Payment Card Industry (PCI)
Point-to-Point Encryption (P2PE)®

Technical FAQs for use with PCI P2PE v3.x

December 04 2024

Table of Contents

Document Changes

Date	Description
October 02, 2024	Document title page changed to accurately reflect the Technical FAQs are associated with both the PCI P2PE Standard and Program. Terminology updates throughout to align terminology with the recently updated P2PE Program Guide v3.1. Note these are not denoted in red as they are not contextual changes. (E.g., Changing ‘PCI-Listed’ to ‘Validated’, adding “PTS’ in front of ‘POI’, etc.). **Updated Technical FAQs:** General: Q2, Q3, Q4, Q7, Q8, Q9 Domain 2: Q2 **New Technical FAQ(s):** Domain 2, Q4
October 31 2024	**New Technical FAQ**: General: Q13
December 04 2024	**New Technical FAQ(s):** General: Q14 Domain 2: Q5

PCI P2PE: 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, including the associated Program. These FAQs are an integral part of the PCI P2PE Standard and Program, 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.**

Refer to the P2PE Program Guide and the P2PE Glossary as necessary regarding terminology used.

General

Q1: Oct 2021 (Updated Mar 2024) - Are remote assessments permitted under the PCI P2PE Program?

A *P2PE Assessors are expected to perform onsite assessments for P2PE Products, where applicable. While onsite assessments continue to be the expected method for PCI SSC assessments, the use of remote assessment methods may provide a suitable alternative in legitimate scenarios where an onsite assessment is not feasible. Refer to the PCI SSC Remote Assessments Guidelines and Procedures for details of remote assessment procedures and methods that may be used when an onsite assessment cannot be performed.*

If remote assessment methods are used in place of an onsite assessment, the P2PE Assessor must complete the Addendum for ROC/ROV: Remote Assessments, as provided in Appendix A of the PCI SSC Remote Assessment Guidelines and Procedures document, for submission to PCI SSC along with the applicable P-ROV(s).

Q2: Oct 2021 (Updated Oct 2024) - What is the current P2PE Standard and Program Guide?

A *The current/latest PCI P2PE Standard is v3.1.*

The current/latest PCI P2PE Program Guide is v3.1.

PCI P2PE v3.1:

- *Mandatory for New Assessments of P2PE Products and Reassessments of Validated P2PE Products as of 01 Jan 2022*
- *Requires use of the latest v3.x P-ROVs*
- *P2PE v3.1 does not affect the Annual Revalidation or Reassessment dates for Validated P2PE Product listings assessed to earlier versions*

Q3: Dec 2020 (Updated Oct 2024) - Will new P2PE Solution or P2PE Component submissions be Accepted if they use an Expired P2PE Product (i.e., an Expired P2PE Component and/or Expired P2PE Application)?

A *No. New P2PE Product submissions will not be Accepted if they use Expired P2PE Products. If at any time prior to Acceptance of the submission, including during the PCI SSC AQM review process, a P2PE Product dependency is expired or expires, the P2PE Product submission will be rejected.*

Refer to the latest P2PE v3.x Program Guide in the PCI SSC Document Library. If a P2PE Component or P2PE Application is not on the List of Validated P2PE Components or the List of Validated P2PE Applications, respectively, then it must undergo a Full Assessment as part of the assessment and submission process. Ultimately the P2PE Product submission must satisfy all applicable P2PE Standard requirements, whether by being assessed or through the use of an applicable Validated P2PE Product(s).

Q4: Dec 2020 (Updated Oct 2024) - Will P2PE Solution or P2PE Component Reassessment submissions (Full Assessments) be Accepted if they use an Expired P2PE Product (i.e., an Expired P2PE Component and/or Expired P2PE Application)?

A *No. Reassessments (Full Assessments) of P2PE Products will not be Accepted if they use Expired P2PE Products. If at any time prior to Acceptance of the submission, including during the PCI SSC AQM review process, a P2PE Product dependency is expired or expires, the P2PE Product submission will be rejected.*

Refer to the latest P2PE v3.x Program Guide in the PCI SSC Document Library. A Reassessment requires a Full Assessment of the P2PE Product. If a P2PE Component or P2PE Application is not on the List of Validated P2PE Components or the List of Validated P2PE Applications, respectively, then it must undergo a Full Assessment as part of the assessment and submission process. Ultimately the P2PE Product submission must satisfy all applicable P2PE Standard requirements, whether by being assessed or through the use of an applicable Validated P2PE Product(s).

Q5: Dec 2020 – Can Expired P2PE Components or Expired P2PE Applications be added to Validated P2PE Solutions or Validated P2PE Components as part of a Delta Change?

A *No. Delta Change submissions will not be Accepted if they use Expired P2PE Products. If at any time prior to Acceptance of the Delta Change submission, including during the PCI SSC AQM review process, a P2PE Product being added as part of the Delta Change is expired or expires, the Delta Change submission will be rejected.*

Refer to the latest P2PE v3.x Program Guide in the PCI SSC Document Library. A Delta Change to add P2PE Components and/or P2PE Applications to an existing Validated P2PE Solution or Validated P2PE Component without further assessment requires the P2PE Product being added to be on the List of Validated P2PE Components or the List of Validated P2PE Applications, respectively.

Q6: Dec 2020 (Updated Oct 2024) - If a Validated P2PE Product uses another Validated P2PE Product as a dependency that expires (and therefore the dependency P2PE Product moves to the P2PE Expired Listings), is that expired P2PE Product automatically removed from the parent Validated P2PE Product listing?

E.g., a Validated P2PE Solution uses a Validated KIF, where the KIF expires and the KIF moves to the Expired P2PE Listings. Is the KIF dependency removed from the Validated P2PE Solution listing?

A *No. However, as P2PE Products on the P2PE Expired Listings are no longer considered validated, the P2PE Product Vendor is encouraged to promptly remediate any expired dependencies.*

Options for remediating the existence of an expired dependency will vary depending on the specific P2PE Products involved. These options may include, but are not limited to, one or more of the following:

- *Discontinuing the use of the expired dependency and removing it from the Validated P2PE Product's Listing, provided the removal of the dependency is remediated as necessary.*
- *Replacing the expired dependency with a commensurate Validated P2PE Product.*
- *Undergo a P2PE assessment to validate the applicable P2PE requirements previously satisfied by the use of the now-expired P2PE Product.*

P2PE Product Vendors are encouraged to consult with a P2PE Assessor Company to determine the appropriate course of action for your unique situation.

Refer to the latest P2PE v3.x Program Guide located in the PCI SSC Document Library.

Q7: Aug 2020 (Updated Oct 2024) - What is the process to use previously-deployed PTS POI devices in a PCI P2PE Solution?

A *(Note the term "Solution Provider" below can be used interchangeably with "Component Provider" depending on the entity managing the PTS POI devices.)*

This FAQ provides guidance concerning previously-deployed PTS 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 PTS 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 have been satisfied, especially when the PTS POI devices were deployed either without knowledge of the requirements and/or prior to a P2PE assessment.

P2PE Solution Providers (or P2PE Component Providers, as applicable) should engage a P2PE Assessor as soon as possible to assess the status of the previously-deployed PTS POI devices. The P2PE Assessor can assess the Solution Provider's documented processes for PTS 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 PTS 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 PTS POI devices must be sent back for re-initialization.

SCENARIO	PROCESS
New Assessments A P2PE Assessor is engaged to perform an initial assessment of a Solution Provider's new P2PE Solution. There are PTS 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 P2PE Solution as required by the PCI P2PE Standard and Program. • If the P2PE Assessor determines the applicable P2PE Standard requirements regarding the previously-deployed PTS POI devices have been satisfied, the P2PE Assessor will document the P-ROV accordingly, which per the Program Requirements, 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 keys NOTE, configurations, and software must be reloaded into the PTS 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 PTS POI Device Types to a Listed P2PE Solution A Solution Provider with a Validated P2PE Solution wants to add a merchant that has already deployed PTS POI devices of the ***same*** PTS POI device type as those approved for use in their P2PE Solution (as shown in the device dependencies on the Validated P2PE Solution 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 PTS 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 keys NOTE, configurations, and software must be reloaded into the PTS POI devices in accordance with applicable P2PE requirements.
ADDING A NEW MERCHANT WITH DIFFERENT PTS 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 keys NOTE, configurations, and software must be reloaded into the POI devices in accordance with applicable P2PE requirements.

Q8: Aug 2020 (Updated Oct 2024) - How do PCI PTS-approved HSM expiry dates affect a Validated P2PE Solution or Validated P2PE Component?

A *P2PE Solutions and applicable P2PE Components undergoing an initial assessment (i.e., they are not performing a Reassessment relative to 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).*

Validated P2PE Solutions and Validated P2PE Components, as detailed in the P2PE Program Guide, require a 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 the 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	**Expired 30 April 2022**	**29 April 2025**	**29 April 2028**
3.x	**30 April 2026**	**29 April 2029**	**29 April 2032**
4.x	**30 April 2032**	**29 April 2035**	**29 April 2038**

* *Existing Validated P2PE Solutions and applicable Validated 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 Validated P2PE Solution or Validated P2PE Component using a v1.x PCI HSM will be prohibited from performing a reassessment after April 29, 2022.*

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

Q9: Aug 2020 (Updated Oct 2024) - How do PCI-approved PTS POI device expiry dates affect a Validated P2PE Product?

A *Validated P2PE Solutions, P2PE Applications, and applicable P2PE Components are allowed to reassess their existing Validated P2PE Product 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 PTS POI device types used in the P2PE Product.*

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

Each PCI-approved PTS POI device is associated with an expiry date relative to the major version of the PCI PTS POI Standard and Program 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 PTS POI device expiry dates and the corresponding Reassessment window for P2PE Products using these devices:

PCI PTS POI version	PTS POI Expiry Date	P2PE Reassessment End-date for Expired PTS POI Devices[1]
1.x	Expired 2014	N/A – v1.x devices are not P2PE eligible
2.x	Expired APR 2017	29April2022
3.x	Expired 30April2021	29April2026
4.x	Expired 30April2024	29April2029
5.x	30April2026	29April2031
6.x [2,3]	30April2031	29April2036

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

2 PCI PTS POI v6+ approvals have additional considerations for firmware expiry. Refer to the FAQ herein regarding how PTS POI device v6+ firmware expiry affects P2PE assessments and listings.

3 The PTS POI v6 expiry date was extended from 30April2030 to 30April2031

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. For further information regarding P2PE Applications and expired PTS POI devices, also refer to Q4 in Domain 2 in this document.

Q10: 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.

Q11: 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.*

Q12: Mar 2022 (updated July 2023) - Can HSMs on the NIST CMVP Historical Validation List be used in a P2PE Solution/Component?

A ***New Assessments****: Yes, however the P2PE Assessor must determine the Historical Reason for the transition to the CMVP Historical list does not compromise the P2PE Solution/Component from satisfying applicable P2PE requirements. This analysis must be documented in the appropriate P-ROV for requirements 4A-1.1 and 1-3, as applicable.*

Annual Revalidations & Reassessments*: Validated P2PE Products can continue to use HSMs that were assessed as part of their initial (New) P2PE assessment that are on the CMVP Historical Validation List, as long as all other requirements are met during the Annual Revalidation and Reassessment processes.*

The P2PE Product vendor is encouraged to make a risk determination on whether to continue using the HSMs on the CMVP Historical Validation List based on their own assessment of where and how the HSM is used within the P2PE Product.

Q13: Oct 2024 - For Delta Change submissions, is it permissible for the P-ROV(s) to contain additional changes (redline or otherwise) that do not pertain to the Delta Change(s) being submitted?

A *No. The Delta Change submission must only include redlined changes in the applicable P-ROV(s) that pertain to the Delta Change(s) being submitted as denoted in the accompanying Change Impact Template. This is in accordance with the Delta Change Process defined and detailed in the PCI P2PE Program Guide as well as accounted for in the P-AOV.*

In addition, the redline P-ROV(s) must not contain any redline from any previous Delta Change submissions. Any previous redline content must be maintained and denoted in black text (unless that previous redline content is subject to the Delta Changes being submitted.)

Q14: Dec 2024 - Where part of the PTS POI device firmware is denoted under the "Applic #:" section on the associated PTS approval listing, how should that be documented in a P2PE assessment?

A *In the PCI PTS POI Program, firmware can also be denoted as an 'Application' (not to be confused with a P2PE Application or Non-payment Software) and listed as such on the PTS POI approval via the 'Applic:' label. This usually occurs if the firmware is modular, and it is at the PTS POI device vendor's discretion in terms of how they prefer it to be listed on the PTS approval of their PTS POI device.*

For P-ROVs and the PIM, denote the 'Applic #' version information under the 'Firmware' column and prefix 'Applic#:' to it. E.g., Applic#: 1.x

Domain 1 – Encryption Device and Application Management

Q1: Mar 2024 – For PTS POI Devices v6 and later, how does the PTS approval expiry date and status of the POI device firmware (denoted on the PTS listing) affect both New P2PE assessments and Validated P2PE Products?

Note: Refer to the PTS POI Program Guide in the PCI SSC Document Library for details regarding PTS POI device v6 and later firmware expiry.

A. ***New Assessments:*** *As per P2PE requirement 1A-1.1, the PCI PTS POI device approval must not be expired. In addition, for PTS POI v6 and later devices, the firmware must not be expired and past its 4-month grace period (i.e., it must not be red status). If at any time prior to Acceptance of the P2PE Product submission, including during the PCI SSC AQM review process, the POI device firmware status turns red, the P2PE Product submission will be rejected.*

Annual Revalidations and Reassessments: *Entities are encouraged to use non-expired POI device firmware. With regard to the overall PTS approval expiry, refer to the FAQ herein "How do PCI-approved PTS POI device expiry dates affect a Validated P2PE Solution?"*

Q2: Mar 2024 – The current v3.1 P2PE Standard states the following regarding sampling (examination and functional testing) of eligible PTS POI devices:

> “***POI devices and applications/software must include every unique combination of hardware, firmware, and versions and configurations of both P2PE applications and P2PE non-payment software used by the solution.***”

Is there revised instruction to the sampling criteria above regarding the POI devices supported by a P2PE Product, especially given the prevalent adoption of Validated P2PE Solutions and the significant availability of eligible PCI-approved PTS POI devices that a P2PE Solution can support on behalf of merchant customers?

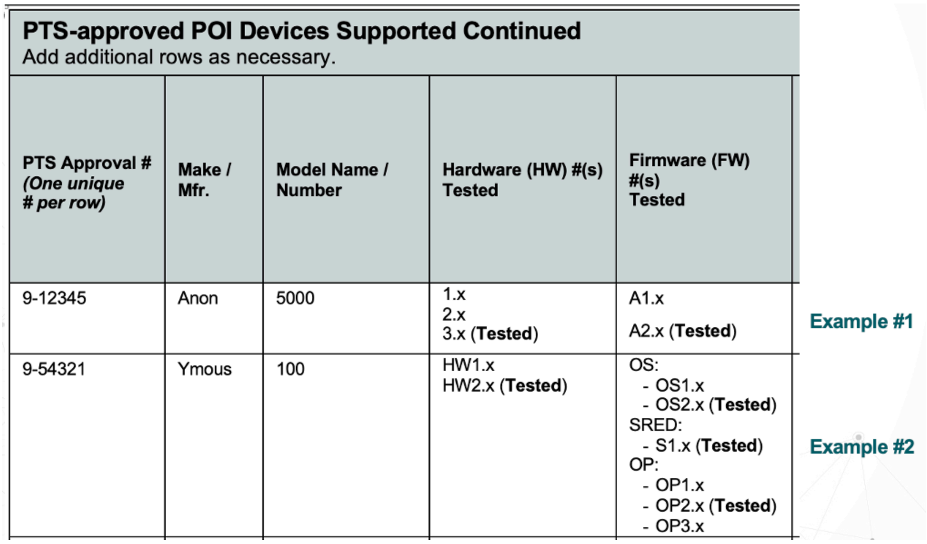
A *Yes. With respect to the PTS POI device HW/FW combinations, at least one unique combination of POI device HW and FW (example #1) supported by the P2PE Product must be validated and functionally tested (as determined by the P2PE requirements and associated testing procedures)* ***from each*** *PTS approval that is being associated with the P2PE Product assessment.*

Where the FW is not monolithic (example #2), i.e., it is split into separate FW functionality (e.g., OS, SRED, OP), every FW required for the device to function as intended must be validated and functionally tested (as determined by the P2PE requirements and associated testing procedures).

The Assessor must document in the appropriate P-ROV, ***for each*** *associated PTS approval, the supported POI device HW/FW(s) combinations that were validated and functionally tested, in addition to all eligible HW and FW from the same PTS approval being supported by and intended to be listed for the P2PE Product. Note that all supported POI devices must be in accordance with the governing P2PE requirements (e.g., 1A-1). When populating the POI device version information in the P-ROV, where the version tested is included in a wildcard version as shown in the PTS approval, document the wildcard version instead of the explicit version tested. E.g., if FW version 1.1 is tested, and the PTS approval denotes 1.x, then populate 1.x.*

The P2PE Assessor is encouraged to determine if more combinations within a PTS Approval should be examined and tested based on their knowledge of the P2PE Product and the POI devices.

Example P-ROV documentation extract (for illustrative purposes only):



PTS-approved POI Devices Supported Continued
Add additional rows as necessary.

PTS Approval # ***(One unique # per row)***	**Make / Mfr.**	**Model Name / Number**	**Hardware (HW) #(s) Tested**	**Firmware (FW) #(s) Tested**	
9-12345	Anon	5000	1.x 2.x 3.x (**Tested**)	A1.x A2.x (**Tested**)	**Example #1**
9-54321	Ymous	100	HW1.x HW2.x (**Tested**)	OS: - OS1.x - OS2.x (**Tested**) SRED: - S1.x (**Tested**) OP: - OP1.x - OP2.x (**Tested**) - OP3.x	**Example #2**

Domain 2 – Application Security

General

Q1: Aug 2020 – Is it expected that applications on a PCI-approved PTS 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 PTS POI device and the P2PE Application to confirm that the P2PE requirements are actually met. The assessor should be able to install the application per the PTS 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 Standard test procedures), and then confirm that the installed configuration meets the applicable P2PE Standard requirements.*

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

Q2: Aug 2020 (Updated Oct 2024) – 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 (Software Development Kit) result in a change in the P2PE Application that qualifies as requiring a Delta Change per the P2PE Program Guide then a Delta Change is required for the P2PE Application.*

An SDK, 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 Change.

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.

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

Q3: Aug 2022 - Requirements 2A-3.1.1 and 4B-1.8 state "as specified in PCI DSS and/or related FAQs that specify allowable digits" as they relate to truncated PANs. Is there an explicit reference that can be provided with regard to truncation and allowable digits?

A *Yes. There are two FAQs on the PCI SSC Website: FAQ 1091 - What are acceptable formats for truncation of primary account numbers? and FAQ 1117 - Are truncated Primary Account Numbers (PAN) required to be protected in accordance with PCI DSS?*

Q4: Oct 2024 – Is it permitted to assess a P2PE Application with an expired PTS POI device in order to support Listed P2PE Solutions that are already using the [now] expired PTS POI device?

A *Yes.*

It is permitted to perform a P2PE Application assessment (A New Assessment or a Delta Change for the P2PE Application, as applicable) with an expired PTS POI device.

The P2PE Application must abide by the P2PE Program Guidance regarding "PTS POI Device Expiry", including the P2PE Technical FAQ "How do PCI PTS-approved POI device expiry dates affect a Validated P2PE Product?"

The P2PE Application ROV must include documentation stating the expired PTS POI device is intended for use in pre-existing Listed P2PE Solutions that are already using the device.

Note: *As per the P2PE Standard and Program, P2PE Solutions (and Components) cannot undergo a New Assessment using an expired PTS POI device and cannot perform a Delta Change to add an expired PTS POI device. I.e., the [now] expired PTS POI device must already be associated with, and denoted on, the Listed P2PE Solution the P2PE Application is intended to be incorporated into.*

Q5: Dec 2024 – Regarding P2PE Application versioning, what are acceptable 'separators' used between alphanumeric elements as denoted in the P2PE Program Guide, Appendix E, section E.1?

A *The following separators may be used (as defined in the ASCII Table) in a P2PE Application version:*

Description	Symbol (Separator)	DEC	HEX
Hyphen, minus	-	45	2D
Period, dot	.	46	2E
Underscore	_	95	5F

Use of any other characters (e.g., spaces, commas, etc.) is not permitted.

Domain 3 – P2PE Solution Management

P2PE Instruction Manual (PIM)

Q1: Aug 2020 – What are secure methods for a merchant to transport a PTS 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 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 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 PTS PIN v3.x Technical FAQs apply to P2PE v3.x (with the exception being applying the appropriate information in P2PE v3.x, including but not limited to P2PE v3.x Annex C). The PIN technical FAQs will be incorporated into this document in a future revision.

General

Q1: Aug 2020 – Are PTS POI device 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., POI devices and HSMs, are not in scope.

12-5

Q2: Aug 2022 – Is it acceptable for any entity (regardless of an existing P2PE implementation) to use triple-length TDEA for HSM MFKs if they have a documented AES migration plan?

A *Yes. A documented plan to migrate from a triple-length TDEA implementation to an AES implementation is acceptable if there are constraints inhibiting an AES implementation at the time of the P2PE assessment. The migration plan and constraints inhibiting a current AES implementation must be provided for review to the P2PE Assessor and documented in the applicable P-ROV accordingly as part of the P2PE assessment.*

The migration plan to AES must, at a minimum:

- *Identify all system components relying on and/or supporting TDEA.*
- *Identify the constraint(s) inhibiting the use of AES for the MFK for each identified system component.*
- *Document the steps and timeframes for updating TDEA to AES for the MFK for each system component using TDEA.*

18-3

Q3: 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).(past)*
- ***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).*

32-9

Q4: Dec 2020 – Are there revisions to P2PE requirement 32-9 based on the PIN v3.1 changes?

A *Yes. The revised requirement is below:*

Requirement 32-9:
The KIF must implement a physically secure room for key injection where any secret or private keys or their components/shares appear in memory outside the secure boundary of an SCD during the process of loading/injecting keys into an SCD.

The secure room for key injection must include the following:

• ***Effective 01 January 2024****, the injection of clear-text secret or private keying material must not be allowed for entities engaged in key injection on behalf of others. This applies to new deployments of PTS POI v5 and higher devices. Subsequent to that date, only encrypted key injection shall be allowed for PTS POI v5 and higher devices.*

• ***Effective 01 January 2026****, the same restriction applies to entities engaged in key injection of devices for which they are the processors.*

Note*: This does not apply to key components entered into the keypad of a secure cryptographic device, such as a device approved against the PCI PTS POI Security Requirements. It does apply to all other methods of loading of clear-text keying material for PTS POI v5 and higher*