Payment Card Industry (PCI)

P2PE Security Requirements and Testing Procedures

Technical FAQs for use with PCI P2PE version 3.x

August 2020

Table of Contents

P2PE Security Requirements and Testing Procedures: Technical Frequently Asked Questions

These Technical Frequently Asked Questions (Tech FAQs) provide answers to questions regarding the PCI SSC (Payment Card Industry Security Standards Council) Point-to-Point Encryption (P2PE) Security Requirements and Testing Procedures (i.e., the P2PE Standard) version 3.x. These FAQs are an integral part of the P2PE Standard and shall be fully considered during a P2PE assessment.

Updates: New or modified questions and/or answers from the last revision are shown in **red.**

General

Q: Aug 2020 - What is the process to use previously-deployed POI devices in a PCI P2PE Solution?

[Note: This FAQ has been imported from the General FAQs on the PCI SSC website]

A *(Note the term "solution provider" below can be used interchangeably with " component provider" depending on the entity managing the POI devices.)*

Please refer to the latest P2PE glossary for definitions of terms used in this FAQ.

This FAQ provides guidance concerning previously-deployed POI devices that can be followed by a P2PE solution provider and a P2PE Assessor as a means to help meet the applicable PCI P2PE requirements.

The P2PE standard contains various requirements regarding the establishment and enablement of POI devices in merchant locations for use in a validated P2PE solution. If these requirements are not specifically adhered to, it may be difficult or impossible for a P2PE Assessor to verify the applicable requirements in P2PE Domains 1, 2, and 5 have been satisfied, especially when the POI devices were deployed either without knowledge of the requirements and/or prior to a P2PE assessment. POI devices already deployed as part of a PCI-listed P2PE v2 solution that are being assessed to the current P2PE Standard should still adhere to this guidance, though, the effort and/or concern is likely minimal.

P2PE solution providers should engage a P2PE Assessor as soon as possible to assess the status of the previously-deployed POI devices. The P2PE Assessor can assess the solution provider's documented processes for POI deployment and note any potential deficiencies requiring remediation.

The following table depicts various scenarios and associated guidance for both a P2PE solution provider and a P2PE Assessor.

NOTE: It is acceptable for the POI devices to retain the necessary keying material to facilitate remote loading (including firmware loading and remote key injection.) If, however, there is any indication there has been a compromise of these keys or the firmware itself, the POI devices must be sent back for re-initialization.	
SCENARIO	**PROCESS**
NEW P2PE ASSESSMENTS A P2PE Assessor has been engaged to perform an initial assessment of a solution provider's new P2PE solution. There are POI device type(s) that need to be assessed that have already been deployed to merchant locations.	The P2PE solution provider engages a P2PE Assessor to assess their solution as required by the PCI P2PE Standard and Program Guide. • If the P2PE Assessor determines the applicable P2PE requirements regarding the previously-deployed POI devices have been satisfied, the P2PE Assessor will document the P-ROV accordingly, which per the P2PE

	Program Guide, can be submitted to the PCI Council upon completion of a successful P2PE assessment. • If the solution provider lacks sufficient evidence to verify the applicable P2PE requirements have been satisfied (as determined by a P2PE Assessor during the course of a P2PE assessment), then all firmware, cryptographic keysNOTE, configurations, and software must be reloaded into the POI devices in accordance with applicable P2PE requirements. At this point, the P2PE Assessor can reassess the applicable requirements.
ADDING A NEW MERCHANT WITH THE SAME POI DEVICE TYPES TO A PCI-LISTED SOLUTION A solution provider with a PCI-listed P2PE solution wants to add a merchant that has already deployed POI devices of the ***same*** POI device type as those approved for use in their P2PE solution (as shown as device dependencies on the P2PE approval listing).	The P2PE solution provider follows their documented processes that were assessed previously as part of their P2PE solution assessment. • If the applicable P2PE requirements regarding the previously-deployed POI devices have been satisfied, the results must be documented by the solution provider and retained for future review. • If the solution provider lacks sufficient evidence to verify the applicable P2PE requirements have been satisfied, then all firmware, cryptographic keysNOTE, configurations, and software must be reloaded into the POI devices in accordance with applicable P2PE requirements.
ADDING A NEW MERCHANT WITH DIFFERENT POI DEVICE TYPES TO A PCI-LISTED SOLUTION A solution provider with a PCI-listed P2PE solution wants to add a merchant that has already deployed POI devices of a ***different*** POI device type as those approved for use in their P2PE solution.	• The solution provider must engage a P2PE Assessor. The P2PE Assessor must follow the P2PE Program Guide Change process to add the new POI device type(s) to the associated PCI P2PE listing. • The P2PE solution provider follows their documented processes that were assessed previously as part of their P2PE solution assessment. ○ If the applicable P2PE requirements regarding the previously-deployed POI devices have been satisfied, the results must be documented by the solution provider and retained for future review. ○ If the solution provider lacks sufficient evidence to verify the applicable P2PE requirements have been satisfied, then all firmware, cryptographic keysNOTE, configurations, and software must be reloaded into the POI devices in accordance with applicable P2PE requirements.

Q: Aug 2020 - How do PCI PTS-approved HSM expiry dates affect a PCI-listed P2PE Solution or Component?

[Note: This FAQ has been imported from the General FAQs on the PCI SSC website]

A *P2PE Solutions and applicable P2PE Components undergoing an initial assessment (i.e., they are not performing a reassessment on an existing PCI P2PE approval listing) must use non-expired HSMs (i.e., not exceeding the PTS HSM approval expiry date as denoted on the applicable PTS listing(s) or FIPS HSMs whose certificates are not on the NIST historical or revoked list).*

PCI-listed P2PE Solutions and Components, as detailed in the P2PE Program Guide, require a full reassessment every 3 years as indicated by the associated "reassessment date" denoted on their PCI P2PE listing. These listed Solutions and Components are allowed to ***reassess*** *their* ***existing*** *PCI P2PE approval* ***up to but not exceeding 3 years*** *past the expiry of any HSMs already included in their approval. This will be checked as part of the reassessment and submittal process to PCI SSC. As the reassessment (provided it results in an updated P2PE listing) is valid for 3 years, this will allow vendors to continue to use the expired HSMs for up to a total of 6 years after any associated PTS HSM listings have expired depending on their reassessment date.*

The Approved PTS Device list with associated expiry dates can be found here: https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices Please refer to the PCI P2PE Standard and Program Guide in our document library for further details.

For quick reference, the following table provides the current PTS HSM expiry dates and the corresponding reassessment window for P2PE Solutions and applicable P2PE Components using these devices:

PCI PTS HSM Version	PCI PTS HSM Approval Expiry Date	P2PE Reassessment End-Date for Expired HSM Devices*	Expired PCI HSMs End Of Life**
1.x	**EXPIRED APR 2019**	**29 April 2022**	**29 April 2025**
2.x	**30 April 2022**	**29 April 2025**	**29 April 2028**
3.x	**30 April 2026**	**29 April 2029**	**29 April 2032**

* *Existing PCI-listed P2PE Solutions and applicable P2PE Components are prohibited from performing a reassessment with any expired HSMs that exceed the reassessment date shown relative to the associated PCI PTS HSM version. E.g., Any PCI-listed P2PE Solution or Component using a v1.x PCI HSM will be prohibited from performing a reassessment after April 29, 2022.*

** *P2PE Solutions and applicable P2PE Components must have replaced any expired HSMs with current (non-expired) HSMs by this date.*

Q: Aug 2020 - How do PCI PTS-approved POI device expiry dates affect a PCI-listed P2PE Solution?

[Note: This FAQ has been imported from the General FAQs on the PCI SSC website]

A *PCI-listed P2PE solutions (and applicable P2PE components) are allowed to reassess their existing PCI P2PE approval with expired PTS POI devices for up to, but not exceeding, 5 years past the PTS POI device expiry dates (as listed on the PCI Approved PTS Devices list) for the POI device types used in the solution.*

POI devices used in a PCI-listed P2PE solution exceeding 5 years past their listed expiry date will no longer be considered valid. A PCI-listed P2PE solution will be delisted if all of its associated POI device types have exceeded the 5-year window (as shown in the table below). In order to understand the impact of P2PE solutions that are using expired POI devices on PCI DSS compliance, please contact the individual payment brands (see How do I contact the payment card brands?).

Each PCI PTS-approved POI device is associated with an expiry date relative to the major version of the PCI PTS POI standard it was evaluated and approved against. Each PTS POI device approval listing indicates its expiry date. The Approved PTS Device list with associated expiry dates can be found here:

https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

For quick reference, the following table provides the current POI device expiry dates and the corresponding revalidation/reassessment window for P2PE solutions using these devices:

PCI PTS POI version	PTS POI Expiry Date	P2PE Revalidation/Reassessment End-date for Expired POI Devices*
1.x	EXPIRED 2014	N/A – v1.x devices are not P2PE eligible
2.x	EXPIRED APR 2017	29April2022
3.x**	30April2021	29April2026
4.x	30April2023	29April2028
5.x	30April2026	29April2031

*** There may be regional variations – please check with the respective payment brands to determine any variances in the dates shown above.**

**** Due to the impact of COVID-19, the PTS POI v3 expiry date has been extended from 30April2020 to 30April2021. As a result, the P2PE Revalidation/Reassessment End-date has changed from 29April2025 to 29April2026. For additional information refer to the PCI SSC POI v3 expiry extension post here.**

Please note that P2PE solutions (and applicable P2PE components) undergoing an initial

assessment must use non-expired (i.e., not exceeding the PTS POI expiry date), eligible PCI PTS POI devices. Please refer to the PCI P2PE Standard and Program Guide in our document library for further details.

Q: Aug 2020 – Is data contained in the "Discretionary Data" field of a payment brand card's track data considered to be sensitive authentication data (SAD), and therefore this data must meet all applicable P2PE requirements (e.g., it must be encrypted)?

A *Discretionary Data fields are defined by the card issuer and/or applicable payment card brand. Issuer-defined fields containing data that are not considered by the issuer/payment brand to be sensitive authentication data (SAD) may be included within the discretionary data portion of the track, and it may be permissible to treat this particular data as non-SAD under specific circumstances and conditions, as defined by the issuer and/or payment card brand.*

A common example is "Fleet cards", which may contain non-sensitive data in the discretionary data field required by the POS system to facilitate certain aspects of the transaction, such as prompting for an odometer reading or restricting the purchase to fuel only.

However, any data considered to be sensitive authentication data (SAD), whether it is contained in a discretionary data field or elsewhere, must be protected according to all applicable P2PE requirements.

A documented record providing justification for handling any data in the discretionary data field as non-SAD must be retained and may be subject to review at any time.

Q: Aug 2020 - Are deprecated RNG-related algorithms acceptable for use in FIPS-approved HSMs, even if the FIPS certificate is still valid?

A *No. While the use of deprecated algorithms for an RNG may not invalidate the FIPS approval, their use is not permitted per the P2PE Standard. However, the HSM can still be used if it is able to utilize non-deprecated algorithms and be shown to disable or otherwise not use deprecated algorithms.*

Domain 1 – Encryption Device and Application Management

Reserved for future use.

Domain 2 – Application Security

General

Q: Aug 2020 – Is it expected that applications on a PTS-approved POI device be assessed according to Domain 2 requirements if forensics tools are not able to observe any data stored locally by the P2PE application due to operating system or firmware constraints, CPU access restrictions, or tamper-resistance mechanisms?

A *It is the expectation of PCI SSC that a P2PE assessor conducting a P2PE application assessment is given sufficient access by the P2PE Application vendor to both the POI device and application software to confirm that the P2PE requirements are actually met. The assessor should be able to install the application per the POI device vendor's security guidance and the P2PE Application's Implementation Guide, run test transactions through the device (or other relevant functionality in order to validate the requirement(s) via the associated P2PE test procedures), and then confirm that the installed configuration meets the P2PE requirements.*

Refer to Domain 2 "Use of a Test Platform" in the P2PE Standard for additional information.

Q: Aug 2020 – If a PTS POI vendor updates their SDK used to develop P2PE Applications, does that require the P2PE Application vendor to perform a Delta change per the P2PE Program Guide to update their existing P2PE Application listing?

A *Yes, if the changes in the SDK result in a change in the P2PE Application that qualifies as requiring a Delta change per the P2PE Program Guide then a Delta is required for the P2PE Application.*

An SDK (Software Development Kit), or any commensurate tool/library/etc. that modifies or has the potential to modify the final code (or binary) of a P2PE Application, even if the P2PE Application vendor does not change any of their own source code, may require a Delta.

Even if the P2PE Application Vendor does not have access to the source code of the SDK, they should have access to information regarding the change to the SDK and understand the effect it will have on their P2PE Application. As a reminder, the Delta criteria for a P2PE Application is: "P2PE Application changes where fewer than half the applicable Requirements/Sub-Requirements are affected.". Note that if at least half of the applicable Requirements/Sub-Requirements are affected, then a full P2PE Application assessment is required.

Refer to the P2PE v3 Program Guide for further details in the PCI SSC document library.

Domain 3 – P2PE Solution Management

P2PE Instruction Manual

Q: Aug 2020 – What are secure methods for a merchant to transport a PTS-approved POI device to satisfy required guidance specified in the P2PE Instruction Manual (PIM) template, for example, if a merchant has to return a POI device to their vendor for repair?

A *The intent in the PIM is that PTS-approved POI devices should be shipped via a trackable shipping method. Examples of trackable shipping methods include private courier services or public shipping companies that provide the status of the package during shipping. The merchant should notify the company to which they are shipping the PTS-approved POI device, and the receiver of the device should validate upon receipt that the bag has not been tampered and is the same bag in which the POI device was shipped.*

Domain 4 – Decryption Environment

Reserved for future use

Domain 5 – P2PE Cryptographic Key Operations and Device Management

NOTE: The PCI PIN v3.0 Technical FAQs apply to P2PE v3.0 (with the exception being applying the appropriate information in P2PE v3.0, including but not limited to P2PE v3.0 Annex C). The PIN technical FAQs will be incorporated into this document in a future revision.

General

Q: Aug 2020 – Are POI vendor-controlled cryptographic keys in scope for Domain 5?

A *Vendor controlled secret and private keys used in connection with the following activities are in scope:*

- *When used in connection with vendor operated PKIs used for remote key loading using asymmetric techniques. Specifically, for the distribution of acquirer keys to transaction originating devices (POIs) for use in connection with PIN and account data encryption whether the actual distribution of acquirer keys occurs from the transaction processing host or is distributed directly by the vendor. This includes Root and Subordinate Certification Authority keys, keys used in connection with associated Registration Authority activities, and other keys associated with the protection of those keys.*
- *When used in connection with KIF activities for loading and/or distribution of acquirer keys to transaction originating devices (POIs) for use in connection with PIN and account data encryption.*

Vendor controlled secret and private keys used for the authentication of firmware on vendor devices, e.g., POIs and HSMs, are not in scope.

18-3

Q: *Aug 2020 – Have the implementation dates for key blocks in requirement 18-3 been changed?*

A *Yes. The Phase 2 and Phase 3 dates have been changed, as detailed below:*

***18-3** Encrypted symmetric keys must be managed in structures called key blocks. The key usage must be cryptographically bound to the key using accepted methods.*

The phased implementation dates are as follows:

- ***Phase 1 –** Implement Key Blocks for internal connections and key storage within Service Provider Environments – this would include all applications and databases connected to hardware security modules (HSM). Effective date: **1 June 2019.** (past)*
- ***Phase 2** – Implement Key Blocks for external connections to Associations and Networks. **New Effective Date: 1 January 2023** (replaces previous effective date of 1 June 2021).*
- ***Phase 3** – Implement Key Block to extend to all merchant hosts, point-of-sale (POS) devices and ATMs. **New Effective Date: 1 January 2025** (replaces previous effective date of 1 June 2023).*

Acceptable methods of implementing the integrity requirements include, but are not limited to:

- *A MAC computed over the concatenation of the clear- text attributes and the enciphered portion of the key block, which includes the key itself – e.g., TR-31;*
- *A digital signature computed over that same data;*
- *An integrity check that is an implicit part of the key- encryption process such as that which is used in the AES key-wrap process specified in ANSI X9.102.*