuals is appropriate to this release.

Relationship to v1.1

All fixes and enhancements in the v1.0 stream up to and including 1110-0921 (v1.1b) are included in v1.2a. Changes in later versions in the v1.1 stream are not included in the v1.2 stream unless these Release Notes explicitly say that they have been included.

New functions

Description
This release is certified to be compliant with the requirements of PCI HSM. This introduces the following new capabilities. Full information about these features is included in the manuals set
The ability to change the software revision number (as viewed using the VR Console report) from format nnnn-09nn to nnnn-19nn if the software is PCI HSM certified and all settings have compliant values.
Various indications on the Console and HSM Manager as to the PCI HSM status of the HSM.
New mode in the NO Host command to allow a Host computer to retrieve the PCI HSM status of the payShield 9000.
Minimum length of 5 digits for PINs used to authenticate Console and HSM Manager users.
60-second time-out when PIN entry is requested to authenticate users.

Description
Maximum of 12 hours allowed when authorizing Console commands.
Ability to switch to new key types required for PCI HSM compliant key separation, and extension of the BW Host command to allow keys to be migrated to the new key types.
Ability to switch on restrictions on PIN block usage and translation as required by PCI HSM and ISO 9564/X9.8.
Automated daily self-tests of the HSM, with a facility (e.g. using the ST Console command) to set the time of day when the self-test is run.
Serial numbers of smartcards used to authenticate users are automatically recorded in the Audit Log.
Certain sensitive events are automatically recorded in the Audit Log.
Certain legacy Console commands have been removed.
Certain legacy Host commands are disabled when the HSM is in a PCI HSM compliant state.

Other Enhancements to existing functions

Ref.	Description
CR 10801	Minor change to Random Bit Generator to allow for possible future application extensions.

Bugs and Errors Corrected

Ref.	Description
CR 10899	HSM Manager may fail to view the Audit Log.
CR 10804	Console may become unresponsive if HSM state is changed a large number of times.
CR 10785	Custom TR-31 key types may fail to Import.
CR 10764	With Keyblock LMKs, GK and EW commands incorrectly expect “FF” in certain fields.

Version 1.1 Development Stream

1110-0921 (v1.1b) – Released May 2011

(Special request only)

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.3.16

Manuals

- Issue 4 of the payShield 9000 manuals is appropriate to this release with the following upgrades:
    - Host Command Reference Manual Issue 4.3
    - Console Reference Manual Issue 4.1
    - Local HSM Manager User's Guide Issue 4.1
    - Installation Manual Issue 4.1

Relationship to v1.0

All fixes and enhancements in the v1.0 stream up to and including 1110-0913 (v1.0e) are included in v1.1a. Changes in later versions in the v1.0 stream are not included in the v1.1 stream unless these Release Notes explicitly say that they have been included.

Enhancements to existing functions

Ref.	Description
CR 10704	MAC commands now support
CR 10616	Printer flow control now allows: ➢ Concurrent software and hardware flow control ➢ Hardware flow control allows selection of which line (RTS, CTS, DTR) to use for flow control. ➢ Configurable time-out when waiting for XON.

Bugs and Errors Corrected

Ref.	Description
CR 10804	Console may become unresponsive if switching between Online and Secure states many times in succession.

Ref.	Description
CR 10777	Printing commands that have 2 responses may return error 15 when working in EBCDIC.
CR 10776	When using parallel printers sometimes only 3 digits of the PIN are printed,
CR 10757	RT console command could hang when creating multiple cards and answering "N" to the prompt about overwriting a card.
CR 10755	RT console command incorrectly reports that a card that has been reset using the RX console command contains an LMK component.
CR 10729	Inability to add some cards to some Remote HSM Manager security groups
CR 10688	When trying to remove a smart card from a Remote HSM Manager security group, an incorrect error report is made that the card was used to connect to HSM Manager.
CR 10682	Settings for "CONFIGCMDS" console command are not being retained over a re-boot.
CR 10671	Loading of code fails
CR 10666	FK console command and HSM Manager give different results when forming a key.
CR 10663	An authorized activity that was previously made "permanent" cannot subsequently be made "persistent".
CR 10660	When unauthorizing a sub-category in a category which is authorized, the unauthorization is applied to all the other sub-categories.
CR 10659	Authorization of commands using HSM Manager does not pick up the setting disallowing persistence if that was made at the console.
CR 10658	When using HSM Manager, a modification to make an authorization persistent may be overridden by a subsequent new authorization which is not persistent.
CR 10620	JU command does not return correct response where Mode Flag is 3 or 4.
CR 10614	Occasional crashing of print resource manager.
CR 10593	Incorrect error code sometimes provided when printing.
CR 10572	EO host command (Import a Public Key) may change the ASN.1 encoding of the public key.

Ref.	Description
CR 10543	Authorization of Export for key types 300 and 400 results in "invalid entry" error.
CR10342	Authorization using LMK cards created on another version of HSM software may not work.

1110-0920 (v1.1a) – Released February 2011

(Special request only)

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future*.)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.3.15

Manuals

- Issue 4 of the payShield 9000 manuals has been created for this release. The following manuals are at Issue 4.1:
    - Local HSM Manager User's Guide
    - Installation Manual
    - Host Command Reference manual.

Relationship to v1.0

All fixes and enhancements in the v1.0 stream up to and including 1110-0913 (v1.0e) are included in v1.1a. Changes in later versions in the v1.0 stream are not included in the v1.1 stream unless these Release Notes explicitly say that they have been included.

New functions

Description
Reset to factory (default) settings. **Important -**This function does not change the software and license installed on the HSM. Therefore any software and license installed since the HSM was delivered to the customer will remain on the HSM.
Use of DUKPT for general data encryption
Enhancements to EMV Card data preparation capabilities to allow the use of an Issuer RSA key set for multiple certificates, the ability to use pre-generated RSA keys for the creation of card certificates, and validation for CA self-signed

Description
certificates (KK Host command). (*This functionality requires Optional License 016.*)
Enhancement to EMV Card data preparation to encompass Multos cards.
Card personalization based on EMV Common Personalization Specification (CPS) and Global Platform (GP) using Secure Channel Protocol 2 (SCP02). The Indirect/Explicit method is supported. Also support for the specific process required for MasterCard PayPass Magnetic Stripe Cards. Implemented in IE and IC Host commands. (*This functionality requires Optional License 018.*)
Enablement of the second Host Ethernet port, allowing for 2 concurrently active ports, each with their own IP address and support for 64 threads/connections. This allows users to set up dual network paths to provide resilience against network failure.
Utilization Statistics, to enable users to see how heavily loaded the HSM is, and the volumes of all Host commands. Data is available via the Console, HSM-attached printer, Local HSM Manager, Remote HSM Manager, Host command, or SNMP.
Health Check Status and Statistics, to enable users to see the current health of their HSM and to access counters for health-related events. Data is available via the Console, HSM-attached printer, Local HSM Manager, Remote HSM Manager, Host command, or SNMP.
SNMP Agent Request/Response support to allow Utilization Statistics Health Check data to be retrieved by an SNMP Manager.

Security Enhancements and Fixes

Ref.	Description
CR 10214	Invalid characters in filenames for code loaded onto the HSM are now handled gracefully.
CR 10307	HSM now handles LS host command with too much data.
CR 10312	HSM now handles multiple successive M0 host commands with large payloads.
CR 10352, CR 10353	Malformed host commands are handled gracefully.
CR 10487	Enhancement made to security relating to code loading. PLEASE NOTE: a side effect of this change is that any user downgrading their installed HSM software from v1.1 (or later) to v1.0 will have to re-load their LMK and recover their Remote HSM Management key data (in the same way as if a tamper had occurred).

Other Enhancements to existing functions

Ref.	Description
CR 10488	Enhanced printing performance.
CR 10535	Hardware and software flow control added to printing function.
CR 10545	HSM now checks the printer connection when trying to print.

Bugs and Errors Corrected

Ref.	Description
CR 9792	A6 Console command can cause the HSM to halt if input is too long.
CR 10163	Auditlog Console command can cause an error if the HSM time has been re-set to an earlier time.
CR 10206	Authorization for custom host commands does not work properly in multiple authorised activities mode.
CR 10308	A2 Host command not returning Key Check Value.
CR 10430	PE Host command returns invalid return code.
CR 10506	LMK selection by port number not working for some Host commands (inc. NC and A0).
CR 10611	VR console command now correctly identifies LIC018 and LIC023 licenses.
CR 10554	When the USB serial printing cable is disconnected and reconnected, sometimes the serial settings aren't set.
CR 10600	HSM Manager issue with scroll-bar button in authorization screen.
CR 10595	HSM Manager issue listing currently authorized activities.
CR 10529	HSM Manager issue with timeout value for authorized activities.
CR 10525	HSM Manager issue with Change PIN function after user login.
CR 10512	HSM Manager issue with changing the host configuration details from Offline state.
CR 10474	HSM Manager now supports authorization of custom host commands.
CR 10464	HSM Manager issue supporting for async host connection.

Ref.	Description
CR 10403	HSM Manager now checks for unique subnets on all Ethernet interfaces.
CR 10203	HSM Manager now retains IP address after connection to the HSM is lost (e.g. cable disconnected, HSM reboot, etc.)
CR 10204	HSM Manager was occasionally missing an entry when displaying the error log.
CR 9945	RG console command now correctly ejects Multos card.

Version 1.0 Development Stream

1110-0914 (v1.0f) – Released March 2011

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future.*)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.2.27
- 3.2.22

Relationship to v1.1

All fixes and enhancements in this release are not included in the v1.1 stream unless these Release Notes explicitly say that they have been included.

Manuals

The manuals introduced for v1.0c (Issue 3) are applicable to this release.

Enhancements to existing functions

Ref.	Description
CR 10535	Hardware and software flow control added to printing function.

Bugs and Errors Corrected

Ref.	Description
CR 10620	JU command does not return correct response when mode flag is 3 or 4.
CR 10560	PIN printing does not resume if printer is reconnected after being disconnected
CR 10549	Intermittent corruption of PIN mailers.
CR10544	PIN mailer printing now supports UTF8 characters.
CR 10530	Certain Host commands (inc. M6, SA, JA), when iterated a number of times, can cause error reports and the HSM to halt.
CR 10477	BG Host command can cause the HSM to halt when encountering certain encrypted PIN values.

1110-0913 (v1.0e) – Released December 2010

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future*.)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.2.22

Manuals

The manuals introduced for v1.0c (Issue 3) are applicable to this release.

Enhancements

Description
Enhancements made to Gemalto ADK.

Bugs and Errors Corrected

Ref.	Description
CR 9869	Corrected incorrect reporting of fans turning slowly.
CR 9873	Fan speed resumes at correct rate after use of DT console command.
CR 10441	A2 command using Key Blocks now returns a Key Check Value.

Special Note

The JS and JU commands introduced in 1110-0904 (v1.0b) are now available in this release, and will be carried forward to future releases.

1110-0912 (v1.0d) – Released November 2010

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future*.)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.2.22

Manuals

- The manuals introduced for v1.0c (Issue 3) are applicable to this release.

Enhancements

Description
Support for new smartcards introduced December 2010.

Bugs and Errors Corrected

Ref.	Description
CR 10163	Error light comes on when running AUDITLOG console command.
CR 10293	Key Type 207 failing with IC and IE commands.
CR10308	Key Check Value not returned with A2 Host Command.

Special Note

The JS and JU commands introduced in 1110-0904 (v1.0b) are **not** available in this release.

1110-0911 (v1.0c) – Released September 2010

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future*.)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 3.2.22

Enhancements to existing functions

Ref.	Description
CR 8257	Modified console command CONFIGCMDS, such that it displays the list of currently enabled host/console commands when in Online & Offline state.

Ref.	Description
CR 8256	Modified console command CONFIGPB, such that it displays the list of currently enabled PIN block formats when in Online & Offline state.
	Added new console command RD, which (in Secure state) deletes all remote management related configuration data.
	Modified console command RY, which (in Secure state) no longer prompts to delete all remote management related configuration data.
CR 9108	Modified HSM Manager to support persistent authorized activities.
CR 9576	Modified HSM Manager to support non-base key types.
	Modified HSM Manager to support download of new firmware into the HSM.
	Modified HSM Manager to support download of a new license into the HSM.
	Modified HSM Manager to allow Remote Configuration to be displayed.
	Modified Remote HSM Manager to allow current HSM's Security Group to be displayed.
CR 9819	Console ROUTE "show" command now displays a list of persistent routes, and avoids deletion of all persistent routes if "delete" command is entered without parameters.
CR 9848	When the HSM enters a tampered state, console/host commands are no longer available.

Bug Fixes and Error Corrections

Ref.	Description
CR 9781	Fixed an issue with changing the Advanced Settings via Local/Remote HSM Manager. After changing these settings, the HSM will reboot– if appropriate.
CR 9806	Fixed problem where KO host command could hang HSM when using certain parameters.
CR 9872	Fixed an issue with authorizing activities, which was not permitting key type 002 to be authorized for export.
CR 9949, CR 9950, CR 9951	Fixed internal issues regarding the underlying protocol between HSM and HSM Manager.

Ref.	Description
CR 10037	Removed undocumented console command QK, which displayed the HSM's current state.
CR 10088	Fixed an issue with console command RY, which was incorrectly formatting the output text.
CR 10104	Fixed an issue with copying LMK components using Local HSM Manager.
CR 9625	Fixed an issue with HSM Manager, where the Key Generation Wizard was failing to generate certain types of keys.
CR 9736	Management Port IP address change no longer requires a re-boot.
CR 9806	Fixed an issue in KO command where some parameter settings could cause the HSM to hang.
CR 9809	A8 command now allows TMK to be exported in TR-31 form, when key usage is K0.
CR 9920	Fixed issues in running PA and PC host commands with large amounts of data.
CR 10048	Prevent lost host connections when both left and right keys turned at the same time from Secure state.
CR 9898	Corrected a problem that was causing code loading by FTP to fail.

Special Note

The JS and JU commands introduced in 1110-0904 (v1.0b) are **not** available in this release.

1110-0904 (v1.0b) – Released September 2010

(Limited release only)

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future*.)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 2.6.4

Enhancements

Ref.	Description
SMO 1358, SMO 1359	Introduction of JS and JU commands (requiring HSM8-LIC031) for CUP.

1110-0902 (v1.0b) – Released April 2010

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future*.)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 2.3.9

Bug Fixes and Error Corrections

Ref.	Description
	Fixed problem with DT console command, which was incorrectly reporting that fans were running slowly. (CR9869)
	Fixed problem with DT console command, which on exit, was setting the fans to high speed. (CR9873)
	Fixed problem where console operation was not being restored in the event of the management session being abnormally terminated. (CR9678)
	Fixed internal issue to do with state requirements for console commands. (CR9525)
	Fixed problem where Ethernet based host comms were still active when unit was configured for async connectivity. (CR9140)

1110-0901 (v1.0a) – Released November 2009

Initial release of base software.

PCI HSM Compliant?

This software has not been certified to the PCI HSM standard. (*Note that there is no requirement for HSMs currently in use to be PCI HSM certified or to become PCI HSM certified in the future*.)

HSM Manager Compatibility

This version of HSM software is compatible with the following release(s) of Local/Remote HSM Manager:

- 2.3.9

Other Useful Information

PCI HSM Certified versions of payShield 9000 base software

This table indicates which versions of payShield 9000 software have been formally certified. Note that:

- From v1.2a onwards, the functionality added for PCI HSM compliance exists in all software versions, including those which have not been formally certified.
- Even if certified software is installed on the payShield 9000, in order for the unit to be PCI HSM compliant the hardware must be certified, the security settings must have appropriate values, and the unit must have been delivered in a compliant manner.
- There is no requirement for HSMs currently being deployed to be PCI HSM compliant or to be become PCI HSM compliant in the future.
- "Planned" means that the software is not yet certified, but it is planned to submit it for certification.
- In all PCI certified versions, the software number included in the PCI certificate is of the format xxxx-19xx (as opposed to xxxx-09xx). The software number automatically changes to the xxxx-19xx format when all security settings are PCI compliant. In addition, all software from v2.3c and software in then 2.1 stream from 2.1c onwards also modify their software number in this way, even if the software has not been PCI certified.

Version	PCI HSM Certified	Software Revision if security settings are ***not*** PCI HSM compliant	Software Revision if security settings ***are*** PCI HSM compliant
V1.0a – V1.1b	No	1110-09xx	N/A
V1.2a	**Yes**	**1317-0900**	**1317-1900**
V1.3a – V1.3e	No	1317-0911 to 1317-0915	N/A
V1.4a - V1.4e	No	1317-0916 to 1317-0920	N/A
V2.0a - V2.0c	No	1346-0900 to 1346-0904	N/A
V2.1c	**Yes**	**1346-0905**	**1346-1905**
V2.1d	**Yes**	**1346-0907**	**1346-1907**
V2.1e	No	1346-0908	1346-1908
V2.2a – V2.2b	No	1346-0910 to 1346-0911	N/A
V2.3a – V2.3b	No	1346-0912 to 1346-0913	N/A
V2.3c	**Yes**	**1346-0914**	**1346-1914**

Version	PCI HSM Certified	Software Revision if security settings are ***not*** PCI HSM compliant	Software Revision if security settings ***are*** PCI HSM compliant
V2.3d – v2.3e	No	1346-0915 to 1346-0916	1346-1915 to 1346-1916
V2.3f	**Yes**	**1346-0917**	**1346-1917**
V2.4a	No	1346-0919	1346-1919
V2.4b	No	1346-0921	1346-1921
V3.0b	No	1407-0901	1407-1901
V3.1a	**Yes**	**1407-0902**	**1407-1902**
V3.1b	No	1407-0903	1407-1903
V3.1c	No	1407-0904	1407-1904
V3.1d	**Yes**	**1407-0905**	**1407-1905**
V3.2a	No	1407-0906	1407-1906
V3.2b	No	1407-0907	1407-1907
V3.2c	**Yes**	**1407-0908**	**1407-1908**
V3.3a	No	1407-0910	1407-1910
V3.3b	**Yes**	**1407-0911**	**1407-1911**
V3.4a	No	1407-0915	1407-1915
V3.4b	No	1407-0916	1407-1916
V3.4c	**Yes**	**1407-0917**	**1407-1917**
V3.5a	**Yes**	**1407-0921**	**1407-1921**
V3.5b	No	1407-0925	1407-1925

Further information about PCI HSM compliance and the payShield 9000 can be found in the following Thales documents:

➢ payShield 9000 General Information Manual (Chapter 10) – provided with software versions 1.2a onwards.

payShield 9000 vs. HSM 8000

The payShield 9000 HSM is functionally backward compatible with the Thales HSM 8000 and RG7000 product lines. The host-side functionality provided in payShield 9000 software v1.0 is identical to that provided by the HSM 8000 software v3.1a. However, in order to support some of the more advanced features of the payShield 9000, there are inevitably some differences between the two products. The table below identifies the most significant differences.

payShield 9000 vs HSM 8000			
	Function	**HSM 8000**	**payShield 9000**
Rear Panel	Power Sockets	x1	x1 or x2 (factory fit option)
	Ethernet Host Ports	x1 (10/100 Mbps)	x2 (10/100/1000 Mbps) [1]
	Management Port	x1 (10 Mbps)	x1 (10/100/1000 Mbps)
	Ethernet Printer Port	No	x1 (10/100/1000 Mbps) [2]
	Console Port	9-way 'D' Console Port	via USB-to-serial cable. Max. cable length may be different to HSM 8000.
	Async Host Port	via DTE-DCE cable dongle	via USB-to-serial cable. Max. cable length may be different to HSM 8000.
	ESCON Host Port	Option	No
	FICON Host Port	No	Option
	Serial Printer Port	25-way 'D' Auxiliary Port	via USB-to-serial cable. Max. cable length may be different to HSM 8000.
	Parallel Printer Port	25-way 'D' Printer Port	via USB-to-parallel cable. Max. cable length may be different to HSM 8000.
	Erase Sensitive Data	Red reset/erase button in Secure state (front panel)	Recessed Erase button
Front Panel	Console Port	9-way 'D' Console Port	via USB-to-serial cable. Max. cable length may be different to HSM 8000.
	Reset HSM	Red reset/erase button	Red reset button
	LMK(s) loaded indicator	Secure LED	LMK LED
	Host Activity indicator	Activity LED	Host 1 & Host 2 LED
	Management Activity indicator	No	Management LED
	Power supply indicator	Power LED (Green)	Power LED (various colours)[3]
	Unit serial number	Rear panel	Front & rear panel

[1] Only one Ethernet host port is functional in release v1.0. Dual host port capability became available with v1.1a.

[2] Ethernet printing is not currently supported. It may be implemented in the future, using the AUX Ethernet port.

[3] Colour indicates status of single/dual power supplies

payShield 9000 vs HSM 8000

	Function	HSM 8000	payShield 9000
Configuration	Motion Detector (Sensitivity)	Off/On	Off/Low/Medium/High
	Console Port speed	300…38400 baud	1200…115200 baud
	Async Host Port speed	300…38400 baud	1200…115200 baud
	Serial Printer Port speed	300…38400 baud	1200…115200 baud
	IP routing	via gateway	via gateway or static route
	ROUTE console command	No	Yes
	CA, QA console commands	Yes	No
	Software Update	via ImageLoader utility	via FTP or USB
	Licence Update	via ImageLoader utility	via FTP
	Startup time	~2-3 mins	~20 seconds
	Maximum performance	800 tps[4]	1500 tps[5]
Misc.	PCI HSM certification	No	Yes (selected hardware & software versions). This introduces functionality differences to the HSM 8000 in payShield 9000 v1.2a onwards – see the payShield 9000 General Information Manual, Chapter 10.
	DB, DF, K, YC console command	Yes	Not available from v1.2a onwards
	AA, AE, FC, FE, FG, HC, KA, OE host command	Yes	Not available from v1.2a onwards depending on security settings – see General Information Manual, Chapter 10
	Functionality	n/a	From payShield 9000 v1.1a additional functionality has been added compared with the HSM 8000 – see the payShield 9000 Release Notes.

[4] Multi-threaded CA host command performance using Variant LMK

[5] Multi-threaded CA host command performance using Variant or Keyblock LMK

payShield Manager Compatibility Information

This table lists the releases of payShield 9000 v3.x software, and for each one, indicates which combinations of operating system and browser are supported for running payShield Manager.

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

Operating System	**Windows 7 Ultimate 64-bit SP1**			**Windows 7 Ultimate 64-bit SP1**			**Windows 10 Ultimate 64-bit SP1**			**Linux Ubuntu LTS 64-bit**		**MAC OSX El Capitan**	**MAC OSX High Sierra**	**macOS Big Sur**
Browser	Chrome 32-bit	Firefox 32-bit	Internet Explorer 32-bit	Chrome 64-bit	Firefox 64-bit	Internet Explorer 64-bit	Chrome 64-bit	Firefox 64-bit	Internet Explorer 64-bit	Chrome 64-bit	Firefox 64-bit	Chrome 64-bit	Chrome 64-bit	Chrome 64-bit
1407-x901 (v3.0b)		☑	☑								☑			
1407-x902 (v3.1a)		☑	☑								☑			
1407-x903 (v3.1b)		☑	☑								☑	☑		
1407-x904 (v3.1c)	☑	☑	☑							☑	☑	☑		
1407-x905 (v3.1d)	☑	☑	☑							☑	☑	☑		
1407-x906/x907/x908 (v3.2a/b/c)	☑	☑	☑							☑	☑		☑	
1407-x910/x911 (v3.3a/b)	☑	☑	☑							☑	☑		☑	
1407-x915/x916/x917 (v3.4a/b/c)	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑		☑	
1407-x921 (v3.5a)	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑		☑	
1407-x925 (v3.5b)							☑	☑	☑	☑	☑			☑

Local & Remote HSM Manager Compatibility Information

This table lists the releases of HSM Manager, and indicates which software numbers/versions of payShield 9000 base software they are compatible with.

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

Note: HSM Manager is not compatible with software v3.0 and above.

Part 1 – Versions 3.5.x and later

	Local & Remote HSM Manager Version ↓																	
HSM Software ↓	3.5.3	3.6.1	3.7.2	3.8.1	3.8.2	4.0.8	4.0.10	4.0.12	4.1.0	4.1.4	4.1.7	5.0.19	5.1.4	5.1.7				
payShield 9000																		
1346-0919 to -0922 (v2.4a-c)														☑				
1346-0912 to -0917 (v2.3a-f)														☑				
1346-0910 & -0911 (v2.2a-b)												☑	☑					
1346-0907 & -0908 (v2.1d-e)											☑							
1346-0905 & -1905 (v2.1c)									☑	☑								
1346-0902 to -0904 (v2.0b-c)								☑	☑	☑								
1346-0900 (v2.0a)						☑	☑											
1317-0922 (v1.4g)					☑													
1317-0916 to -0919 (v1.4a-d)				☑														
1317-0915 (v1.3e)			☑															
1315-0914 (v1.3d)		☑																
1317-0911 to -0913 (v1.3a-c)	☑																	

Part 2 – Versions up to 3.4.x

	Local & Remote HSM Manager Version ↓														
HSM Software ↓	2.1.4	2.1.5	2.1.15	2.3.9	2.6.4	2.6.5	3.2.17	3.2.19	3.2.21	3.2.22	3.2.27	3.3.14	3.3.15	3.3.16	3.4.7
payShield 9000															
1317-0900 & -1900 (v1.2a)															☑
1110-0921 (v1.1b)														☑	
1110-0920 (v1.1a)													☑		
1110-0914 (v1.0f)										☑	☑				
1110-0911 to -0913 (v1.0c-e)										☑					
1110-0910 (v1.0c)							☑								
1110-0904 (v1.0b)					☑										
1110-0901 to -0902 (v1.0a-b)				☑											

NOTES:

1. This table can also be used to determine compatibility between HSM Manager and Customised software, by using the version of base software that the customised software was developed from.
2. HSM Manager is designed to work with standard base software, and therefore additional or changed functionality introduced in customised software will not be available through HSM Manager.

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

Contact us

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

> cpl.thalesgroup.com <