Payment Card Industry (PCI)

Point-to-Point Encryption

Technical FAQs for use with P2PE Versions 1.x

July 2014

Table of Contents

Technical Frequently Asked Questions for *Point-to-Point Encryption Versions 1.x*

These technical FAQs provide answers to questions regarding the application of the *Payment Card Industry (PCI) Point-to-Point Encryption (P2PE)* standards. These FAQs provide additional and timely clarifications to the application of the *P2PE Solution Requirements and Testing Procedures*. The FAQs are an integral part of those requirements and shall be fully considered during the P2PE assessment process. Each answer is followed by the associated reference from the *PCI Point-to-Point Encryption Solution Requirements and Testing Procedures.*

The references below apply to both P2PE Hardware/Hardware and Hardware/Hybrid Standards for v1.x, unless otherwise indicated.

Updates: New questions or those modified for clarity are shown in **red.**

General Questions

No FAQs in this section – Reserved for future use.

Introduction: Solution Requirements for Point-to-Point Encryption

No FAQs in this section – Reserved for future use.

Scope of Assessment for P2PE Solutions

Third Parties/Outsourcing

Q 1 July 2014 – Can a P2PE solution provider outsource elements of their P2PE solution?

A *Yes, a P2PE solution provider can outsource certain functions of their P2PE solution to third parties. The solution provider still maintains overall responsibility for ensuring their third parties are meeting P2PE requirements.*

References:

"Roles and Responsibilities":

> *The P2PE solution provider is a third-party entity (for example, a processor, acquirer, or payment gateway) that has overall responsibility for the design and implementation of a specific P2PE solution, and (directly or indirectly through outsourcing) manages P2PE solutions for its customers and/or manages corresponding responsibilities.*
>
> *The solution provider has overall responsibility for ensuring that all P2PE requirements are met, including ensuring that P2PE requirements are met by any third-party organizations that perform P2PE functions on behalf of the solution provider, such as Certification Authorities and key-injection facilities.*

"Third Parties/Outsourcing":

> *A given P2PE solution may be entirely performed and managed by a single solution provider, or the solution provider may outsource certain functions (for example, loading keys into POIs) to third parties who perform these functions on behalf of the solution provider. All third parties that perform P2PE functions on behalf of the assessed P2PE solution provider, including POI vendors, KIFs, CAs, etc., must be validated per P2PE solution requirements.*

Q 2 **July 2014 – Can a third-party entity that performs P2PE functions on behalf of a P2PE solution provider undergo their own P2PE assessment, rather than undergoing an assessment each time a customer undergoes a P2PE assessment?**

A *Yes, per P2PE "Third parties/Outsourcing" section noted below. Note that certain entities may have no P2PE responsibilities. For example, they may only resell the solution and never touch the hardware or the merchant environment. However, for those entities that perform P2PE functions such as key injection, transport and/or installation of devices, securing/managing POI devices during the lifecycle, device administration, merchant support, etc. there are relevant P2PE requirements, for example in Domains 1 and 6.*

Reference:

"Third Parties/Outsourcing":

There are two options for third-party entities performing functions on behalf of solution providers to validate compliance:

1. *They can undergo a P2PE assessment of relevant P2PE requirements on their own and provide evidence to their customers to demonstrate their compliance; or*
2. *If they do not undergo their own P2PE assessment, they will need to have their services reviewed during the course of each of their solution provider customers' P2PE assessments.*

Third-party providers that have been validated as meeting all relevant P2PE criteria may complete a specific attestation of validation (signed by the third party and the QSA (P2PE), which can be used as evidence for each individual P2PE solution provider (per option 1, above).

Q 3 **July 2014 - What is acceptable evidence concerning P2PE compliance for a third-party entity that underwent a P2PE assessment for services they offer on behalf of P2PE solution providers, such that the third-party can provide that evidence to subsequent P2PE solution providers who use those same services?**

A *This topic will be addressed in P2PE v2.0. In the interim and for P2PE v1.1.1 assessments, a third-party who is providing services on behalf of P2PE solution providers can provide a statement to solution providers pursuing a P2PE assessment based on a prior P2PE assessment of the third-party entity. Note that this FAQ applies only to services governed under P2PE Domains 1, 5, or 6 (including Annexes A and B) such as POI device management, decryption environment related functions, Key Injection Facility (KIF) services, Certification Authority (CA), or Registration Authority (RA).*

The date the P2PE statement is signed for the third-party's P2PE assessment (whether assessed as part of a full P2PE solution or in isolation) must be less than one year before the date of any subsequent solutions provider's P2PE assessment completion date (i.e., the statement described herein is only valid for one year).

This statement, as stated above, must be prepared by the QSA (P2PE) who assessed the third-party. The statement must be signed and dated by both the third-party and the QSA (P2PE), and must attest to the fact that the third-party entity is compliant with all applicable P2PE requirements. The statement must also contain [at a minimum] the following information, as applicable to the third-party. Note that the statement is not required to contain any sensitive information.

- *Provide a summary of services being offered by the third party.*
- *Provide information per the following bullets, which reference sections and tables present in the Solution P-ROV Template v1.1.1. Please refer to that document as applicable.*

- *Provide administrative information regarding the third-party and the QSA (P2PE) using Section 1.1 as a reference.*
- *Provide information requested in Sections 1.2 and 1.3 regarding the date and timeframe of the assessment, as well as the version of the P2PE Standard utilized.*
- *Provide information requested in Section 2.4 regarding the P2PE decryption environment(s).*
- *Provide all information requested in Section 3.5 regarding key management.*
- *Provide the information requested in Table 1.1 and 1.2 in Domain 1 regarding the POI devices used. Exclude information regarding payment applications as they are not relevant to third-party P2PE services applicable to this attestation.*
- *Provide all information requested in Table 1.3 and 1.4 in Domain 1 regarding SCDs used to generate, load, or encrypt cryptographic keys. Examples include HSMs, key-injection/loading devices (KLDs) and other devices that generate or load keys.*
- *Provide all information requested in Table 5.1 and 5.2 in Domain 5 regarding HSM's used in the decryption environment.*
- *Provide all information requested in Table 5.3 in Domain 5 regarding Host Systems used in the decryption environment (HW/Hybrid ONLY).*
- *Provide all information requested in Table 6.1 and 6.2 (Domain 6), as well as Tables 6A.1 (Domain 6, Annex A) and 6B.1 (Domain 6, Annex B) regarding cryptographic key types and their associated hardware devices.*

- *List each high-level P2PE requirement assessed and indicate whether the requirement was assessed in full (i.e., inclusive of all its sub-requirements), partially, or deemed not applicable. Provide a justification for all applicable requirements only tested partially or deemed not applicable. "Not Applicable" in this context infers the requirement may apply but was deemed not applicable via the assessment process and the review of relevant information. For example, applicable in this context would not refer to Domain 2 requirements that govern POI-resident payment applications. An example of requirements later deemed not applicable via the course of the assessment would be a KIF facility that doesn't utilize DUKPT keys.*
- *Include an explicit confirmation attesting to the fact the third-party entity's prior P2PE assessment includes all services, processes, and systems appropriate to the services the third party offers to P2PE solution providers. At any time during the one-year period of the statement's validity, if any services, processes, or systems were changed or added, the third-party must document any additions or changes and provide that documentation to applicable current and potential P2PE solution providers.*

Reference:

"Third Parties/Outsourcing":

> *There are two options for third-party entities performing functions on behalf of solution providers to validate compliance:*
>
> 1. *They can undergo a P2PE assessment of relevant P2PE requirements on their own and provide evidence to their customers to demonstrate their compliance; or*
> 2. *If they do not undergo their own P2PE assessment, they will need to have their services reviewed during the course of each of their solution provider customers' P2PE assessments.*
>
> *Third-party providers that have been validated as meeting all relevant P2PE criteria may complete a specific attestation of validation (signed by the third party and the QSA (P2PE), which can be used as evidence for each individual P2PE solution provider (per option 1, above).*

P2PE At-a-Glance

No FAQs in this section – Reserved for future use.

Domain 1 – Encryption Device Management

1A-1 Use of SRED devices

Q 1 May 2013 – Can a previously-deployed POI be included in a P2PE solution?

A *Solution providers wishing to validate their solutions to the P2PE Hardware/* Standards may include POI devices that are already deployed, as long as all P2PE Requirements are followed during the process of bringing the devices into compliance, and all applicable requirements are verified as being in place for each deployed device. This applies only to deployed POI devices that have already been validated to PTS with SRED.*
There are two options:

- *Option 1: The solution provider has sufficient evidence to verify that all POIs were deployed in accordance with all applicable P2PE requirements (Domains 1, 2, 3, 6 and applicable Annexes)*
- *Option 2: If there is insufficient evidence to support Option 1, deployed POI devices must be reset and all firmware, cryptographic keys, configurations and software must be reloaded in accordance with P2PE requirements. Cryptographic keys may be loaded either by remote key distribution (Annex A) or by returning the POI to a KIF (Annex B).*

Additional Guidance for Option 1:

The P2PE assessor would verify that all currently-deployed POIs were implemented according to P2PE requirements. The P2PE assessor would rely on documented evidence (e.g. records of key loading activities, device configuration records, pre-installation test results, chain of custody records, etc.) and interviews with appropriate personnel. The P2PE assessor would not observe POIs already deployed to merchant environments.

Documented evidence must exist for every deployed POI (sampling is not permitted). Option 2 must be followed for all deployed POIs where sufficient evidence is not available.

Additional Guidance for Option 2:

The P2PE assessor would verify that all currently-deployed POIs are reset and that all firmware, cryptographic keys, configurations and software are reloaded. The P2PE assessor would observe processes for bringing deployed devices into compliance (sampling may be used), and would verify that the processes:

- *Cover all deployed devices*
- *Address all applicable P2PE requirements*
- *Result in devices being brought into compliance*
- *Are complete*

Deployed devices must be updated to the identical application and device configuration that was verified by the P2PE assessor during lab testing (per Domain 2).

Applicable P2PE requirements will depend on whether the devices are updated remotely or are returned to the solution provider, for example:

- *If POI devices are returned to the solution provider for reloading, applicable P2PE requirements include ensuring the secure return of devices to the solution provider (Domains 1, 3), device integrity checks and secure key-loading (Domains 1, 6, and Annex B), secure installation/ configuration of applications (Domain 2), and secure deployment of devices (Domains 1, 3).*

- *If POI devices are reloaded remotely, the applicable P2PE requirements will include device integrity checks and secure remote key-loading (Domains 1, 6 and Annex A), and secure remote access and installation/configuration of applications (Domains 2, 3).*

Where devices are being reset and reloaded remotely, the process for device integrity checks prior to key loading may be performed by the merchant (as instructed by solution provider by phone, via PIM, etc.). Device integrity checks and verification of device serial numbers (per Domain 3) must take place before any remote key-loading is initiated.

In both Option 1 and Option 2, the PIM must have been distributed to all merchants using the deployed devices.

1A.1.1.1 SRED capabilities must be enabled and active

Q 2 July 2014 – Must SRED devices leave the deployment facility in an already-encrypting state? Can a solution provider use a tool or method to monitor and alert if any unencrypted transactions are received, in lieu of always enabling SRED prior to a device leaving the deployment facility?

A *If the device meets requirements specified in the* PTS POI Technical Frequently Asked Questions v3.0 *for requirement K4, including – "Can a POI device approved for SRED have a default configuration to not encrypt account data?" it will be allowable for solution providers to confirm that all encryption functions are fully operational before receiving any transactions from a merchant, using the processes already required at 5D-2.1. This PTS POI FAQ is fully applicable for SRED devices used in P2PE solutions and says in part:*

> For devices that allow the enablement (turning on) or the disablement (turning off) of SRED functionality, the enablement must result in the firmware revision number changing and the device providing visual indication of SRED enablement. Disablement must result in the firmware revision number reverting and the device no longer providing visual indication of SRED enablement. The visual indication must not be transient. This must be documented in information provided by the vendor to the entities deploying these devices.

If SRED capabilities are not enabled and active when devices are deployed to merchants, the P2PE assessor should confirm that:

a) The solution provider has processes in place to detect and immediately resolve any unencrypted transactions they receive (Requirement 5D-2.1), and

b) The device firmware number changes between SRED being enabled and disabled, and the device provides a non-transient visual indication when SRED is enabled.

The P2PE assessor should document these results in the P-ROV and refer to this FAQ.

References:

1A.1.1.1 SRED capabilities must be enabled and active.

5D-2.1 Implement controls to detect encryption failures and provide immediate notification.

Domain 2 – Application Security

2A-1.2 Secure Deletion of PAN and SAD in Applications

Q 1 **July 2014 – Is it expected that applications on a hardened P2PE device be assessed according to Domain 2 requirements (for example, 2A-1.2.c) 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 an application vendor assessment is given sufficient access to both the device and application 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 application's* Implementation Guide, *run test transactions through the device, and then confirm that the installed configuration meets requirements (in the case of 2A-1.2.c, that any PAN or SAD stored by the application during processing is securely deleted).*

Reference:

2A-1.2.c Use forensics tools and/or methods (commercial tools, scripts, etc.) to examine all output created by the application and verify that, by following the Implementation Guide *instructions, the methodology or process provided by the application vendor renders all PAN and SAD data irrecoverable.*

2A-2.1 Applicability of SRED Encryption

Q 2 **July 2014 – Does this requirement mean that PIN data (which is an element of SAD) must be encrypted by the SRED functions of the PCI-approved POI device? How does this impact PIN security requirements for PTS devices processing PINs?**

A *The definition of "account data" is aligned across the various PCI standards, and does include any elements of SAD that are present. With respect to P2PE requirements and PIN security requirements (which must be met by PTS devices processing PINs), SRED covers account data (with the exception of PIN) and does not interfere with any PIN functions. PINs are encrypted separately from other SAD elements using a key specific and unique to PIN encryption. Note that if the PIN is encrypted a second time as part of the encipherment of other SAD elements (for example, via SRED), this secondary encryption is neither required by P2PE nor is it a violation of PIN Security Requirements. Refer to the note (referenced below) on page 3 of the P2PE standard.*

References:

2A-2.1.a …the application only exports PAN or SAD that has been encrypted by the approved SRED functions of the PCI-approved POI device.

Page 3, "Relationship between P2PE and other PCI standards (PCI DSS, PA-DSS, PTS, and PIN":

Please note that the PCI PIN Security Requirements specify an independent set of requirements for PINs, and that this P2PE standard does not supersede or replace any requirements in the PCI PIN Security Requirements.

Q 3 **July 2014 – Is there an exception to the requirement that the application can only export PAN or SAD encrypted by the firmware of the PCI-approved POI device for those areas where there is a legal or regulatory obligation to print the full PAN on merchant receipts?**

A *See 3B-3.1, "Merchant cannot view full PAN," in Domain 3 below.*

Reference:

2A-2.1 The application only exports PAN or SAD data that has been encrypted by the firmware of the PCI-approved POI device, and does not export clear-text PAN or SAD outside of the device.

2A-3 Applications with no access to account data

Q 4 **July 2014 – Can a P2PE PCI-approved POI device have a "separation layer" that is assessed once in a P2PE assessment and thereafter relied upon to provide sufficient separation that applications on the device with no access to cardholder data can be excluded from review?**

A *PCI SSC believes there may be security risks that won't be addressed if these applications are excluded from further assessment and maintenance requirements. In general, the only requirement that applies to applications that never have access to account data is 2A-3 with three sub-requirements. 2A-3 requires that applications with no access to account data 1) only communicate with SRED firmware via APIs that provide no access to account data, 2) are authenticated with an approved security protocol of the POI, and 3) that dual-control is required for the application signing process. It is unclear how an assessor could demonstrate that an application has no access to account data without confirming that the application meets these requirements. Additionally, while it is understood that these applications may be frequently updated and thus require management and maintenance to remain valid for use in a P2PE solution, the fact remains that security risks can be introduced by changes to any application on a device, and it is necessary to confirm that any changes result in the application still meeting Requirement 2A-3.*

That being said, PCI SSC understands that there may be market needs for more flexibility for P2PE solutions regarding applications on devices, and is considering other options for the future including the feasibility of a separation layer and what testing procedures may be required to adequately prove that separation.

Reference:

2A-3 All applications without a business need do not have access to account data.

Domain 3 – Encryption Environment

3A-2.4 Guidance for merchants to transmit POI devices securely

Q 1 **July 2014 – What are secure methods for a merchant to transport a terminal to meet requirements specified in the *P2PE Instruction Manual*, for example, if a merchant has to return a POI device to their vendor for repair?**

A *This requirement is under revision for P2PE v2.0. The intent is that 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 device was shipped. In the interim, the P2PE assessor should document these results in the P-ROV and refer to this FAQ.*

Reference:

3A-2.4 Physically secure POI devices in transit, including:

- *Packing devices in tamper-evident packaging prior to transit.*
- *Implementing procedures for determining whether device packaging has been tampered with.*
- *Use of a defined secure transport method, such as bonded carrier or secure courier.*

3A-4.2 Physically secure POI devices

Q 2 **July 2014 – Are POI devices required to be physically secured (e.g. bolted to a counter-top or tethered with a cable) in the merchant environment? How does this requirement apply to handheld/wireless POI devices?**

A *The intent of this requirement is for the solution provider to provide instructions in the PIM about how to physically secure the POI device – for example, if the device has a cable connection or a fixed bracket, the PIM should describe how to use these features. The merchant should be able to use these instructions to secure devices as appropriate for their environment. Whether the merchant applies the physical security instructions will depend on the type of environment the device is being used in, and does not impact the P2PE solution assessment.*

If a POI device is not intended to be secured in one place – for example, it is a handheld or wireless device – the solution provider is expected to provide merchants with instructions for how to implement process controls to protect the device. Examples of process controls could include storing the device in an area inaccessible to the public when the device is not in use, assigning responsibility to specific personnel for supervising use of the device, and so on. Again, the solution provider's responsibility is to provide this information in the PIM so the merchant is aware of best practices. The actual methods implemented by merchants to secure POI devices may vary according to the needs of the particular merchant.

Reference:

3A-4.2 Provide instructions via the P2PE Instruction Manual for the merchant to physically secure deployed devices to prevent unauthorized removal or substitution, including examples of how devices can be physically secured.

3A-4.2.1 Provide instructions via the P2PE Instruction Manual for the merchant to implement procedures to prevent unauthorized removal or substitution of devices that cannot be physically secured (such as wireless or handheld devices).

For example, secure devices in a locked room when not in use, assign responsibility to specific individuals when in use, observe devices at all times, sign devices in/out, etc.

3B-1 Solution provider securely maintains devices

Q 3 July 2014 – Are solution providers required to maintain the physical security of devices throughout their lifecycle regardless of where the devices are located?

A *Solution providers and their agents are required to maintain strict control of the devices while in their possession (for example, prior to deployment, during replacement, or prior to device destruction). Once a merchant receives a device, it is thereafter the merchant's responsibility to manage the physical security of that device (as defined in the PIM) unless they ship it back to the solution provider or a solution provider's agent, or unless arrangements have been made between the solution provider and merchant for the ongoing management of the devices on the merchant's behalf.*

Reference:

3B-1 The solution provider securely maintains devices being returned, replaced, or disposed of, and provides related instructions to merchants.

3B-3.1 Merchant cannot view full PAN

Q 4 July 2014 – Is there an exception to the requirement that a merchant cannot view full PAN for those areas where there is a legal or regulatory obligation to print the full PAN on merchant receipts?

A *First, to clarify, it is not the intention for PCI SSC's standards to supersede local or regional laws, government regulations, or other legal requirements. Our answer provides an exception ONLY where there is a legal or regulatory obligation in place to print the full PAN on merchant receipts. Where such a legal or regulatory obligation exists, P2PE requirements may still be met as follows (note that this exception applies only to PAN and never applies to SAD):*

- *SRED passes the clear-text PAN to an application that transmits the PAN internally within the device for printing. Since this application sees clear-text PAN, it must be assessed to Domain 2 and listed on the PCI SSC website.*
- *The application can only transmit clear-text PAN to an integrated printer—this printer is part of the PCI-approved POI device itself and is not attached via cabling or other networking mechanisms. This application cannot transmit PAN to any other device, process, or system.*
- *After completion of printing, the application securely deletes the clear-text PAN, and the device completes the SRED encryption of the account data for transmission to the processor.*
- *The merchant needs to protect paper receipts in accordance with PCI DSS Requirements 9.5-9.8.*
- *Merchants are allowed to view PANs printed on receipts in these markets.*

The P2PE assessor should document these results in the P-ROV and refer to this FAQ.

Reference:

3B-3.1 The solution provider ensures merchant has no administrative access to the device and cannot change anything on the device that could impact the security settings of the device. Merchant access if needed, must meet the following:

- *…Cannot view or access full PAN.*

3B-5 Solution provider protects POI devices from known vulnerabilities

Q 5 July 2014 – Is it the responsibility of the solution provider to "push" patches to all affected POI devices, or is it sufficient for them to merely make it available for download and advise the merchant how to download and install the patches?

A *In a P2PE solution, the solution provider is responsible for managing the application, including the deployment of application updates. Solution providers should work with their merchants to schedule updates at appropriate times—for example, the solution provider could make the patch available, provide instructions for the merchant on how to trigger the update process, and notify merchants that the patch needs to be installed within a defined period of time. If the patch is not installed during this required timeframe, the provider may need to follow-up with merchant to ensure the application is updated. Alternatively, the solution provider may push the patch to devices at a time that is pre-agreed with the merchant. Whatever process the solution provider uses to manage the update process, they are ultimately responsible for ensuring that P2PE applications are kept up-to-date with required patches and security updates.*

Reference:

3B-5 and 3B-5.3 The solution provider protects POI devices from known vulnerabilities and implements procedures for secure updates to devices [including]: Develop and deploy patches and other device updates in a timely manner.

Domain 4 – Segmentation between Encryption and Decryption Environments

No FAQs in this section – Reserved for future use.

Domain 5 – Decryption Environment and Device Management

No FAQs in this section – Reserved for future use.

Domain 6 – P2PE Cryptographic Key Operations

6E-4 All secret and private keys must be unique (except by chance) to that device.

Q 1 **July 2014 – Testing procedures 6E-4.1.c & d specify unique POI keys – does this mean that unique public encryption keys must exist for each POI?** *The intent of this requirement is that all secret and private cryptographic keys used in transaction-originating POI devices for any function directly or indirectly related to account data protection are unique per POI device. The intent is not that each individual POI must have its own public encryption keys, but that where a POI does have its own public/private key pairs (for example, for authentication or key conveyance), the private key(s) owned by the POI and its associated public key(s) must be unique per POI. Therefore, the focus of the test at 6E-4.1.c & d are, IF POIs have their own public/private key pairs, to confirm that each individual POI has a unique public key(s), and thereby confirm the uniqueness of each POI's private key(s).*

Reference:

6E-4.1.d Compare all POI public keys, if used, across all decryption points as well as for every POI connection, to ensure there are no duplicates across POI devices.

Appendix A – Minimum Key Sizes and Equivalent Key Strengths

Q 2 **No FAQs in this section – Reserved for future use.**