Security Standards Council®

Version: 1.1

Date: June 2020

Author: PCI Security Standards Council

Information Supplement:

Assessment Guidance for Non-Listed Encryption Solutions

Document Changes

Date	Document Version	Description	Pages
November 2016	1.0	Initial release	All
June 2020	1.1	Update references based on P2PE v3.0	Various

Table of Contents

1 Introduction

1.1 Purpose of this Document

Assessment Guidance for Non-Listed Encryption Solutions is intended to provide **guidance** with regard to merchants using PCI-approved PTS POI device-based account-data encryption solutions that are not listed on the PCI Security Standards Council website[1]. Non-listed encryption solutions, within the context of this document, are account-data encryption solutions that have not been validated[2] per the PCI P2PE Program Guide.

While the adoption of PCI-validated P2PE solutions is strongly encouraged, the PCI SSC understands that there are merchants currently using non-listed encryption solutions, and that these account-data encryption implementations are often an aspect of a Qualified Security Assessor's (QSA's) PCI DSS assessment of the merchant's environment. This guidance is provided based on the expectation that these non-listed encryption solutions will remediate any identified gaps and eventually be assessed by a P2PE QSA per the PCI P2PE Program Guide with the intent of becoming a PCI-validated P2PE solution.

1.2 Scoping Criteria

This guidance is intended solely for consideration of a merchant's encryption environment (as defined in the PCI P2PE standard and associated documents) and its use of a solution provider's existing non-listed encryption solution. This guidance is based on the following:

- The merchant is using PCI-listed PTS POI v2 (or higher) devices for the acceptance and encryption of payment brand account data.
- The merchant never has access to account data decryption (secret and/or private) keys.
- The merchant never has access to clear-text account data transmitted outside of the device.

This guidance is not intended to address encryption solutions using:

- PCI PTS v1 (or previous) POI devices
- Encryption of account data outside of a PTS-approved POI v2 (or higher) device
- Any other form of payment acceptance device

The non-listed encryption solution may not meet requirements in Domains 1, 2, or 3 of the latest P2PE Standard; however, the solution is expected to meet all the applicable requirements in Domains 4 and 5.

1.3 Intended Audience

This document is intended for use by acquirers, PCI Qualified Security Assessors (QSAs), P2PE QSAs, solution providers of existing non-listed encryption solutions, as well as merchants using non-listed encryption solutions.

1 Excluding merchant-managed solutions as defined by the PCI P2PE Program.
2 Reference the PCI P2PE Program Guide for the definition and meaning of "validated."

1.4 Intended Usage

This document and the NESA (Non-listed Encryption Solution Assessment) documentation support a consistent approach for evaluating non-listed encryption solutions. This guidance includes the following recommendations for the stakeholders shown below:

- **Acquirers:** Should use the NESA documentation created by a P2PE QSA for their merchant base requiring a PCI DSS assessment that includes the use of a solution provider's non-listed encryption solution. The NESA documentation can be used to provide insight in evaluating risk and determining the appropriate PCI DSS validation effort for these merchants.
- **Solution Providers:** Should engage a P2PE QSA to facilitate an analysis of their non-listed encryption solution in use by their merchant customers. This guidance document provides insight into what can be expected from the involvement of a P2PE QSA.
- **P2PE QSAs:** Should assess a solution provider's non-listed encryption solution and create the NESA documentation. Note that it is not the intent that a P2PE QSA, as part of creating the NESA documentation, assess merchant environments with regard to PCI DSS.
- **QSAs[3]:** Should use the NESA documentation created by a P2PE QSA for merchant customers requiring a PCI DSS assessment that includes the use of a solution provider's non-listed encryption solution.
- **Merchants:** May benefit from this guidance by gaining insight into the various expectations from the other stakeholders involved with respect to their use of a non-listed encryption solution and a PCI DSS assessment of their merchant environment.

Note: *P2PE QSAs are additionally qualified by PCI SSC and confirmed to have relevant experience and skills in evaluating encryption implementations. Non-listed encryption solutions evaluated by anyone other than a P2PE QSA are not supported by this guidance.*

1.5 Documentation

The P2PE QSA should populate the P2PE Report on Validation (P-ROV) template as part of their assessment of the solution. The documented P-ROV is used as an input to create the NESA documentation[4].

The NESA documentation is created by a P2PE QSA as part of their assessment of a solution provider's non-listed encryption solution and is ultimately intended to be provided to the merchant or its assessor by the solution provider. The populated P-ROV can also serve as a gap analysis for the solution provider should they pursue a PCI-listed P2PE Solution (contingent on following the PCI P2PE Program Guide). The NESA documentation consists of:

- A description of the non-listed encryption solution
- A summary for P2PE Domains 1, 2, and 3 indicating the solution's non-compliance, partial compliance, or full compliance with each domain
- A statement of compliance indicating the "Scoping Criteria" detailed in this guidance and Domains 4

[3] Or other eligible entity as determined by the acquirer or payment brand(s).
[4] The documented P-ROV and/or the NESA documentation are not submitted to PCI SSC or to the Payment Brands.

and 5 of the PCI P2PE v3.x standard are met

- The P2PE QSAs recommendation as to how the solution potentially affects a merchant's PCI DSS assessment

Providers of non-listed encryption solutions should perform an annual self-assessment of their solution. The self-assessment confirms that the solution has not changed; and the solution provider should attest to zero changes in its current NESA documentation.

If changes to the solution have occurred, a P2PE QSA should assess the changes and determine the necessity to reassess the solution, including creating a new P-ROV and/or NESA documentation.

Providers of non-listed encryption solutions with NESA documentation should have their solutions undergo a full assessment at least every three years by a P2PE QSA.

1.6 Process Flow

The following diagram depicts the general process flow for the entities mentioned in Section 1.4 above:

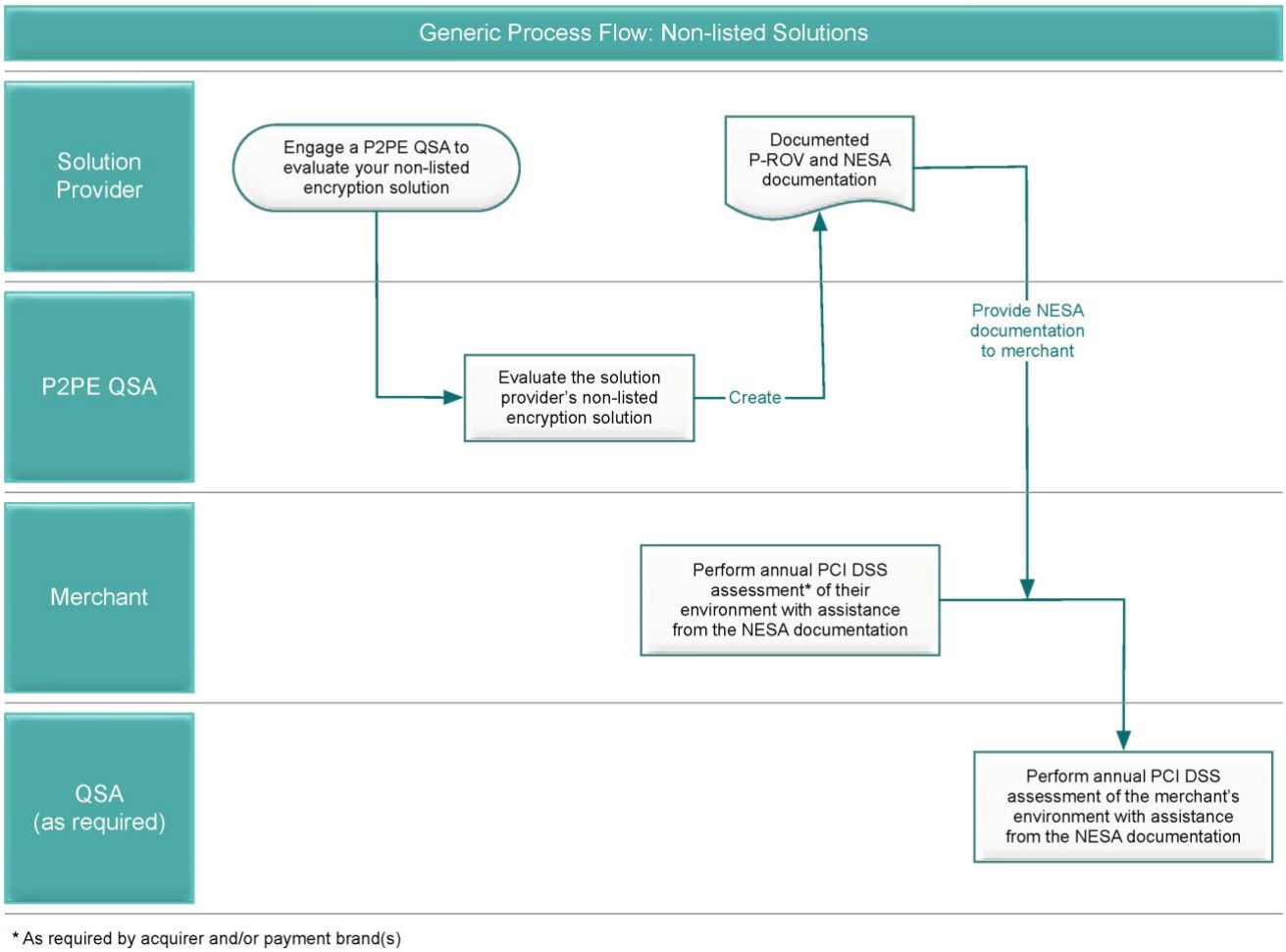

Figure 1: *Process Flow*

Reference the PCI P2PE v3.x standard, program guide, and glossary located here on the PCI SSC website.

2 About Listed and Non-Listed Encryption Solutions

The use of encryption is an effective method to protect account data. All entities are strongly encouraged to use PCI-validated[5] P2PE solutions. PCI-validated P2PE solutions are assessed by a P2PE QSA per the P2PE Program Guide. Merchants using these PCI-validated encryption solutions can effectively decrease their PCI DSS validation effort by using the SAQ P2PE[6], thereby simplifying their PCI DSS compliance efforts. Currently listed PCI P2PE Solutions can be found here on the PCI Council's website.

PCI-validated P2PE solutions focus on protecting account data by encrypting it at the point of interaction (POI) where the account data is captured within the merchant's environment and transmitted to the solution provider's secure decryption environment where the data is decrypted, effectively removing clear-text account data between the encryption and decryption points.

The P2PE standard requires PCI-listed PTS POI devices using SRED (secure reading and exchange of data). In addition to the physical and logical protections SRED provides for account data inside the device, SRED is also required to encrypt account data prior to transmission outside the protected SRED boundary. The list of Approved PTS POI devices (including their SRED approval status) can be found here on the PCI Council's website.

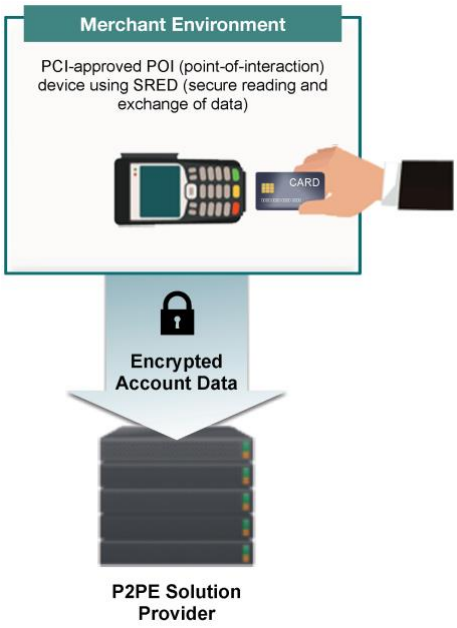

Figure 2: *PCI PTS POI Device using SRED*

The P2PE Standard provides flexibility and increased options for merchants and solution providers—in addition to companies that provide components for integration within P2PE solutions, referred to as P2PE Component Providers. The list of PCI component providers makes it easy for a solution provider to integrate these validated components into its encryption solution. The same flexibility applies to merchants who are acting as their own solution provider in a merchant-managed solution. The PCI P2PE v3.x materials can be found here in the document library on the PCI Council's website.

5 Both (and only) PCI-listed P2PE solutions and merchant-managed solutions are considered PCI-validated encryption solutions within the context of this document. Note that PCI-validated merchant-managed solutions (MMS) are not currently listed by the PCI Council.

6 SAQ P2PE is intended for SAQ-eligible merchants (as determined by the individual payment card brands), who process cardholder data only via approved payment terminals as part of a Council-listed P2PE solution or merchant-managed solution. Merchants wishing to use SAQ P2PE must meet payment brand requirements for using an SAQ. Please see FAQs 1247 and 1331 for greater detail regarding the use of SAQ P2PE and SAQs in general, respectively.

Figure 3 below is a conceptual illustration depicting how merchants using a PCI-validated encryption solution benefit from the greatest reduction in PCI DSS validation. For merchants using a non-listed encryption solution, the merchant's PCI DSS validation effort increases accordingly, as fewer PCI P2PE requirements are met.

Note: *The use of PCI-listed or merchant-managed solutions does not completely remove PCI DSS applicability. The merchant environment remains in scope for PCI DSS because account data is always present within the merchant environment. Further details can be found in FAQ 1158.*

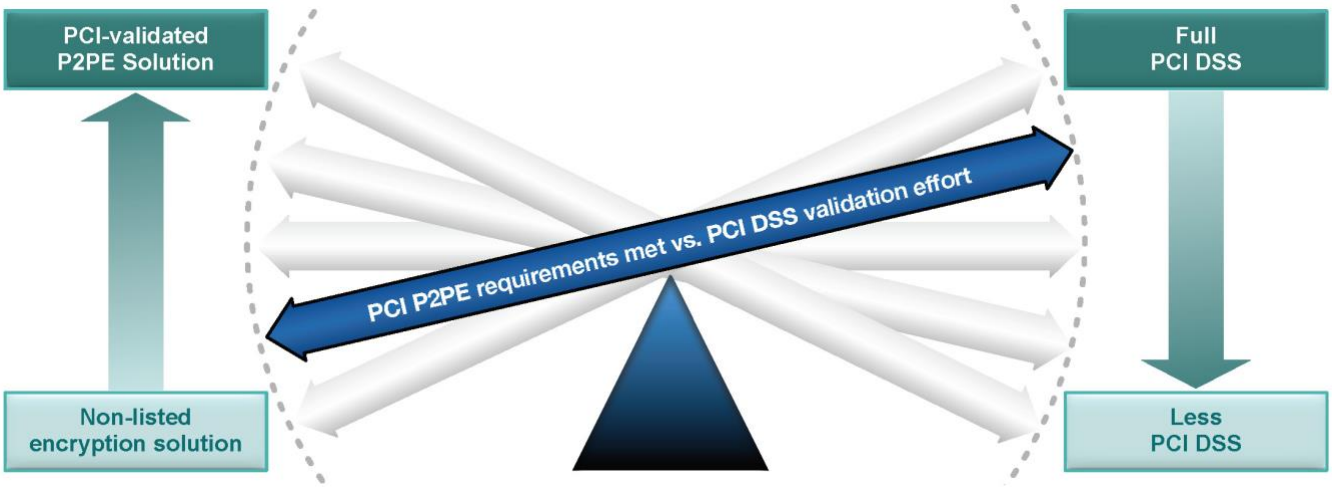

Figure 3: *Illustrative example of PCI P2PE requirements met vs. PCI DSS validation effort*

3 Guidance for Solution Providers

Solution providers should engage a P2PE QSA to facilitate an analysis of their non-listed encryption solution in use by their merchant customers. This guidance document provides insight into what can be expected from the involvement of a P2PE QSA. In addition, a solution provider should provide their merchant customers with their NESA documentation:

- As soon as it is completed by a P2PE QSA
- After any significant changes that require the NESA documentation to be updated
- At least annually to support merchants' PCI DSS assessments

4 Guidance for Merchants

Merchants using non-listed encryption solutions should work closely with their acquirer and/or payment brands in determining their PCI DSS compliance obligations. What, if any, PCI DSS validation reduction is permitted through the use of a non-listed encryption solution is determined by the merchant's acquirer and payment brands and may depend on the extent that the solution has been assessed by a P2PE QSA as well as the current NESA documentation. Merchants should request NESA documentation from their non-listed encryption solution provider upon installation and on an annual basis thereafter. The solution provider should also provide the merchant updated NESA documentation after any significant changes that could impact the intended security of the solution.

5 Guidance for QSAs

This guidance aims to reduce the burden on QSAs from assessing non-listed encryption solutions as well as provide P2PE QSAs with an approach to perform this analysis. In addition, the NESA documentation created by the P2PE QSA should facilitate QSAs making informed decisions for merchant environments using an associated non-listed encryption solution.

QSAs performing a PCI DSS assessment of a merchant using a non-listed encryption solution should review the NESA documentation prepared by a P2PE QSA in accordance with this guidance. The purpose is to:

- Understand and verify the documented components of the non-listed encryption solution are implemented in the merchant's environment
- Be used as input to help determine the scope and the applicable PCI DSS requirements of the merchant's environment based, in part, on the NESA documentation

  NOTE: The QSA should not solely rely on the NESA documentation to determine the appropriate scoping of the merchant's environment. The QSA should confirm the "Scoping Criteria" in this guidance document is being met, as well as validate the scope is accurate and appropriate per the PCI DSS. Any reduction in scope should be recorded in the appropriate section in the Reporting Template for use with PCI DSS

The QSA should review the instruction manual associated with the non-listed encryption solution to ensure the merchant has implemented the solution per the instructions and detail in the instruction manual. QSAs

should retain all relevant work papers, including the NESA documentation and the instruction manual, per the PCI QSA Qualification Requirements.

6 Guidance for P2PE QSAs

P2PE QSAs should create both a documented P-ROV and NESA documentation per Section 1.5, "Documentation."

The following sections contain considerations for P2PE Domains 1, 2, and 3—as non-listed encryption solutions may not meet these requirements and therefore may warrant additional analysis, with explanation provided in the P-ROV. However, the solution is expected to meet all the requirements in Domains 4 and 5as detailed in the current PCI P2PE standard.

Note: *This list of considerations for a P2PE QSA analyzing non-listed encryption solutions is not intended to be exhaustive. This guidance is not prescriptive—each solution is unique and warrants an appropriate analysis.*

6.1 PTS POI Device Approval Attributes

First and foremost, the PTS POI devices in use should be checked to ensure their basic attributes match their associated PCI approval on the "Approved PTS Devices" listing located here on the PCI SSC website. The following considerations should be taken into account:

- **Do the model name, hardware number, and firmware number of the POI device type match a PCI PTS listing for an approved PTS POI device?**

  The PCI PTS POI security requirements require these attributes to be made available on the POI device. For example, the model name and hardware number should be printed on an affixed label, while the firmware number is displayed when the device boots up and is potentially accessible via a menu system on the POI device. Note that more than one "firmware" may be present in the POI device—e.g., a core firmware and a SRED-based firmware. All firmware present, along with the other attributes, should be checked and verified.

- **Is the associated PTS listing for the POI device type approved for PTS v2.x or higher?**

  All PTS listings of approved POI devices indicate the major version of the PTS standard the device was evaluated and approved against. Verify the POI device is approved to PTS POI v2.x or higher. Note that a POI device may have multiple PTS listings—for example, if it was approved to more than one major version of the PTS POI standard. Ensure the appropriate PTS POI listing is being reviewed. As a reminder, this guidance is only intended for non-listed encryption solutions using PCI-listed PTS POI v2.x (or higher) devices.

- **What are the "Functions Provided" by the POI device, as well as "Additional Information"?**

  Clicking on the associated PTS "Approval Number" in the applicable Approved PTS Devices listing will provide additional information for that POI device type. Review any such notes to help determine the appropriate use of the POI device. For example, the notes may indicate that certain implementation restrictions apply. In addition, the "Functions Provided" column includes valuable information regarding the "as-approved" use of the POI device for various functions. For example, if the device was

approved for contactless use, the "CTLS" designation will be present. The same applies to other interfaces, such as the Integrated Circuit Card Reader (ICCR) and the Magnetic Stripe Reader (MSR). All interfaces being used on the POI device should have a representative designator on the device's associated PCI listing. Two additional designations, "SRED" and "OP," are equally important. Please see below for additional information.

- **Is "OP" listed as a function provided on the PTS listing?**

  The Open Protocols (OP) designation in the "Functions Provided" on the PTS listing indicates the device was assessed against the PTS POI Open Protocol requirements. The "OP" designator provides a level of assurance regarding the device's ability to securely account for its open protocol implementations. The Open Protocols module is to ensure that open protocols and associated services in POI devices do not have vulnerabilities that can be remotely exploited and yield access to sensitive data or resources in the device.

  The POI device vendor defines the protocols and services supported by the device and provides guidance for their proper use. Adding or enabling additional services and protocols, or failing to follow the POI device vendor's issued security guidance after the PTS evaluation, invalidates the approval status of that device for that implementation.

  If the device is utilizing any open protocols (as defined in the PCI PTS POI standard), the device should have the "OP" designator indicated on its associated PCI listing and those functions should be restricted to the approved firmware in the POI device.

- **Is the POI device approved with SRED functionality?**

  The PCI SSC recommends the use of PCI PTS POI devices approved with SRED, and to use the SRED functions of the device for the protection and encryption of account data. However, in terms of this guidance, the use of SRED is optional.

  - **Checking the PTS Approval listing for SRED**

    The Secure Reading and Exchange of Data (SRED) tag under "Functions Provided" indicates the device was assessed against the PTS POI SRED requirements governing the protection of the PAN (both physically and logically) during its entire existence within the POI device, protecting any associated sensitive data or functions, and encrypting account-data transmissions prior to leaving the secure SRED boundary of the POI device. The SRED designator on the listing provides a level of assurance regarding the device's ability to protect account data. The P2PE QSA's analysis should factor in whether the POI device is using SRED as defined in the PTS POI Standard's security requirements.

  - **Checking for whitelisting**

    It should be noted that while a POI device may have been approved with SRED, the POI device might "whitelist" account data, essentially sending out account data in clear text. In some situations the clear-text account data is only sent from the device's firmware to an internal non-SRED boundary within the POI device (e.g., to an internal POI application). In other scenarios the clear-text data may be sent out of the POI device entirely. In other words, an "SRED" designator on the POI device's PCI listing does not imply that the device never externally

transmits clear-text account data. Therefore, due diligence necessitates determining both the POI device listing attributes as well as the intended POI device configuration and any intended use of whitelists. As a reminder, this guidance is based on the POI device preventing the external (to the device) output of clear-text account data into the merchant's environment, whether it is accomplished via the POI's approved SRED functionality or other internal POI mechanism.

- **If SRED isn't being used, what is?**

  If the SRED-provided encryption functions of the POI device's firmware are not being used to encrypt the account data, the P2PE QSA should determine by what mechanisms inside the POI device the encryption is being performed. Due diligence would suggest this will lead to further analysis, as the assurances provided by using the SRED encryption functions are not available. For example, is the encryption being performed outside the PTS-approved firmware (e.g., application-level encryption or communication protocol-based encryption). If so, try to determine the answers to and the potential impact from the following considerations. Note this list contains suggestions and is not exhaustive:

  - How do the following attributes compare, for example, to the PCI P2PE Standard's Domain 5 Normative Annex C—i.e., is the encryption implementation acceptable per industry standards?
    - Which cryptographic algorithm(s) and, if applicable, mode(s) of operation are being used to encrypt the account data (e.g., TDEA, AES, RSA, ECC, etc.)? Are the algorithms in use considered industry-acceptable?
    - What are the associated cryptographic key lengths available for each algorithm in use? Are they appropriate for the associated algorithm being used?
    - Which key-management schemas are associated to the cryptographic algorithms in use (e.g., DUKPT, MK/SK, fixed, etc.)?
  - How are the relevant cryptographic keys managed within the POI device? For example, is the encryption key simply hard-coded in the application (considered insecure and poor practice); or is it managed in a secure manner, preventing malicious substitution and discovery?
  - Does the merchant have access to the decryption keys (or ability to decrypt the encrypted account data)? If the merchant can easily decrypt the encrypted account data, the overall assurance level of the encryption implementation is drastically reduced. As a reminder, the scoping criteria in this guidance is based on the merchant never having access to account data decryption (secret and/or private) keys.

Review the PTS POI standard and associated documentation on the PCI SSC website. Note that it is critical to understand that the intent of a P2PE QSA's role is not to "re-assess" the PCI PTS evaluation and therefore the existing approval of the POI device's hardware and firmware. PTS-approved firmware is already validated according to the PCI PTS program. This guidance with respect to SRED is first and foremost to understand whether the POI is approved with SRED—and if it is, whether the SRED functions are being used for account-data encryption. If not, the mechanisms providing the

encryption and associated functionality in the POI device in lieu of any SRED functions should be determined and analyzed. The PTS POI materials can be found here in the document library on the PCI Council's website.

Please see the question "Are additional applications present on the device?" in Section 6.2 below regarding additional considerations for applications (non-firmware) present on the POI device.

6.2 Additional POI Device Considerations

Beyond using the PCI listing of Approved PTS Devices, there are also additional considerations regarding the POI device, such as:

- **Are additional applications present on the device?**

  "Firmware" as defined in the PTS standard is "... any code within the device that provides security protections needed to comply with (PTS) device security requirements or can impact compliance to these (PTS) security requirements. Firmware may be further segmented by code necessary to meet the PTS Core, OP (Open Protocols) or SRED (Secure Reading and Exchange of Data). Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware." Note that it is not the intent here to reassess the PTS-approved firmware.

  While it may be possible for a PCI POI device to implement all its necessary functionality solely within its existing PTS-approved firmware, generally the POI device will contain additional software (e.g., payment applications). Any software that does not meet the PTS definition of firmware is not reviewed as part of the device's PTS assessment or included in the PTS approval. Evaluating non-listed encryption solutions should include identifying any (non-firmware) software on the POI device.

  Understanding the purpose and overall function of additional applications should be considered. For example, is the application performing its own encryption of account data? Clear-text account data within the POI device should not be disclosed to any component or device outside of the POI device. Reference the question "Is the POI device approved with SRED functionality?" in Section 6.1 above for further considerations regarding account-data encryption.

  Other key considerations for applications present on the POI are:

  - Are applications required to be cryptographically signed and therefore cryptographically authenticated by the POI device?
    - If yes, is there a process in place to provide this assurance?
    - If not, what controls, if any, protect the device from the addition of unauthorized software?
  - Is installation and secure configuration guidance available from the software vendor? Are processes in place to help facilitate the secure installation and configuration of the software on the POI device?
  - Is account data being properly handled by the application software? For example, consider storage, printing, truncation, deletion, etc.
  - Does the application use any whitelisting functionality relative to payment card data?
    - Is the whitelist cryptographically authenticated?
    - Is there a process in place that provides assurance that clear-text account data isn't being

transmitted outside the POI device?

- Has the application on the POI device been previously approved and/or assessed to PCI PA-DSS or the Secure Software Standard? Is there an existing PCI SSC approval? Is there additional related documentation that can be obtained and reviewed with regard to the configuration?

Application software can significantly impact the overall security of the POI device. P2PE QSAs should evaluate the software as diligently as possible with respect to the security of account data.

- **Will merchant-level personnel have logical access to the POI devices?**

  The ability, or lack thereof, of merchant personnel to logically access the POI device should be considered. If merchant personnel have logical access to the device, what functionality is available to them and are there any security ramifications of such access? For example, can the merchant:

  - Alter the device configuration in a way that would impact the security characteristics of the device?
  - Enable any disabled interfaces on the POI device?
  - Access the POI devices remotely?

  Merchants may have logical access to the POI device. However, it should be assessed that the access available does not grant the ability to impact (either directly or indirectly) the security of account data. As a reminder, this guidance does not apply if merchants have access to clear-text account data or to associated encryption/decryption keys.

- **How are the POI devices managed?**

  Consideration should be given to the overall management of the POI devices. For example, are policies and procedures in place that govern the following:

  - Firmware and/or application updates (or new installations)
  - Security-relevant updates (patching)
  - POI device configuration (e.g., vendor instruction manual)
  - Application configurations
  - Whitelisting
  - Inventory of POI devices
  - Installation with respect to physical security of the POI devices

  The intent is to determine that sufficient assurance exists with regard to properly managing the POI devices in order to preserve the security aspects governing account data.

6.3 Instruction Manual

The provider of the non-listed encryption solution should have an instruction manual for its merchant customers. The P2PE QSA should determine the existence and availability of an instruction manual, as well as the adequacy of the information provided. For example, the P2PE “PIM” template can be used as a reference to determine useful information for the merchant.

7 Conclusion

The use of encryption is an effective method to protect account data. All entities are strongly encouraged to use PCI-validated P2PE solutions to help merchants benefit from the greatest reduction in their PCI DSS validation efforts.

In the event an existing solution cannot meet the current PCI P2PE standard, this document can be used as guidance to help evaluate non-listed encryption solutions and their impact on PCI DSS assessments of respective merchant environments.

8 About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Created in 2006 by the founding payment card brands American Express, Discover Financial Services, JCB International, Mastercard, and Visa Inc., the Council has more than 650 Participating Organizations representing merchants, banks, processors, and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.