Security Standards Council™

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

Frequently Asked Questions for PCI Point-to-Point Encryption (P2PE)

August 2012

Frequently Asked Questions (FAQs)
For PCI Point-to-Point Encryption (P2PE)

Purpose

The Council has released the first phase of the PCI Point-to-Point Encryption (P2PE) program, including version 1.1 of the *PCI P2PE Solution Requirements and Testing Procedures* (P2PE Standard) for hardware-based P2PE solutions. This document has been compiled to address frequently asked questions around this topic.

Please refer to the P2PE Standard and P2PE Program Guide for further information.

August 2012: General FAQs

Q 1 What is a point-to-point encryption (P2PE) solution?

A. *A point-to-point encryption (P2PE) solution is provided by a third party solution provider, and is a combination of secure devices, applications and processes that encrypt data from the point of interaction (for example, at the point of swipe or dip) until the data reaches the solution provider's secure decryption environment.*

A PCI P2PE solution must include all of the following:

- *Secure encryption of payment card data at the point-of-interaction (POI)*
- *P2PE-validated application(s) at the point-of-interaction*
- *Secure management of encryption and decryption devices*
- *Management of the decryption environment and all decrypted account data*
- *Use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading/injection, administration and usage.*

Q 2 What is a P2PE solution provider?

A. *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 manages P2PE solutions for its merchant customers.*

The solution provider has overall responsibility for ensuring that all P2PE requirements are met, including any P2PE requirements performed by third-party organizations on behalf of the solution provider (for example, certification authorities and key-injection facilities).

Q 3 What is the Point-to-Point Encryption (P2PE) Standard?

A. *The PCI Point-to-Point Encryption (P2PE) Standard contains detailed security requirements and testing procedures for application vendors and providers of P2PE solutions to ensure that their solutions can meet the necessary requirements for the protection of payment card data.*

Version 1.1 of the P2PE Standard contains security requirements and testing procedures for third-party, hardware-based P2PE solutions. Subsequent releases of the P2PE program will address requirements for securing software-based decryption and key management operations, as well as scenarios where merchants manage their own cryptographic keys.

P2PE assessors [QSA (P2PE)s and PA-QSA (P2PE)s] are qualified by the Council to evaluate P2PE solutions and applications.

Q 4 Are merchants using Council-listed P2PE solutions out of scope for PCI DSS?

A. *No. While use of a validated, listed P2PE solution can help to reduce the scope of a merchant's cardholder data environment, it does not remove the need for PCI DSS in the merchant environment. The merchant environment remains in scope for PCI DSS because cardholder data is always present within the merchant environment. For example, in a card-present environment, merchants have physical access to the payment cards in order to complete a transaction, and may also have paper reports or receipts with cardholder data. As another example, in card-not-present environments (such as mail-order or telephone-order), payment card details are provided via other channels that need to be evaluated and protected according to PCI DSS.*

Only Council-listed P2PE solutions are recognized as meeting the requirements necessary for merchants to reduce the scope of their cardholder data environment through use of a P2PE solution. Merchants using encryption solutions that are not included on the Council's List of Validated P2PE Solutions should consult with their acquirer or payment brand about use of these solutions.

Q 5 Is a "P2PE Assessor" required for a merchant's PCI DSS assessment if the merchant uses a Council-listed P2PE solution?

A. *No, merchants using P2PE solutions are not required to engage a P2PE assessor [that is, a QSA (P2PE) or PA-QSA (P2PE)] for their PCI DSS assessments.*

Merchants using Council-listed P2PE solutions will continue to validate their PCI DSS compliance as determined by the payment brand compliance programs. For example, a merchant may need to engage a QSA to perform an onsite assessment, or they may be eligible to complete a self-assessment questionnaire (SAQ). Merchants should contact their acquirer (merchant bank) or payment brand directly to understand their validation requirements. Merchants wishing to engage a QSA for their PCI DSS review can find a list of QSAs on the Council website - https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

Q 6 Can merchants use P2PE solutions not listed on the Council's website for PCI DSS scope reduction?

A. *Only Council-listed solutions are recognized as meeting the requirements necessary for merchants to reduce the scope of their cardholder data environment (CDE) through use of a P2PE solution. In addition to using a validated, Council-listed P2PE solution, merchants wishing to reduce the scope of their CDE must meet certain characteristics, as documented in the "Merchants Using P2PE Solutions" section of the P2PE Standard. SAQ-eligible merchants can review the P2PE-HW SAQ on our website for eligibility criteria and applicable PCI DSS requirements.*

Merchants using encryption solutions that are not included on PCI SSC's list of Validated P2PE Solutions should consult with their acquirer or the payment brands about the use of these solutions.

Q 7 Is the P2PE Standard applicable for merchants that have developed/implemented their own P2PE solution?

A. *Version 1.1 of the P2PE Standard applies only to third party P2PE solutions, where all encryption and decryption operations, and all cryptographic keys, are managed by a third party solution provider, and the merchant has no access to cleartext account data or to the P2PE cryptographic keys.*

Future phases of P2PE will address scenarios where merchants manage their own cryptographic keys. In the interim, merchants who manage their own cryptographic keys and/or encryption solution should consult with their acquirer or the payment brands about the use of these solutions.

Q 8 Are P2PE solution providers required to have their solutions validated and listed by the Council?

A. *Only Council-listed P2PE solutions are recognized as having met the rigorous controls defined in the PCI P2PE Standard for the protection of payment card data, as well as meeting the requirements necessary for merchants to reduce the scope of their cardholder data environment (CDE) through use of a P2PE solution.*

For solutions that are not yet validated, a qualified P2PE assessor can assess the solution against the P2PE Standard and provide the outcome of the assessment to the solution provider. The solution provider can then use this information as a gap analysis to help them to prepare their solution to meet all the P2PE requirements in order to become a validated and listed P2PE solution.

Q 9 Which PCI PTS point-of-interaction (POI) devices can be used in a validated P2PE solution?

A. *A Council-listed P2PE solution must use a PCI-approved point-of-interaction device (POI), which has been evaluated and approved via the PCI PTS program with SRED (secure reading and exchange of data) listed as a "function provided" and with SRED enabled and active. PCI PTS v3.0 is the first version of the PTS Standard to include SRED. Devices assessed to PCI PTS 3.0 with SRED are eligible for use in a P2PE solution.*

For PCI PED 2.0 devices, the PCI SSC announced at the 2011 Community Meeting that PCI PTS 2.0 devices can be submitted to PCI PTS testing laboratories for SRED approval. In support of the P2PE initiative, previously approved v2.0 devices have a twelve month window starting 1 January 2012 to undergo a delta evaluation against the SRED module, and if applicable, the Open Protocols module. As a delta evaluation, the v2.0 approved device may leverage requirements that it previously met in v2.0 where those requirements parallel SRED requirements. For example, the devices may utilize algorithms and key sizes allowed in v2.0 in lieu of those specified in SRED requirements. Similarly, v2.0 devices may utilize v2.0 attack potential calculations for SRED requirements previously addressed under v2.0.

PTS v2.0 devices "upgraded" using encrypting card readers must meet not only SRED, but the applicable card reader requirements in the Core section (the same as is done for approving card readers under PTS POI v3.1). The expiration of v2.0 devices' approval will remain as April 2017.

A summary of the PTS versions and applicability is provided below:

PTS version	***Eligible for SRED approval?***	***Can be used in P2PE solutions?***	***Expiry date of PTS approval***
3.x	Yes	Yes, if approved with SRED	April 2020
2.x	Yes, through delta evaluation of SRED, and any other applicable modules, before December 31, 2012	Yes, for devices that have been approved with SRED and any other applicable PTS modules	April 2017
1.x	No	No	April 2014

Q 10 Can PCI PED 1.x devices receive SRED validation and be used in a P2PE solution?

A. *No, PCI PED 1.x devices are not eligible for SRED validation, and therefore cannot be used in a PCI P2PE solution.*