Payment Card Industry (PCI)

Point-to-Point Encryption

Program Guide

Version 1.0

June 2012

Document Changes

Date	Version	Description
June 2012	1.0	Initial Release of the *PCI P2PE Program Guide*

.

Table of Contents

1 Introduction

1.1 Related Publications

The following documents are the basis for the assessment of point-to-point encryption solutions and implementations:

- *Payment Card Industry (PCI) Point-to-Point Encryption Solution Requirements and Testing Procedures: Encryption, Decryption and Key Management within Secure Cryptographic Devices ("P2PE Solution Requirements")*

The following additional PCI SSC documents are used in conjunction with the aforementioned:

- *P2PE Glossary of Terms, Abbreviations and Acronyms*
- *PCI Data Security Standard Requirements and Security Assessment Procedures*
- *PA-DSS Requirements and Security Assessment Procedures*
- *PTS PIN Security Requirements*
- *PTS Hardware Security Module (HSM) Security Requirements*
- *PTS POI Modular Security Requirements*
- *PTS Device Testing and Approval Program Guide*
- *PCI DSS Glossary of Terms, Abbreviations, and Acronyms*
- *PCI DSS QSA Qualification Requirements – Supplement for P2PE Qualified Security Assessors– QSA (P2PE) and PA-QSA (P2PE)*

Note:

The P2PE Solution Requirements and Testing Procedures *document defines the specific technical requirements and provides the assessment procedures and template used to validate the point-to-point encryption solution's adherence to the P2PE Standard.*

The QSA Qualification Requirements – Supplement for Point-to-Point Encryption Security Assessors *document defines the requirements that must be met by a QSA (P2PE) and PA-QSA (P2PE) in order to perform assessments.*

All documents are available in electronic form at www.pcisecuritystandards.org (the "PCI SSC website").

1.2 Updates to Documents and Security Requirements

Security is a never-ending race against potential attackers. As a result, it is necessary to regularly review, update and improve the security requirements used to evaluate point-to-point encryption (P2PE) solutions. As such, PCI SSC endeavors to publish formal updates to its P2PE security requirements every 36 months, at a minimum. Additionally, PCI SSC provides interim updates to the PCI community through a variety of means, including required P2PE Assessor training, email bulletins, frequently asked questions and others.

PCI SSC reserves the right to change, amend or withdraw security requirements at any time. If such a change is required, PCI SSC will endeavor to work closely with PCI SSC's community of Participating Organizations, P2PE Solution Providers and P2PE Assessors to help reduce the impact of any changes.

1.3 Terminology

Note that throughout this document, the following terms shall have meanings shown in the chart below.

Term	Meaning
Accepted	A P2PE Solution is deemed to have been "Accepted" (and "Acceptance" is deemed to have occurred) when PCI SSC has: a) Received the corresponding P-ROV from the P2PE Assessor, in which the P2PE Assessor determines that the P2PE Solution satisfies all applicable requirements of the P2PE Standard and supporting documents; b) Confirmed that the P-ROV is correct as to form, the P2PE Assessor adequately reported the P2PE compliance of the P2PE Solution in accordance with the P2PE Program requirements and the detail provided in the P-ROV meets PCI SSC's reporting requirements; c) Received the P2PE Solution Acceptance Fee and all documentation required with respect to the P2PE Solution; and d) Listed the P2PE Solution on the List of Validated P2PE Solutions provided that PCI SSC may suspend, withdraw, revoke, cancel or place conditions upon (including without limitation, complying with remediation requirements) Acceptance any P2PE Solution in accordance with P2PE Program policies and procedures. ***Note:*** *As further addressed in Appendix A hereto, "Acceptance" is limited to the specific P2PE Solution that has met all of the above requirements.*
Application P-ROV	A P-ROV covering P2PE Domain 2 Requirements relating to a P2PE Application.
AOV	The "Attestation of Validation" Is a declaration of the P2PE Solution or P2PE Application's validation status with the P2PE Standard (as further described in the *PCI DSS QSA Qualification Requirements supplement for Point-to-Point Encryption Qualified Security Assessors – QSA (P2PE) and PA-QSA (P2PE)*). The P2PE Solution AOV, signed by a QSA (P2PE) and the P2PE Solution Provider, is used when validating, revalidating or submitting changes to a P2PE Solution. The P2PE Application AOV, signed by a PA-QSA (P2PE) and the P2PE Application Vendor, is used when validating, revalidating or submitting changes to a P2PE Application.
List of Validated P2PE Applications	The Council's authoritative List of Validated P2PE Applications appearing on the PCI SSC website.
List of Validated P2PE Solutions	The Council's authoritative List of Validated P2PE Solutions appearing on the PCI SSC website.
Listed (and "list" and similar terms)	Refer to the listing of a Validated P2PE Solution on the List of Validated. P2PE Applications or List of Validated P2PE Solutions (as applicable).
Listing	The listing and related information regarding a P2PE Solution or P2PE Application on the List of Validated P2PE Solutions or List of P2PE Validated Applications.

Term	Meaning
P-ROV	A "P2PE Report on Validation" completed by a P2PE Assessor and submitted directly to PCI SSC for review and Acceptance. For a P2PE Solution to be included on the List of Validated P2PE Solutions, a Solution P-ROV must be submitted directly to PCI SSC for review and Acceptance. For a P2PE Application to be included on the List of P2PE Validated Applications, an Application P-ROV must be submitted directly to PCI SSC for review and Acceptance.
P2PE Application	A software application that is included in a P2PE Solution and assessed per P2PE Domain 2 Requirements, and is intended for use on a PCI-approved point-of-interaction (POI) device or otherwise by a merchant.
P2PE Application Assessment	Assessment of a P2PE Application in order to validate that such P2PE Application adheres to all P2PE Domain 2 Requirements.
P2PE Assessor	A P2PE Assessor is a company then qualified by PCI SSC as either a QSA (P2PE) or PA-QSA (P2PE).
P2PE Components	Refer to *P2PE Glossary of Terms, Abbreviations and Acronyms*.
P2PE Domain 2 Requirements	The requirements of the P2PE Standard applicable to P2PE Applications.
P2PE Domain or Domain	Any of the six control domains of the P2PE Standard, which together represent the core areas where security controls need to be applied and validated in order for a P2PE Solution to be listed on the PCI SSC website.
***P2PE Instruction Manual* or "PIM"**	An instruction manual prepared by a P2PE Solution Provider in accordance with the P2PE Standard to instruct its customers and resellers/integrators on secure P2PE Solution implementation, to document secure configuration specifics, and to clearly delineate vendor, reseller/integrator, and customer responsibilities for installing and/or using P2PE Solutions. P2PE Solutions when implemented in accordance with the *P2PE Instruction Manual* should support merchants' PCI DSS compliance and also support reduced scope for PCI DSS requirements.
P2PE Non-Domain 2 Requirements	The requirements of the P2PE Standard other than P2PE Domain 2 Requirements.
P2PE Solution	Refer to *PCI P2PE Glossary of Terms, Abbreviations and Acronyms.*
P2PE Solution Assessment or P2PE Assessment	Assessment of a P2PE Solution in order to validate compliance with the P2PE Standard as part of the P2PE Assessor Program, and with respect a given PA-QSA (P2PE), includes P2PE Application Assessments of P2PE Applications incorporated into or a part of the P2PE Solutions assessed by such PA-QSA (P2PE).
P2PE Solution Provider	Refers to "P2PE solution provider" as defined in the *PCI P2PE Glossary of Terms, Abbreviations and Acronyms.*

Term	Meaning
P2PE Standard	The then-current versions of (or successor documents to) each component of PCI SSC's Solution requirements and Testing procedures for Point-to-Point Encryption, including but not limited to the *Payment Card Industry (PCI) Point-to-Point Encryption Solution Requirements and Testing Procedures*, any and all appendices, exhibits, schedules, and attachments to any of the foregoing and all materials incorporated therein, in each case, as from time to time amended and made available on the PCI SSC website.
P2PE Vendor Release Agreement or P2PE VRA	The current and applicable form of release agreement that PCI SSC: a) Requires to be executed by P2PE Solution Providers and/or P2PE Application Vendors (as applicable) in connection with the P2PE Assessor Program, and b) Makes available on the PCI SSC website.
PA-QSA (P2PE) Employee	An individual employed by a PA-QSA (P2PE) who has satisfied, and continues to satisfy, all PA-QSA (P2PE) Requirements applicable to employees of PA-QSA (P2PE)s who will conduct P2PE Assessments, as described in further detail herein.
Participating Payment Brand	A payment card brand that, as of the time in question, is also then a formally admitted member of PCI SSC (or affiliate thereof). The Participating Payment Brands as of the release of this version of this document were American Express Travel Related Services Company, Inc., DFS Services LLC, JCB Advanced Technologies, Inc., MasterCard International Incorporated and Visa International Service Association (or their affiliates).
Payment Application Qualified Security Assessor for Point-to-Point Encryption, or PA-QSA (P2PE)	A Payment Application Qualified Security Assessor (PA-QSA) company that: a) Is qualified by PCI SSC to provide services to P2PE Solution Providers and/or P2PE Application Vendors in order to validate that such providers' or vendors' P2PE Solutions and/or P2PE Applications adhere to all aspects of the P2PE Standard, including but not limited to, validation that payment applications, when incorporated into or used as part of a P2PE Solution, adhere to all P2PE Domain 2 Requirements; and b) Remains in Good Standing (as defined in Section 1.3 of the *QSA Qualification Requirements – Supplement for Point-to-Point Qualified Security Assessors*) as a PA-QSA (P2PE).
PCI SSC or the Council	PCI Security Standards Council, LLC.
PCI SSC Website	The then-current PCI SSC web site, which is currently available at http://www.pcisecuritystandards.org.
PCI-approved POI Device	Refer to *PCI Point-to-Point Encryption Glossary of Terms, Abbreviations and Acronyms*.
QSA (P2PE) Employee	An individual employed by a QSA (P2PE) who has satisfied, and continues to satisfy, all QSA (P2PE) Requirements applicable to employees of QSA (P2PE)s who will conduct P2PE Assessments, as described in further detail herein.

Term	Meaning
QSA Qualification Requirements	The then-current version of the *Payment Card Industry (PCI) Data Security Standard Validation Requirements for Qualified Security Assessors (QSA)* (or successor document), as from time to time amended and made available on the PCI SSC website.
Qualified Security Assessor for Point-to-Point Encryption or QSA (P2PE)	A Qualified Security Assessor (QSA) company that: ▪ Is qualified by PCI SSC to provide services to P2PE Solution Providers in order to validate that such providers' P2PE Solutions adhere to P2PE Non-Domain 2 Requirements and ▪ Remains in Good Standing (as defined in the *QSA Qualification Requirements – Supplement for Point-to-Point Qualified Security Assessors*) as a QSA (P2PE).
Secure Cryptographic Device (SCD)	Refer to *PCI Point-to-Point Encryption Glossary of Terms, Abbreviations and Acronyms.*
Solution P-ROV	A P-ROV covering all applicable P2PE Domains relating to a P2PE Solution.
Third-Party Service Provider	An entity that provides a service or function on behalf of a P2PE Solution Provider, which is incorporated into and/or referenced by the applicable P2PE Solution, such as a Certification Authority (as defined in the P2PE Standard), key-injection facility, payment gateway or data center.
Validated P2PE Application	A P2PE Application that has been assessed and validated by a PA-QSA (P2PE) to be in scope for the P2PE Program and to have met all P2PE Domain 2 Requirements and then Accepted by PCI SSC, so long as such Acceptance has not been revoked, suspended, withdrawn or terminated.
Validated P2PE Solution	A P2PE Solution that has been assessed by a QSA (P2PE) or PA-QSA (P2PE) to be in scope for the P2PE Program and to have met all of the requirements of the P2PE Standard and then Accepted by PCI SSC, so long as such Acceptance has not been revoked, suspended, withdrawn or terminated.

1.4 About the P2PE Standard

PCI SSC reflects a desire among constituents of the Payment Card Industry (PCI) at all levels for a single, standardized set of security requirements, security assessment procedures, and processes for recognizing P2PE Solutions validated by P2PE Assessors. The P2PE and related PCI SSC standards define a common security assessment framework that is currently recognized by all Participating Payment Brands.

Stakeholders in the payments value chain benefit from these requirements in a variety of ways, including but not limited to the following:

- Customers may choose to implement Validated P2PE Solutions in order to reduce the scope of their PCI DSS assessments.
- Listed P2PE Solutions have been validated as compliant with the P2PE Standard by P2PE Assessors.
- P2PE Solutions validated and listed by the Council are recognized by all Participating Payment Brands (however, each brand develops and manages their own compliance programs).

For more information regarding PCI SSC, please see the PCI SSC website.

1.5 P2PE Program Overview

This *Payment Card Industry (PCI) Point-to-Point Encryption Program Guide* (as from time to time amended and published on the PCI SSC website, the "P2PE Program Guide") reflects a single set of requirements currently recognized by all Participating Payment Brands regarding:

Note:
P2PE P-ROVs are reviewed and Accepted directly by PCI SSC.

- P2PE Solution Requirements
- Processes for recognizing P2PE Assessor validated P2PE Solutions
- Quality assurance processes for P2PE Assessors

P2PE Solution Providers may choose to have their P2PE Solutions validated for compliance with the P2PE Standard in accordance with this P2PE Program Guide in order to have those solutions included in the List of Validated P2PE Solutions on the PCI SSC website.

Merchants may choose to implement P2PE Solutions to reduce the scope of their PCI DSS assessments in accordance with specific P2PE scenarios (e.g. hardware-hardware). Merchants should consult with their acquirers or payment brands to determine any required PCI DSS validation processes.

There are six control Domains for validation of P2PE Solutions. These Domains represent the core areas where security controls need to be applied and validated in order for the P2PE Solution to be listed on the PCI SSC website, as follows:

Domain Name	Description
Domain 1: Encryption Device Management	Use secure encryption devices and protect devices from tampering
Domain 2: Application Security	Secure applications in the P2PE environment
Domain 3: Encryption Environment	Secure environments where POI devices are present
Domain 4: Segmentation between Encryption and Decryption Environments	Segregate duties and functions between encryption and decryption environments
Domain 5: Decryption Environment and Device Management	Secure decryption environments and decryption devices
Domain 6: P2PE Cryptographic Key Management	Use strong cryptographic keys and secure key-management functions

Further information about these Domains is contained in the P2PE Standard.

PCI SSC reserves the right to require revalidation due to changes to the P2PE Standard and/or due to specifically identified vulnerabilities in listed P2PE Solutions.

1.6 Roles and Responsibilities

There are several stakeholders in the P2PE community. Some of these—payment device vendors, application vendors, QSAs, P2PE Solution Providers, and PCI SSC—participate more directly in the assessment process. The following sections define the roles and responsibilities of these P2PE stakeholders.

PCI Security Standards Council, LLC (PCI SSC)

PCI SSC is the standards body that maintains the payment card industry standards, including the PCI DSS, PA-DSS, PTS, and P2PE. In relation to P2PE, PCI SSC:

- Performs quality assurance reviews of P-ROVs to confirm report consistency and quality
- Lists P2PE Validated Solutions and Applications on the PCI SSC website
- Qualifies and trains QSA (P2PE) and PA-QSA (P2PE) assessors to perform P2PE reviews
- Maintains and updates the P2PE Standard and related documentation according to a standards lifecycle management process

Note that PCI SSC does not approve reports from a validation perspective. The role of the QSA (P2PE) and PA-QSA (P2PE) is to validate the P2PE Solution meets all requirements of the P2PE Standard as of the date of the P2PE Assessment. PCI SSC Accepts P2PE Solutions only after performing quality assurance reviews to help ensure that QSAs (P2PE) and PA-QSAs (P2PE) accurately and thoroughly document the results of their P2PE Assessments.

Participating Payment Brands

The Participating Payment Brands develop and enforce their respective compliance programs, including but not limited to, related requirements, mandates and due dates.

P2PE Solution Providers

P2PE Solution Providers are entities (for example, processors, acquirers, or payment gateways) that have overall responsibility for the design and implementation of specific P2PE Solutions, and (directly or indirectly through outsourcing) manage P2PE Solutions for their customers and/or manage corresponding responsibilities.

P2PE Solution Providers have overall responsibility for ensuring that their P2PE Solutions satisfy all requirements of the P2PE Standard, including ensuring that such requirements are met by any Third-Party Service Providers that perform P2PE functions on behalf of the P2PE Solution Provider, such as Certification Authorities and key-injection facilities.

P2PE Assessors

P2PE Assessors are companies that have been qualified by PCI SSC as either QSAs or PA-QSAs, and have satisfied additional requirements to perform P2PE Assessments of certain P2PE Solutions, depending on whether they have been qualified as QSA (P2PE)s or PA-QSA (P2PE)s. Both categories of P2PE Assessors also submit corresponding P-ROVs on behalf of the applicable P2PE Solution Providers or P2PE Application Vendors (as applicable) directly to PCI SSC for review and Acceptance. P2PE Assessors are responsible for performing P2PE Assessments in accordance with the P2PE Standard and related P2PE Program documents, including this document, the *P2PE Reporting Instructions* and the P2PE Standard.

1. QSA (P2PE)s

QSA (P2PE)s are companies that have been (and remain) qualified by PCI SSC to perform P2PE Assessments with respect to P2PE Non-Domain 2 Requirements.

Note: *Not all QSAs are QSA (P2PE)s—there are additional qualification requirements that must be met for a QSA to become a QSA (P2PE).*

QSA (P2PE)s are responsible for:

a) Performing assessments of P2PE Solutions in accordance with the P2PE Standard.

b) Providing an opinion regarding whether the P2PE Solution and environment satisfies the P2PE Standard.

c) Confirming that the *P2PE Instruction Manual* specific to a given P2PE Solution effectively documents secure configuration settings, merchant guidance, and other required information for merchants and, where applicable, resellers/integrators.

d) Providing adequate documentation within the P-ROV to demonstrate the P2PE Solution and environment‘s compliance with the P2PE Standard.

e) Submitting the P-ROV to PCI SSC, along with the Solution AOV (signed by both QSA (P2PE) and P2PE Solution Provider).

f) Maintaining an internal quality assurance process for its QSA (P2PE) efforts in accordance with the P2PE Standard.

g) Staying up to date with Council rules, requirements and procedures, and industry trends and best practices.

h) Determining the scope and applicability of the P2PE Standard as it applies to a given P2PE Assessment, in accordance with the P2PE Standard.

It is the QSA (P2PE)’s responsibility to validate that the P2PE Solution meets all requirements of the P2PE Standard.

2. PA-QSA (P2PE)s

PA-QSA (P2PE)s are companies that have been (and remain) qualified by PCI SSC to perform P2PE Assessments of P2PE Applications used within P2PE Solutions with respect to P2PE Domain 2 Requirements. Note: not all PA-QSAs are PA-QSA (P2PE)s — there are additional qualification requirements that must be met for a PA-QSA to become a PA-QSA (P2PE). Additionally, not all QSA (P2PE)s are PA-QSA (P2PE)s.

PA-QSA (P2PE)s are responsible for:

- Performing P2PE Assessments of P2PE Applications in accordance with P2PE Domain 2 Requirements.
- Providing an opinion regarding whether the P2PE Application meets P2PE Domain 2 Requirements.
- Providing adequate documentation within the P-ROV to demonstrate the P2PE Application’s compliance with P2PE Domain 2 Requirements.
- Maintaining an internal quality assurance process for its PA-QSA (P2PE) efforts in accordance with the P2PE Standard.
- Staying up to date with Council rules, requirements and procedures, and industry trends and best practices.

- Determining the scope and applicability of the P2PE Standard as it applies to a given P2PE Assessment of a P2PE Application, in accordance with the P2PE Standard.

It is the PA-QSA (P2PE)'s responsibility to validate that the P2PE Application meets all P2PE Domain 2 Requirements.

PCI PTS Laboratories

Security laboratories qualified by PCI SSC under the PCI SSC PTS laboratory program ("PCI PTS laboratories") are responsible for the evaluation of POI devices against PCI SSC's PTS standards and requirements ("PTS requirements"). Evaluation reports on devices found compliant with the PTS requirements are submitted by the PCI PTS laboratories to PCI SSC for approval, and if approved, the device is listed on PCI SSC's list of PTS validated devices. Note: device evaluation by a PCI PTS laboratory is a separate process from the assessment and validation of a device as part of a P2PE Solution Assessment; the P2PE Solution Assessment will confirm whether or not a device is listed on PCI SSC's list of PTS validated devices.

Payment Device (Hardware) Vendors

A POI device vendor submits a POI device for evaluation to an independent PCI PTS security laboratory. Per PTS requirements, device vendors must develop a supplement document describing the secure operation and administration of their equipment to assist merchants and P2PE Solution Providers.

Application (Software) Vendors

As part of establishing the P2PE compliance of its applications, an application vendor that develops applications with access to account data on a POI device must have those applications assessed for secure operation within the applicable POI devices, and must provide an *Implementation Guide* that describes secure installation and administration of such applications on the corresponding POI devices.

If an application is to be used in multiple P2PE Solutions, the vendor may, optionally, seek to have that application validated and Accepted as a Validated P2PE Application, and accordingly listed on the List of Validated P2PE Applications, by submitting to PCI SSC the corresponding P-ROV, Application AOV signed by both PA-QSA (P2PE) and vendor, the application's *Implementation Guide* and payment of appropriate fees (see Appendix C, "Listing of Applications Used in Validated P2PE Solutions").

Integrators and Resellers

Integrators and Resellers are those entities that may sell, install, and/or service P2PE Solutions and/or components thereof on behalf of device vendors, P2PE Solution Providers or others. Integrators and Resellers performing (or purporting to perform) services relating to Validated P2PE Solutions are responsible for:

- Implementing Validated P2PE Solutions in compliance with:
  - **a)** All applicable requirements in this document; and
  - **b)** The *P2PE Instruction Manual.*
- Configuring P2PE Solutions (where configuration options are provided) according to the validated processes provided by the P2PE Solution Provider, as documented in the *P2PE Instruction Manual.*
- Servicing P2PE devices (for example, troubleshooting, delivering remote updates, and providing remote support) according to the validated processes in the *P2PE Instruction Manual.*

Integrators and Resellers do not submit P2PE Solutions for P2PE Assessment. Only a P2PE Solution Provider may submit a P2PE Solution for P2PE Assessment.

Certification Authorities

A Certification Authority (CA) (as defined in the P2PE Standard) is a trusted party (which may be a Third-Party Service Provider or the Solution Provider) that is responsible for the issuance of digital certificates. For purposes of these requirements, a certificate is any digitally signed value containing a public key.

Specific requirements for CAs involved in remote key distribution are set out in Annex A of the P2PE Standard. CA requirements apply to all entities signing public keys, whether in X.509 certificate-based schemes or other designs. These requirements apply equally to third-party CAs and CAs that are hosted by the P2PE Solution Provider.

Ultimately, it remains the P2PE Solution Provider's responsibility to ensure that the CA is in compliance with the requirements set out in the P2PE Standard.

Key-Injection Facilities

The term "key-injection facility" (KIF) describes the entities performing key injection into POI devices. Key injection may be performed by the P2PE Solution Provider or by a Third-Party Service Provider such as a POI terminal manufacturer or vendor. Environmental and key-management requirements are defined in Domains 1, 5 and 6 of the P2PE Standard; and Domain 6 Annex B contains additional requirements for KIFs.

Ultimately, it remains the P2PE Solution Provider's responsibility to ensure that the KIF is in compliance with the requirements set out in the P2PE Standard.

Merchants

Merchants are the P2PE Solution consumers and users. Merchant roles and responsibilities as P2PE stakeholders include:

- Use of Validated P2PE Solutions, coordinating with their acquirers to determine which solutions and devices to implement.
- Adherence to the *P2PE Instruction Manual* (PIM), provided to the merchant by the P2PE Solution Provider.
- If the merchant has other non-P2PE payment channels, ensuring the P2PE environment is adequately segmented (isolated) from any non-P2PE payment channels.
- Removing any legacy cardholder data or systems from the P2PE environment.
- Validating applicable PCI DSS requirements in accordance with payment brand requirements.

2 Overview of P2PE Solution Validation Processes

The P2PE Solution review process is initiated by the P2PE Solution Provider. The PCI SSC website has all of the associated documents needed to navigate the P2PE review process. The following is a high level overview of the process:

1. The P2PE Solution Provider selects a P2PE Assessor from the Council's list of recognized P2PE Assessors and negotiates the cost and any associated P2PE Assessor services or confidentiality agreements with the P2PE Assessor.
2. The P2PE Solution Provider then provides access to the P2PE Solution to the P2PE Assessor, including details of all Third-Party Service Providers used, access to facilities, details of applications and devices used within the solution, *Implementation Guides* for P2PE Applications used in the solution*, P2PE Instruction Manual*, and all associated manuals and other required documentation, including but not limited to the P2PE Solution Provider's signed P2PE VRA and all materials required thereby.
3. The P2PE Assessor must determine the scope of the review including:

   a) Third-Party Service Providers to be assessed (e.g. key-injection facilities, Certification Authorities and others)

      If these Third-Party Service Providers have already been assessed per the P2PE Standard and a P-ROV to that effect has been produced by a QSA (P2PE), then the P2PE Assessor must evaluate the scope and relevance of the prior assessment to the current P2PE Solution review, and identify any further testing required in accordance with the P2PE Standard.

   b) Devices used in P2PE Solutions.

      The P2PE Assessor must ensure that all devices used in the P2PE Solution are identified and include only PCI-approved POI devices and HSM's which are **either** FIPS 140-2 Level 3 (or higher) certified **or** PCI-approved (listed on the PCI SSC website, with a valid SSC listing number, as Approved PCI PTS Devices under the approval class "HSM").

   c) Applications used in P2PE Solutions.

      The extent of the P2PE Assessment to be performed on these applications is dependent on whether the application has access to clear-text account data and whether the application is already included in the List of Validated P2PE applications on the PCI SSC website.

   d) PCI DSS compliance status of the secure decryption environment.

      If the secure decryption environment has already been validated as PCI DSS compliant by a QSA, the P2PE Assessor must evaluate the scope and relevance of that assessment to the P2PE Solution review and identify any further testing required.

4. The P2PE Assessor then assesses the P2PE Solution's security functions and features to determine whether the solution complies with the security requirements of the P2PE Standard. If the P2PE Assessor determines that the P2PE Solution is in compliance with the P2PE Standard, the P2PE Assessor submits to the P2PE Solution Provider a corresponding Solution P-ROV (using the template and Reporting Instructions from the PCI SSC website), opining to compliance and setting forth the results, opinions and conclusions of the P2PE

Note: *If the P2PE Solution being assessed includes an application which is not included in the List of Validated P2PE Applications on the PCI SSC website then an Application P-ROV for that application must be submitted with the Solution P-ROV.*

See Appendix C for details of Listing of Validated P2PE Applications.

Assessor on all testing procedures. *If approved by the P2PE Solution Provider, the P2PE Assessor then submits such Solution P-ROV to PCI SSC, along with the Solution AOV, the signed P2PE VRA, and all other required materials*.

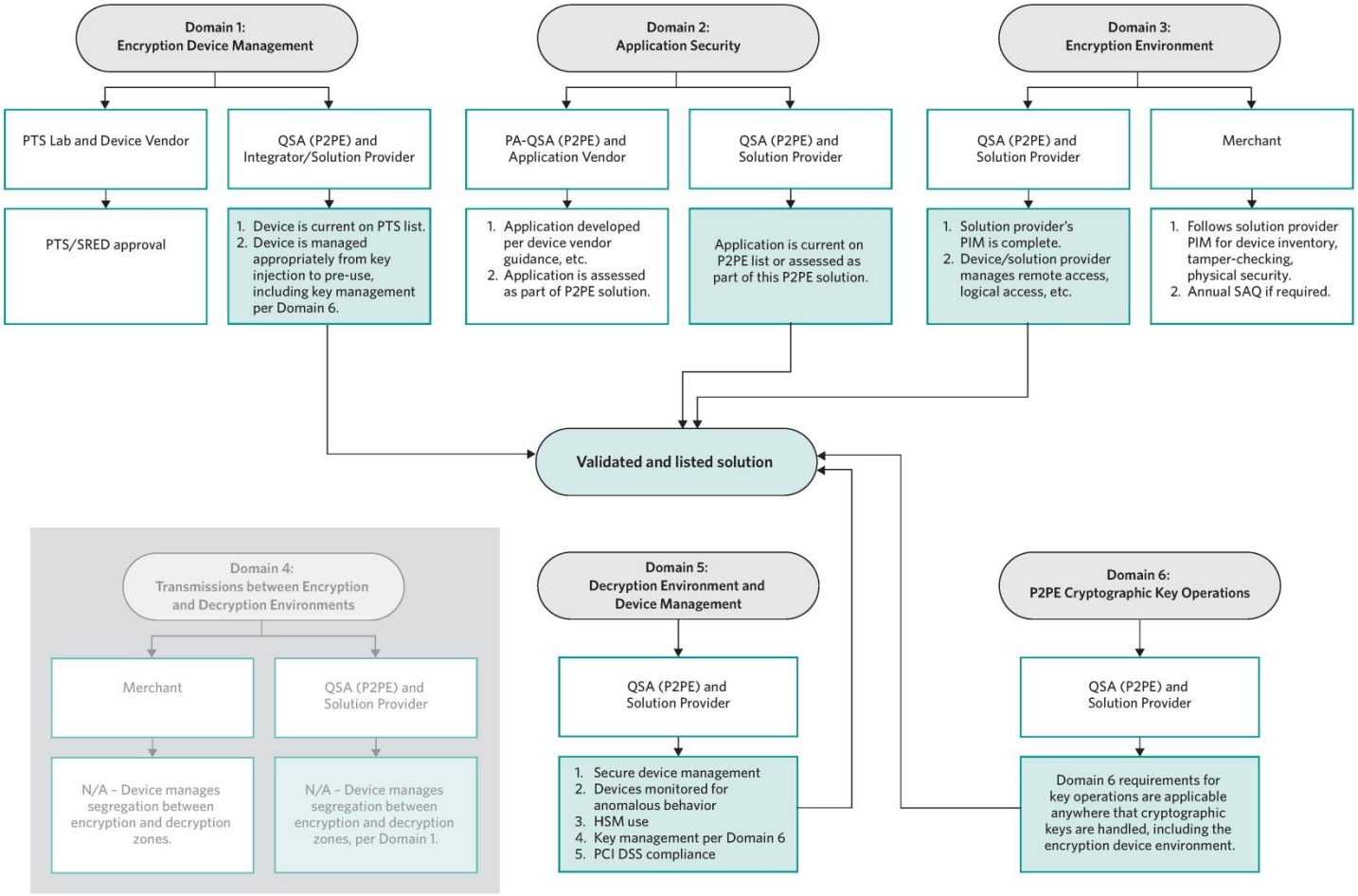
5. Once PCI SSC has received all required information and materials, PCI SSC reviews the Solution P-ROV to confirm that it meets the P2PE Program requirements. If confirmed, PCI SSC will notify the P2PE Assessor and P2PE Solution Provider that the Solution P-ROV meets requirements and issue an invoice to the P2PE Solution Provider for the applicable fee.
6. Once all applicable fees have been received, the Council will sign the corresponding Solution AOV and add the P2PE Solution to the List of Validated P2PE Solutions on the PCI SSC website, and the P2PE Solution is deemed to be Accepted.

***Note**: As further addressed in Appendix A hereto, "Acceptance" is limited to the specific P2PE Solution that has met all Acceptance requirements. See Appendix A, "P2PE Solutions and Acceptance."*

2.1 Developing and Validating a P2PE Solution

The process for developing and validating a P2PE Solution that uses SCDs for encryption, decryption, and cryptographic key management is provided below. The following flow chart and table illustrate the responsible parties for implementing requirements and validating compliance with each Domain, the high-level purpose of controls for each Domain, and the role of specific Domain validation within the overall P2PE Solution validation process.

Note: *Domain 4 is greyed out in the diagram below as there are no applicable requirements in this Domain for the current phase of P2PE.*



3 Considerations for Vendors of P2PE Components and Applications Used in P2PE Solutions

The P2PE Standard is a cross-functional PCI SSC standard with specific requirements to use devices, applications, and environments that have been validated through other PCI SSC programs, such as PTS or PCI DSS, but that also contains specific requirements for overall P2PE Solutions and for the encryption device processes, merchant guidance, decryption environment and cryptographic keys that are used throughout the P2PE Solution.

3.1 Considerations for Vendors of Secure Cryptographic Devices Used in P2PE Solutions

The P2PE Standard requires the use of SCDs for encryption and decryption of account data and management of cryptographic keys. SCDs are subject to device level approval before being used as part of a P2PE Solution.

- POI devices must be PCI SSC approved PTS devices with SRED (secure reading and exchange of data) listed as a "function provided."
- HSMs must be either FIPS 140-2 Level 3 (or higher) certified or PCI-approved (listed on the PCI SSC website, with a valid SSC listing number, as Approved PCI PTS Devices under the approval class "HSM").

Vendors of SCD's are responsible for obtaining and maintaining the device approvals required for their devices to be used in P2PE Solutions. P2PE Assessors will request evidence of device approvals being in place and current as part of performing the assessment of a P2PE Solution.

a) Considerations for Vendors of POIs used in P2PE Solutions

PCI SSC approved PTS devices (also called "PCI-approved POI devices") provide a trusted foundation of physical and logical security that is the foundation of P2PE Solutions. Any SCD used for the acceptance and encryption of account data at the point of sale is required to be a PCI-approved POI device with SRED (secure reading and exchange of data) listed as a "function provided", and with SRED capabilities enabled and active. PTS approval requires validation that all key-management and key-loading functions can be implemented within SRED-approved firmware for POI devices, and that all account data outputs from the device to external systems or untrusted applications are encrypted.

Obtaining PTS approval is the responsibility of the device vendor and is a prerequisite for the devices being assessed as part of a P2PE Solution. POI vendors wishing to obtain PTS approval should consult the PCI SSC website for further information.

Obtaining PTS approval does not replace or supersede any payment brand specific device approval processes.

b) Considerations for Vendors of HSMs used In P2PE Solutions

SCDs used for cryptographic key-management functions and/or the decryption of account data include HSMs (host/hardware security modules). Any HSMs that support key-management functions within P2PE Solutions are required to be either FIPS 140-2 Level 3 (or higher) certified or PTS HSM Approved.

Obtaining such approval is the responsibility of the device vendor and is a prerequisite for the devices being assessed as part of a P2PE Solution.

HSM vendors wishing to obtain PTS approval for their devices should consult the PCI SSC website for further information.

3.2 Considerations for Vendors of Applications Used in P2PE Solutions

All applications which function within a P2PE Solution must be validated by a PA-QSA (P2PE) against the P2PE Domain 2 Requirements. Such applications operate on the PCI-approved POI device and either:

- Have access to clear-text account data; or
- Do not have access to clear-text account data.

Requirements in Domain 2 entail protecting account data, developing and maintaining secure applications, and incorporating secure application management processes. Applications which have access to clear-text account data must undergo validation per all P2PE Domain 2 Requirements. All other applications are subject to one testing procedure which validates they do not have any access to clear-text account data.

1) Domain 2 Assessments for Applications with Access to Clear Text Account Data

Applications *with access to clear-text account data* must undergo validation per all P2PE Domain 2 Requirements, and will be either:

- Independently listed on the List of Validated P2PE Applications

  OR

- Appear only as a component of a specific Validated P2PE Solution (without any independent application listing).

Note: *The process for submitting a P2PE Application for inclusion on the List of Validated P2PE Applications is detailed in Appendix C.*

Seeking independent listing of an application on the List of Validated P2PE Applications is optional and requires separate P2PE Assessment. However, as described further below, such independent listing may be important for applications used in multiple P2PE Solutions because it avoids the need to repeat certain tests each time the same listed application is later used within new P2PE Solutions.

Domain 2 testing procedures have two parts; Application Vendor testing procedures and Solution Provider testing procedures. Application Vendor testing procedures address those application development and maintenance controls which are the responsibility of the application vendor. Solution Provider requirements address the secure implementation of the application within a P2PE Solution in accordance with the advice and guidance provided by application vendor in the application *Implementation Guide*.

If an application is on the List of Validated P2PE Applications, then an Application P-ROV validating the Application Vendor testing procedures has already been accepted by PCI SSC. As a result, only the Domain 2 Solution Provider testing procedures must be validated and evidenced in the P-ROV for the P2PE Solution Assessment.

If an application is not on the List of Validated P2PE Applications, then both the Domain 2 Application Vendor and Domain 2 Solution Provider testing procedures must be validated and

evidenced in the P-POV for the P2PE Solution Assessment. This applies for **each** assessment of **each** P2PE Solution in which the application is used.

2) Domain 2 Assessments for Applications without Access to Clear Text Account Data

For applications that *do not have access to account data*, only Requirement 2A-3 is applicable. These tests are completed as part of each P2PE Solution Assessment by a PA-QSA (P2PE) and validate that these applications do not have access to clear-text account data, and are not bypassing or overriding any security features provided by the other approved components of the P2PE Solution. Such applications are listed only as components of Validated P2PE Solutions and are not eligible for inclusion in the List of Validated P2PE Applications.

3) PA-DSS Applicability to P2PE

Applications used within P2PE Solutions may or may not be eligible for PA-DSS validation. PA-DSS and P2PE are distinct PCI SSC standards with different requirements; validation against one of these standards does not guarantee or provide automatic validation against the other standard.

4 P2PE Solution Provider Considerations – Preparation for Assessment

4.1 Prior to the P2PE Assessment

P2PE Solution Providers are encouraged to take the following preparatory actions prior to commencing a P2PE Assessment with a P2PE Assessor:

- Review the PCI DSS, the P2PE Standard and all related documentation located at the PCI SSC website.
- Determine/assess the P2PE Solution's readiness to comply with the P2PE Standard Requirements
  - Perform a "gap" analysis between how the P2PE Solution functions compared to the P2PE Standard
  - Correct any gaps.
- If desired, the P2PE Assessor may be engaged separately to perform a pre-assessment or "gap" analysis of a P2PE Solution Provider's P2PE Solution. If the P2PE Assessor notes deficiencies that would prevent a clean opinion, the P2PE Assessor should provide to the P2PE Solution Provider a list of P2PE Solution features to be addressed before the formal review process begins.
- Determine which applications used within the P2PE Solution have, or potentially have, access to clear-text account data. Any such applications that do not appear on the List of Validated P2PE Applications require assessment against all P2PE Domain 2 Requirements. Such assessments may be done separately, prior to validation of the P2PE Solution (resulting in the application being listed on the List of Validated P2PE Applications) **OR** may be completed as part of the P2PE Solution validation (resulting in identification of the application as a component of the P2PE Solution, but no independent application listing). These application assessments must be completed by a PA-QSA (P2PE). See Appendix C for details of the listing process for such applications.
- Determine whether the P2PE Solution Providers decryption environment is PCI DSS compliant. This assessment may be completed separately, prior to validation of the P2PE Solution or may be completed as part of the P2PE Solution validation (note; the resulting Report on Compliance should not be included in the Solution P-ROV submitted to PCI SSC)
- Determine whether the P2PE Solution Provider's *P2PE Instruction Manual* for merchants meets the P2PE Standard.
- Determine whether any Third-Party Service Providers are used in the P2PE Solution, e.g. key-injection facility or Certification Authority. For each Third-Party Service Provider identified determine whether the entity has a P2PE Assessment completed and if so the scope of that assessment in relation to the services being performed for the P2PE Solution Provider. P2PE Solution Providers are responsible for ensuring that the Third-Party Service Providers they use are compliant with all applicable requirements of the P2PE Standard*"* and that appropriate agreements are in place to ensure proper information disclosures if required under the P2PE Vendor Release Agreement.

4.2 Required Documentation and Materials

As a requirement for the P2PE Solution Assessment, the P2PE Solution Provider must provide the P2PE Assessor with all required documentation, software, access to facilities and access to Third-Party Service Providers used in connection with the P2PE Solution.

Complete versions of all required P2PE Solution-related materials (such as manuals, the *P2PE Instruction Manual*, the P2PE Vendor Release Agreement and all other required materials relating to the review and participation in the P2PE Program) must be delivered to the P2PE Assessor, not to PCI SSC.

Documents and items to submit to the P2PE Assessor include (without limitation):

1. Lists of all components used in the P2PE Solution including but not limited to:
    - All PCI-approved POI devices with associated device approval details
    - All HSM's used with associated device approval details
    - All applications used in the P2PE Solution identifying which, if any, have access to clear-text account data and which POI's they are used on
    - Detailed cryptographic key matrix
2. Documentation that relates to installing and configuring the P2PE Solution, or which provides information about the P2PE Solution. Examples of such documentation include:
    - *P2PE Instruction Manual;*
    - *Implementation Guides* for applications assessed against Domain 2
    - Key-management procedures and
    - Change control documentation that shows how changes are illustrated to customers;
3. Additional documentation—such as diagrams and flowcharts—that will aid in the P2PE Solution Assessment process (the P2PE Assessor may request additional material when necessary); and
4. The executed P2PE Vendor Release Agreement and all materials required thereby (see Section 4.4 below).

4.3 P2PE Assessors

PCI SSC qualifies and provides required training for P2PE Assessors (QSA (P2PE) and PA-QSA (P2PE)) to assess and validate P2PE Solutions and P2PE Applications for adherence to the P2PE Standard.

In order to perform P2PE Solution Assessments, a P2PE Assessor must have been qualified by PCI SSC and remain in good standing as both a QSA and QSA (P2PE).

If also assessing P2PE Domain 2 Requirements, the Assessor must also be both a PA-QSA and PA-QSA (P2PE) in good standing and complete all required P2PE Assessor training.

All recognized P2PE Assessors are listed on the PCI SSC website. These are the only assessors recognized by PCI SSC as qualified to perform P2PE Assessments. The diagram in Appendix E illustrates the relationships between QSA (P2PE) and PA-QSA (P2PE) companies.

The prices and fees charged by P2PE Assessors are not set by PCI SSC. These fees are negotiated between the P2PE Assessor and their customer. Before deciding on a P2PE Assessor, it is recommended that a prospective customer should check PCI SSC's list of recognized P2PE Assessors, talk to several P2PE Assessor firms, and follow their own vendor selection processes.

Non-P2PE assessment services that may be offered by P2PE Assessors

The list below provides examples of non-P2PE assessment services that may be offered by P2PE Assessors. None of these services are required by PCI SSC. If these services are of interest to your company, please contact P2PE Assessors for availability and pricing. Examples of non-P2PE assessment services include:

- Guidance on designing P2PE Solutions in accordance with the P2PE Standard.
- Review of P2PE Solution design, response to questions via e-mail or phone, and participation in conference calls to clarify requirements.
- Guidance on preparing the *P2PE Instruction Manual*.
- Pre-assessment ("gap" analysis) services prior to beginning formal P2PE Solution Assessment.
- Guidance for bringing the P2PE Solution into compliance with the P2PE Standard if gaps or areas of non-compliance are noted during the assessment.

Please Note: *When arranging for non-P2PE Solution assessment services with a P2PE Assessor, care should be taken by both the P2PE Solution Provider and the P2PE Assessor to ensure that the P2PE Assessor is not put in a position where it is later required to assess its own work product as part of the actual P2PE Solution Assessment. Conflicts of interest may cause a P2PE Solution to be rejected by PCI SSC.*

4.4 P2PE Vendor Release Agreement

The P2PE Solution Provider's signed *P2PE Vendor Release Agreement* (and related materials) should be provided to the P2PE Assessor along with access to the P2PE Solution and all documents and materials at the beginning of the P2PE Assessor's assessment process, and must be provided to PCI SSC by the P2PE Assessor along with the initial P-ROV submitted to PCI SSC. Among other things, the P2PE VRA covers confidentiality issues, the P2PE Solution Provider's agreement to P2PE Program requirements, policies and procedures, and gives the P2PE Solution Provider's permission to the P2PE Assessor to release P-ROVs and related materials to PCI SSC for review. Pursuant to the P2PE VRA, P2PE Solution Providers must adopt appropriate required vulnerability handling programs and policies ("VHPs") and attest to their compliance therewith (a "VHP Attestation"). The signed P2PE VRA and required accompanying materials **must be delivered directly** to PCI SSC by the P2PE Assessor, along with the corresponding P-ROV.

A P-ROV will not be reviewed by PCI SSC without a current P2PE VRA and accompanying materials on file from the relevant P2PE Solution Provider.

So long as an executed current version of the P2PE VRA is on file with PCI SSC for the relevant P2PE Solution Provider, it is not required to re-submit a newly executed P2PE VRA with each subsequent P-ROV for the same P2PE Solution Provider.

4.5 The Portal

All documents relating to the P2PE Solution validation process are to be submitted by P2PE Assessors, on behalf of the P2PE Solution Provider, to the Council through the PCI SSC's secure website ("Portal"). Submissions are pre-screened in the Portal by Council staff to ensure that all required documentation has been included and the basic submission requirements have been satisfied.

The Portal is also used by the Council to track all communications relating to a particular submission.

4.6 P2PE Solution Acceptance Fees

P2PE Solution Providers are also required to pay a *P2PE Solution Acceptance Fee* (all P2PE Program Fees are posted on the PCI SSC website) to PCI SSC immediately prior to Acceptance of each new P2PE Solution. For each new P2PE Solution, the P2PE Solution Acceptance Fee will be invoiced immediately prior to Acceptance, and must be received by PCI SSC for the P2PE Solution to be Accepted and added to PCI SSC's List of Validated P2PE Solutions. Upon Acceptance, PCI SSC will sign and return a copy of the Solution AOV to both the P2PE Solution Provider and the P2PE Assessor.

Note:

The P2PE Solution Provider pays all P2PE Assessment and validation fees directly to P2PE Assessor (these fees are negotiated between the P2PE Solution Provider and the P2PE Assessor).

PCI SSC will bill the P2PE Solution Provider for all P2PE Solution Acceptance Fees and the P2PE Solution Provider will pay these fees directly to PCI SSC.

There are no annual recurring PCI SSC fees associated with the Acceptance of a Validated P2PE Solution. There are, however, PCI SSC fees associated with updates that may be made from time-to-time by Solution Providers to Validated P2PE Solutions. Please see the PCI SSC website for more information.

5 P2PE Solution Provider Considerations – Managing Validated P2PE Solutions

Following successful initial P2PE Assessment, Acceptance of a P2PE Solution is generally valid for two years from the date of Acceptance (subject to earlier Revocation in accordance with the P2PE VRA and P2PE Program procedures).

5.1 Revalidation of Listed P2PE Solutions

In order for a Validated P2PE Solution to remain on the List of Validated P2PE Solutions, it must undergo a new full P2PE Solution Assessment (resulting in Acceptance) every two years, and an "interim assessment" twelve months after each Acceptance.

5.1.1 Interim Assessment (Healthcheck)

Interim assessments (or "healthchecks") are required in order to provide additional confidence that between full assessments the:

- P2PE Solution continues to meet the requirements of the P2PE Standard,
- P2PE Solution Provider's change management processes are operating effectively, and
- P2PE Solution Provider gives consideration to whether updates to the P2PE Solution are necessary to address changes to the external threat environment in which the P2PE Solution operates.

12 months after each Acceptance, by the Revalidation Date noted on the List of Validated P2PE Solutions, the P2PE Solution Provider is **required** to submit an updated Solution AOV, performing the "interim assessment steps" This includes a healthcheck which must be completed by a P2PE Assessor. The tests to be performed in the healthcheck are available on the PCI SSC website.

There are no PCI SSC fees associated with interim assessments.

Upon receipt of the updated Solution AOV, PCI SSC will:

(i) Review the submission for completeness;

(ii) Once completeness is established, update the List of Validated P2PE Solutions with the new Revalidation Date; and

(iii) Sign and return to both the P2PE Solution Provider and the P2PE Assessor a copy of the updated Solution AOV.

If an updated Solution AOV is not submitted for a listed P2PE Solution, the P2PE Solution will be subject to early administrative expiry, as follows: On the Revalidation Date, the List of Validated P2PE Solutions will be updated to show the P2PE Solution in **Orange** for a period of 60 days. If the updated and complete Solution AOV is received within this 60-day period, PCI SSC will update the List of Validated P2PE Solutions with the new Revalidation Date and remove the **Orange** status. If the updated and complete Solution AOV is not received within this 60-day period, the List of Validated P2PE Solutions will be updated to show the P2PE Solution in **Red**, and an additional fee will be levied if the P2PE Solution Provider wishes to revalidate the P2PE Solution.

5.1.2 Full Re-assessment

24 months after Acceptance, on the Expiry Date noted on the List of Validated P2PE Solutions, that Acceptance and the corresponding Solution AOV will expire. Accordingly, in order for a listed P2PE Solution to remain on the List of Validated P2PE Solutions, it is **required** to successfully undergo a new full P2PE Solution Assessment, resulting in a new Acceptance, on or before the applicable Expiry Date. This re-assessment must follow the same process as an initial P2PE Solution Assessment.

If a new P-ROV and Solution AOV is not timely submitted for a listed P2PE Solution, the P2PE Solution will be deemed to be subject to expiry, as follows. On the Expiry Date, the List of Validated P2PE Solutions will be updated to show the P2PE Solution in **Orange** for a period of 60 days. If the updated and complete required documentation is received within this 60-day period, PCI SSC will update the List of Validated P2PE Solutions with the new Revalidation and Expiry Dates and remove the **Orange** status. If the required and complete documentation is not received within this 60-day period, the List of P2PE Validated Solution will be updated to show the P2PE Solution in **Red.**

5.2 Changes to Listed P2PE Solutions

P2PE Solution Providers update already-listed current P2PE Solutions for various reasons—for example, upgrading the types of SCDs used or adding additional software applications. Changes do not have any impact on Revalidation Dates or Expiry Dates of P2PE Solutions. Changes are categorized as follows:

- ***Administrative Changes*** are changes made to a listed P2PE Solution that have no impact on compliance of the listed P2PE Solution with any requirements of the P2PE Standard. In this case, for the modified P2PE Solution to be listed, the P2PE Solution Provider documents the change for the P2PE Assessor to review—see Section 5.2.1, "Change Documentation and Process," for specifics—and if ultimately approved by PCI SSC, the List of Validated P2PE Solutions is updated to reflect the change. Examples of administrative changes include, but are not limited to, corporate identity changes and P2PE Solution name changes.
- ***Designated Changes*** are changes made to a listed P2PE Solution to either:
  - Add or remove a validated POI device;
  - Add or remove a validated POI application with access to clear-text account data; or
  - Add or remove a POI application that does not have access to clear-text account data

  The P2PE Solution Provider advises the P2PE Assessor of the changes and arranges for a delta assessment to be completed. See Section 5.2.1, "Change Documentation and Process," for details.
- ***Other Changes*** are changes made by the P2PE Solution Provider which affect compliance with the requirements of the P2PE Standard. These changes must be implemented in a P2PE compliant manner that ensures adherence to P2PE requirements for the entire solution. An assessment of the changes must be performed by an appropriate P2PE Assessor as part of the interim assessment/healthcheck process or full-reassessment, whichever is sooner.

The sections below provide information on the supporting documentation that must be generated and the processes that are to be followed in order to successfully effect changes to previously listed P2PE Solutions.

The process flow for changes to listed solutions is detailed in Figure 3.

5.2.1 Change Documentation and Process

5.2.1.1 Administrative Changes

All Administrative Changes to Validated P2PE Solutions must be disclosed by the P2PE Solution Provider in a *Solution Provider Change Analysis* document. This must be submitted to the P2PE Assessor and contain the following information at a minimum:

- Name and reference number of the Validated P2PE Solution;
- Description of the change;
- Description of why the change is necessary;
- The updated *P2PE Instruction Manual*

Note:

Administrative and Designated Changes are only permissible to already-listed P2PE Solutions that have not expired.

It is *strongly recommended* that the P2PE Solution Provider submit the *Solution Provider Change Analysis* to the same P2PE Assessor used for the original P2PE Solution Assessment.

If the P2PE Assessor agrees that the change as documented by the P2PE Solution Provider has no impact on the P2PE related functions of the P2PE Solution:

(i) The P2PE Assessor must so notify the P2PE Solution Provider

(ii) The P2PE Solution Provider prepares and signs an Solution AOV, and sends it to the P2PE Assessor

(iii) The P2PE Assessor signs their concurrence on the Solution AOV and forwards it, along with the *Solution Provider Change Analysis* and the P2PE Solution's updated *P2PE Instruction Manual* to PCI SSC and

(iv) PCI SSC will then review the Solution AOV and *Solution Provider Change Analysis* for quality assurance purposes.

If the P2PE Assessor does not agree with the P2PE Solution Provider that the change, as documented, has no impact on the P2PE related functions of the P2PE Solution, the P2PE Assessor must return the *Solution Provider Change Analysis* to the P2PE Solution Provider and should work with them to consider what actions are necessary to address the P2PE Assessor's observations.

Following successful PCI SSC quality assurance review of an Administrative Change:

- An invoice for the applicable Administrative Change Fee will be issued to the P2PE Solution Provider
- Upon payment of the invoice to PCI SSC as described in Validation Maintenance Fees below,

PCI SSC will: (i) update the List of Validated P2PE Solutions on the PCI SSC website accordingly with the new information and (ii) sign and return a copy of the Solution AOV to both the P2PE Solution Provider and the P2PE Assessor. The Revalidation Date and Expiry Date of this P2PE Solution will remain unchanged i.e. an administrative change has no impact on the Revalidation Date or Expiry Date of a listed P2PE Solution. PCI SSC communicates quality issues associated with any aspect of the submission to the P2PE Assessor, and those issues are resolved according to the process depicted in Figure 2. PCI SSC reserves the right to reject any *Solution Provider Change Analysis* if it determines that a change described therein and purported to be an Administrative Change is ineligible for treatment as such.

5.2.1.2 Designated Changes

If a previously listed P2PE Solution is modified, and that modification is deemed to be a Designated Change (as set out above), then the P2PE Solution Provider prepares documentation of the change and submits the *Solution Provider Change Analysis* to the P2PE Assessor for review. It is *strongly recommended* that the P2PE Solution Provider submit this to the same P2PE Assessor used for the original assessment.

If the P2PE Assessor agrees that the changes as documented in the *Solution Provider Change Analysis* by the P2PE Solution Provider are eligible Designated Changes then the P2PE Assessor must so notify the P2PE Solution Provider, following which:

(i) The P2PE Assessor must perform an assessment of the requirements of the P2PE Standard that are affected by the change. Details of the tests which must be performed are available from the PCI SSC website. For device changes, a subset of Domain 1 tests will be required; for application changes, a subset of Domain 2 tests will be required;

(ii) The P2PE Assessor must produce a *Designated Change Assessment Report* and document the testing completed per PCI SSC requirements;

(iii) The P2PE Solution Provider prepares and signs an Solution AOV and sends it to the P2PE Assessor;

(iv) The P2PE Assessor signs its concurrence on the Solution AOV and forwards it, along with the P2PE Solution's updated *P2PE Instruction Manual* and the *Designated Change Assessment Report* to PCI SSC; and

(v) PCI SSC will then review the Solution AOV and the *Designated Change Assessment Report* for quality assurance purposes.

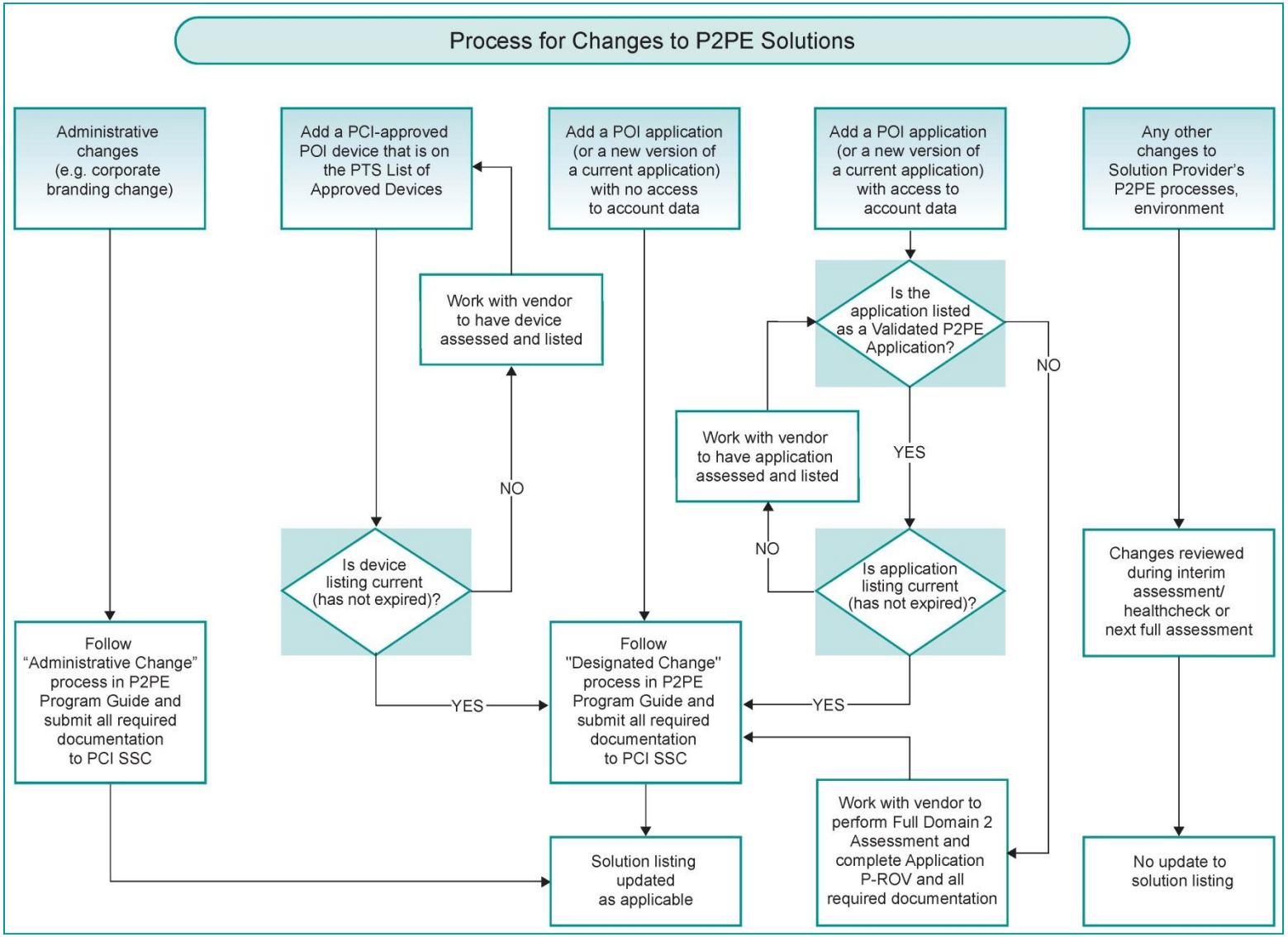
If the P2PE Assessor does not agree with the P2PE Solution Provider that the change, as documented in the *Solution Provider Change Analysis*, is eligible as a Designated Change, the P2PE Assessor must return the *Solution Provider Change Analysis* to the P2PE Solution Provider and should work with them to consider what actions are necessary to address the P2PE Assessor's observations.

Following successful PCI SSC quality assurance review of a Designated Change:

- An invoice for the *Designated Change Fee* will be issued to the P2PE Solution Provider; and
- Upon payment of the invoice to PCI SSC as described in *Validation Maintenance Fees* below, PCI SSC will: (i) update the List of Validated P2PE Solutions on the PCI SSC website accordingly with the new information; and (ii) sign and return a copy of the Solution AOV to both the P2PE Solution Provider and the P2PE Assessor. The Revalidation Date and Expiry Date of this P2PE Solution will remain unchanged i.e. a designated change has no impact on the Revalidation Date or Expiry Date of a listed P2PE Solution. PCI SSC will communicate quality issues associated with any aspect of the submission to the P2PE Assessor, and those issues are resolved according to the process depicted in Figure 2. PCI SSC reserves the right to reject any *Designated Change Assessment Report* if it determines that a change described therein and purported to be a Designated Change is ineligible for treatment as such

The process flow for changes to Listed P2PE Solutions is illustrated in Figure 1, below.

Figure 1: Changes to Listed P2PE Solutions



5.3 Validation Maintenance Fees

If a listed P2PE Solution is revised, the P2PE Solution Provider is required to pay the applicable *Change Fee* (all P2PE Program Fees are posted on the PCI SSC website) to PCI SSC immediately prior to Acceptance of each such change.

For any Administrative or Designated Change to a Validated P2PE Solution, the applicable fee will be invoiced immediately prior to Acceptance, and must be received by PCI SSC for the change to be Accepted and added to PCI SSC's List of Validated P2PE Solutions. Upon Acceptance, PCI SSC will sign and return a copy of the Solution AOV to both the P2PE Solution Provider and the P2PE Assessor.

All P2PE Program fees are non-refundable and are subject to change upon posting of revised fees on the PCI SSC website.

Note:

The P2PE Solution Provider pays all P2PE Assessment related fees directly to the P2PE Assessor (these fees are negotiated between the P2PE Solution Provider and the P2PE Assessor).

PCI SSC will invoice the P2PE Solution Provider for all Validation Maintenance Fees and the P2PE Solution Provider will pay these fees directly to PCI SSC.

A P2PE Solution must be listed on the List of Validated P2PE Solutions and not have reached its Expiry Date in order to have a change accepted and listed.

5.4 Notification Following a Security Breach, Compromise, or Known or Suspected Vulnerability

P2PE Solution Providers must promptly notify PCI SSC upon becoming aware of any actual or suspected vulnerability, security compromise or breach of any of their listed P2PE Solutions that the P2PE Solution Provider in good faith believes jeopardizes or could reasonably be expected to jeopardize the security of account data (each a "Security Issue").

5.4.1 Notification and Timing

Notwithstanding any other legal obligations the P2PE Solution Provider may have, they must promptly notify PCI SSC of any Security Issue relating to any of their listed P2PE Solutions, in accordance with the P2PE VRA.

Note: *Notification must take place no later than 24 hours after the P2PE Solution Provider first discovers the Security Issue.*

5.4.2 Notification Format

Formal notification to PCI SSC must be in writing in accordance with the P2PE VRA, and should be preceded by a phone call to the PCI SSC P2PE Program Manager.

5.4.3 Notification Details

As part of the initial notification to PCI SSC, the P2PE Solution Provider must supply the PCI SSC P2PE program manager with the information required by the P2PE VRA. At a minimum, this must include:

- The name, PCI SSC approval number and any other relevant identifiers of the P2PE Solution;
- A description of the general nature of the Security Issue;
- The P2PE Solution Provider's good faith assessment, to its knowledge at the time, as to the severity of the vulnerability or vulnerabilities associated with the Security Issue (using CVSS scoring or an alternative industry accepted standard that is reasonably acceptable to PCI SSC); and

- The P2PE Solution Provider's good faith determination, based on its knowledge at the time, as to whether the Security Issue is a Unique Security Issue (defined in the P2PE VRA).

5.4.4 Actions following a Security Breach or Compromise

In the event of PCI SSC being made aware of a Security Issue related to a Validated P2PE Solution, PCI SSC may take the actions specified in the P2PE VRA, and additionally, may:

- Notify Participating Payment Brands that a Security Issue has occurred.
- Communicate with the applicable P2PE Solution Provider about the Security Issue and, where possible, share information relating to the Security Issue.
- Support the P2PE Solution Provider's efforts to try and mitigate or prevent further Security Issues.
- Support the P2PE Solution Provider's efforts to correct any Security Issues.
- Work with the P2PE Solution Provider to communicate and cooperate with appropriate law enforcement agencies to help mitigate or prevent further Security Issues.

5.4.5 Withdrawal of Acceptance

PCI SSC reserves the right to suspend, withdraw, revoke, cancel or place conditions upon its Acceptance of (and accordingly, remove from the *List of Validated P2PE Solutions*) any listed P2PE Solution in accordance with the P2PE VRA, including but not limited to, when it is clear that the P2PE Solution does not offer sufficient protection against current threats and does not conform to the requirements of the P2PE Program, when the continued Acceptance of the P2PE Solution represents a significant and imminent security threat to its users, or if PCI SSC determines that the P2PE Solution is subject to a Security Issue.

6 P2PE Assessor Reporting Considerations

This section is focused on P2PE Assessors that have achieved the designated qualifications to submit P-ROVs for P2PE Solutions or P2PE Applications.

If a P2PE Solution Provider wishes to have its P2PE Solution included on the PCI SSC website List of Validated P2PE Applications then a corresponding Solution P-ROV must be submitted to PCI SSC by a P2PE Assessor for review and Acceptance. All P-ROVs which are to be submitted to PCI SSC for review must be submitted via the Portal.

6.1 P-ROV Acceptance Process

Note that all P-ROVs and other materials must be submitted to PCI SSC in English or with certified English translation.

The P2PE Assessor performs the P2PE Solution Assessment in accordance with the P2PE Standard, and produces a P-ROV that is shared with the P2PE Solution Provider. If the P-ROV has all items in place, then the P2PE Assessor submits the P-ROV, the Solution AOV and the signed P2PE VRA, and all other required materials to PCI SSC. If the P-ROV does not have all items "in place," then the P2PE Solution Provider must address those items highlighted in the P-ROV prior to submission to PCI SSC. For example, this may include updating documentation or updating configuration options or changing cryptographic key-management practices. Once the P2PE Assessor is satisfied that all documented issues have been resolved by the P2PE Solution Provider and all items "in place," the P2PE Assessor submits the P-ROV to PCI SSC for review, along with the completed and signed P2PE VRA and all other required materials.

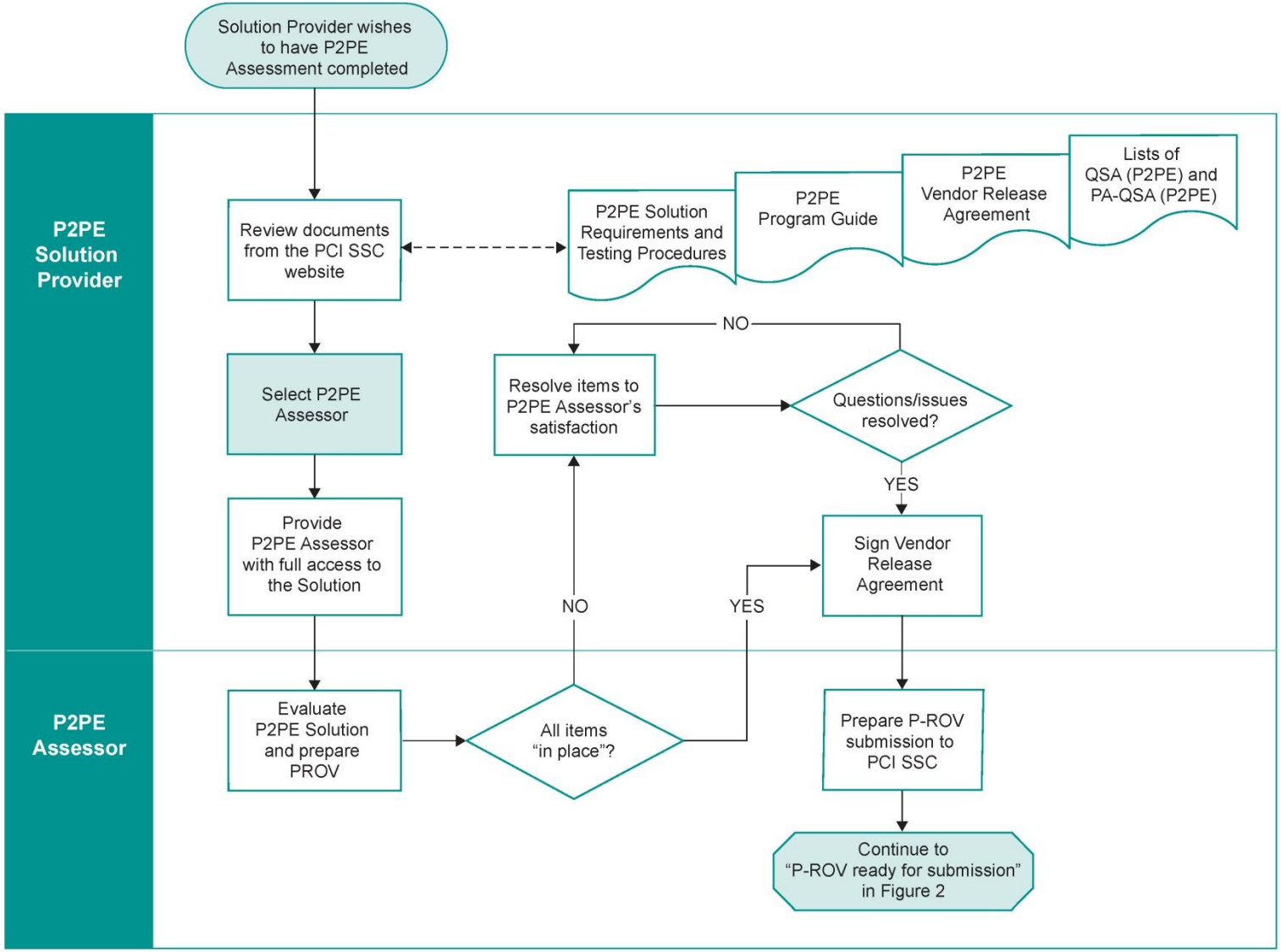
Once PCI SSC receives the P-ROV and all other required materials, the submission is reviewed from a quality assurance perspective. If the P-ROV meets all applicable quality assurance requirements (as documented in the *QSA Qualification Requirements* and related P2PE Program materials), and the P2PE Solution Provider has paid the applicable fees for the corresponding P2PE Solution, then PCI SSC sends a P2PE Solution AOV, countersigned by PCI SSC, to both the P2PE Solution Provider and the P2PE Assessor, and then adds the product to the *List of Validated P2PE Solutions.*

PCI SSC communicates any quality issues associated with P-ROVs to the P2PE Assessor, and it is then the responsibility of the P2PE Assessor to resolve those issues with PCI SSC and/or the P2PE Solution Provider, as applicable. Such issues may be limited or more extensive. Limited issues could simply require updating the P-ROV to reflect adequate documentation to support the P2PE Assessor's decisions. More extensive issues might require that the P2PE Assessor perform further testing, requiring the P2PE Assessor to notify the P2PE Solution Provider that re-testing is needed and schedule that testing with the P2PE Solution Provider.

The process flow for P-ROV Acceptance is illustrated in Figure 2, below.

.

Figure 2: P-ROV Acceptance Process



6.2 Delivery of the P-ROV and Related Materials

All documents required to be submitted to PCI SSC in connection with the P2PE validation process must be submitted to PCI SSC, by the P2PE Assessor, on behalf of the P2PE Solution Provider, through the Portal. Council staff pre-screen Portal submissions to ensure that all required documentation has been included and the basic submission requirements have been satisfied.

There must be consistency between the information in documents submitted for review via the Portal and the 'Details' fields within the Portal. Common errors in submissions include inconsistent application names or contact information and incomplete or inconsistent documentation. Incomplete or inconsistent submissions may result in a significant delay in the processing of requests for listing and/or may not be accepted for review by PCI SSC.

The Portal maintains a first-in-first-out order to all submissions while they await review by the Council. Should a new submission be intended as a replacement for a previously validated P2PE Solution with known vulnerabilities, the Portal allows such submissions to be brought forward for immediate review.

The Portal is also used by the Council to track all communications relating to a particular submission

6.2.1 Access to the Portal

Once a P2PE Assessor has had its first employee successfully complete the individual P2PE Assessor certification process, PCI SSC will send login credentials and instructions for use of the Portal to the company's Primary Contact. Additional credentials can be requested by each company's Primary Contact through PCI SSC's P2PE Program Manager. Portal credentials may be issued to any employee of a P2PE Assessor and are not limited to P2PE Assessors.

6.2.2 New P2PE Solutions

For all initial submissions to PCI SSC, the P2PE Assessor must submit the following by uploading to the Portal:

- Completed P-ROV which contains the following information:
  - Executive Summary (Includes Reseller/Integrator List).
  - Requirements – Testing Procedures.
- Solution AOV signed by both the P2PE Solution Provider and the P2PE Assessor.
- *P2PE Instruction Manual* for the assessed P2PE Solution.
- Current version of P2PE VRA signed by the P2PE Solution Provider together with any related documentation.

6.2.3 Resubmissions

For subsequent reviews, if multiple iterations of a P-ROV are required before PCI SSC can accept the report; the P2PE Assessor must submit P-ROV versions that include tracking of cumulative changes within the document.

6.2.4 Administrative Changes

For all submissions of an Administrative Change to an already listed P2PE Solution, the P2PE Assessor must submit the following documents through the Portal.

- *Solution Provider Change Analysis* document

- Updated *P2PE Instruction Manual* for the assessed P2PE Solution
- Solution AOV signed by both the P2PE Solution Provider and the P2PE Assessor
- If requested by PCI SSC, current version of P2PE VRA, together with any related documentation

6.2.5 Designated Changes

For all submissions of a Designated Change to an already listed P2PE Solution, the P2PE Assessor must submit the following documents through the Portal.

- *Solution Provider Change Analysis* document
- Specified testing documentation, dependent on the type of change
- Updated *P2PE Instruction Manual* for the assessed P2PE Solution
- Solution AOV signed by both the P2PE Solution Provider and the P2PE Assessor
- If requested by PCI SSC, current version of P2PE VRA, together with any related documentation

6.3 P2PE P-ROV Review Process

PCI SSC will base Acceptance of a P2PE Solution primarily on the results documented in the P-ROV. Upon receipt of the P-ROV, the following will apply:

- PCI SSC shall review the P-ROV (generally within 30 calendar days of receipt) and determine if it is acceptable.
- If no issues or questions for the P2PE Assessor are identified, PCI SSC shall bill the P2PE Solution Provider for the applicable Acceptance or change fee. Once the fee is received, PCI SSC will issue the Solution AOV, countersigned by PCI SSC, post the P2PE Solution and P2PE Solution Provider's information to the PCI SSC website, and the P2PE Solution is thereby Accepted.
- If questions or issues are identified and sent to the P2PE Assessor, the process described above will restart upon receipt of a complete and acceptable revised P-ROV or response ("Revised P-ROV") from the P2PE Assessor. PCI SSC reserves the right to ask for additional supporting documentation that may be necessary to substantiate the findings documented in the P-ROV. The process re-start does not occur until receipt of an acceptable Revised P-ROV addressing all previously identified items. PCI SSC will generally review a Revised P-ROV within 30 calendar days of receipt.
- Should additional questions or issues arise, the cycle repeats until a satisfactory Revised P-ROV is received, at which time, subject to receipt of the applicable Acceptance or change fee, PCI SSC will issue the Solution AOV, post the information to the PCI SSC website, and the P2PE Solution is thereby Accepted. Additional issues or questions may be raised at any time prior to Acceptance.
- P-ROVs that have been returned to the P2PE Assessor for correction must be resubmitted to PCI SSC within 30 days. If this is not possible, the P2PE Assessor must inform PCI SSC of the timeline for response. Lack of response on P-ROVs returned to the P2PE Assessor for correction may result in the submission being closed. Submissions that have been closed will not be reopened and must be resubmitted as if they are new P-ROV submissions.

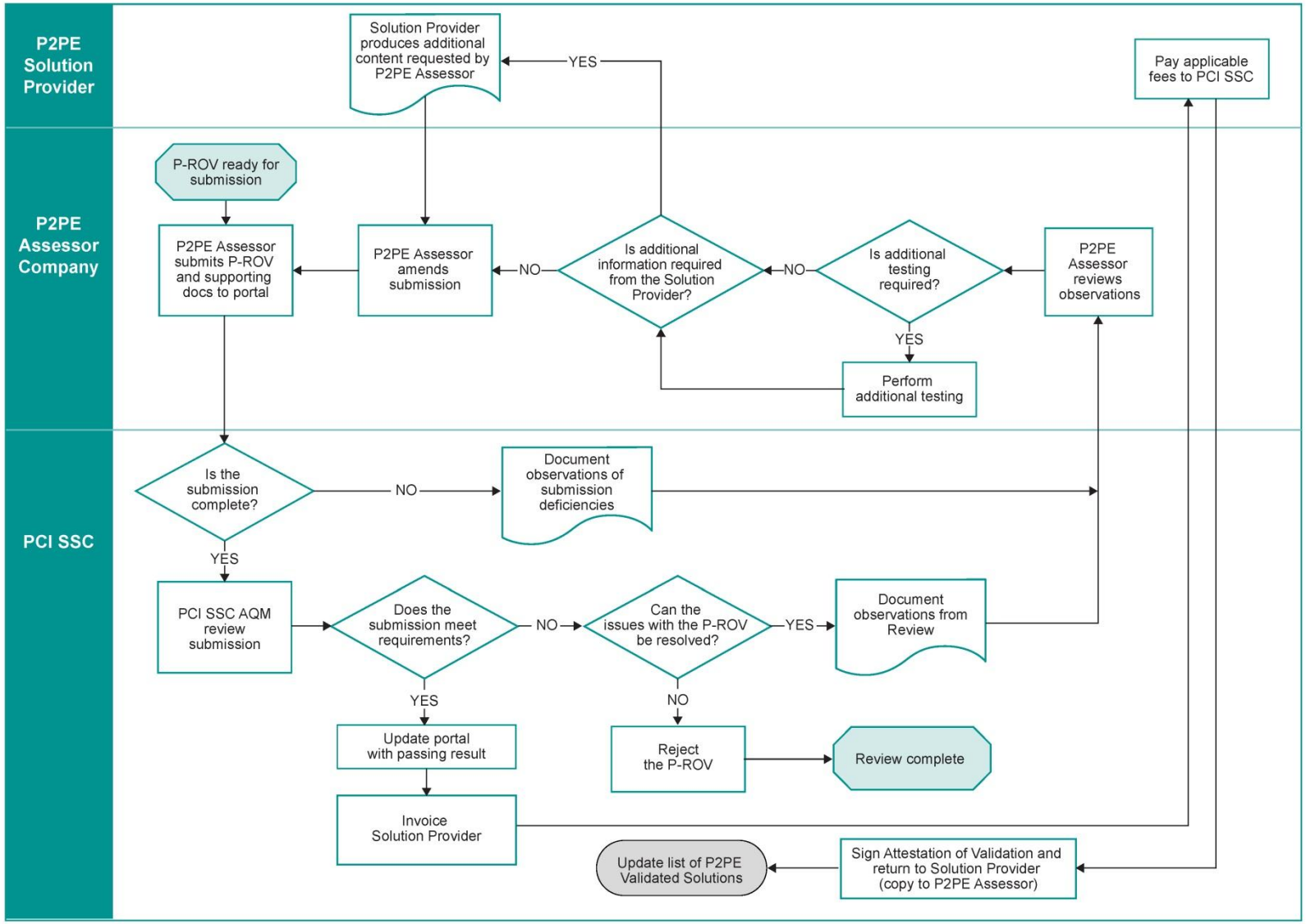
For reports related to changes to existing listed P2PE Solutions, based on the P2PE Solution Provider's Attestation of Validation, the above P2PE Solution P-ROV Acceptance process is the same, and PCI SSC shall issue a revised Solution AOV and post the revised information to the PCI SSC website unless issues or questions arise, in a manner similar to the aforementioned.

The process flow for P-ROV reviews is illustrated in Figure 3, below.

The information shown on the List of Validated P2PE Solutions is specified in Appendix B, "Elements for List of Validated P2PE Solutions."

Refer to Appendix C for the information included in the listing of the List of Validated P2PE Applications.

Figure 3: P-ROV Review Process



6.4 Assessor Quality Management Program

PCI SSC reviews P-ROVs and P2PE Assessor performance for quality assurance purposes. As stated in the *QSA Qualification Requirements – Supplement for Point-to-Point Qualified Security Assessors* and the *P2PE QSA Agreement*, P2PE Assessors are required to meet all quality assurance standards set by PCI SSC. The various phases of the assessor quality management program are described below.

The process flow for the Assessor Quality Management program is detailed in Figure 2.

6.4.1 Outcomes of a P-ROV Review

Quality assurance reviews of P-ROVs will result in one of following outcomes:

- The P2PE Solution is determined to be ineligible for Acceptance under the P2PE Program and the P-ROV will not be Accepted; or
- The P2PE Solution is determined to be eligible for Acceptance under the P2PE Program and therefore the P-ROV will be reviewed and determined to either:
    - Meet the requirements of the P2PE Program; or
    - Not meet the requirements of the P2PE Program in which case all identified issues with the P-ROV must be resolved before the P-ROV review can be completed.

6.4.2 Types of P-ROV Reviews

The type of review done on a particular P-ROV submission is determined by the status of the P2PE Assessor (see Section 6.4.4 below on "P2PE Assessor Status") and is variable at the discretion of PCI SSC.

6.4.2.1 Full Reviews

This level of review examines all aspects of the P-ROV submission and accompanying documents. The purpose is to ensure that P2PE Assessors are given detailed feedback and guidance.

6.4.2.1 Detailed Full Reviews with Work Papers

This level of review examines all aspects of the P-ROV submission and the supporting documentation and information that was either provided to the P2PE Assessor by the P2PE Solution Provider or created by the P2PE Assessor as a result of the assessment process. The purpose is to establish confidence in the efforts taken by the P2PE Assessor to reach their assessment of the subject P2PE Solution and to provide detailed feedback and guidance.

6.4.3 P2PE Assessor Audit Program

The P2PE Assessor audit program helps to ensure that the overall quality of report submissions remains at a level that is consistent with the general objectives of the P2PE Program Guide, and that P2PE Assessors are reviewing and validating P2PE Solutions consistent with P2PE Program requirements.

Each calendar year all P2PE Assessors submitting reports to PCI SSC are subject to an audit of their submissions.

The audit process is a more formalized method of review involving a robust evaluation of the P2PE Assessor's work. The audit will evaluate the work product of the P2PE Assessor for a set of P-ROVs and related materials. The audit process will encompass the report submission (P-ROV), along with an evaluation of work papers and the P2PE Assessor's internal Quality Assurance manual. This will help to ensure the organization's internal Quality Assurance processes are being followed. Additionally, the

P2PE Instruction Manual and/or other supporting documents pertaining to the P2PE Solution under audit will be reviewed. Finally, PCI SSC may at its discretion conduct onsite audits.

6.4.4 P2PE Assessor Status

The P2PE Assessor quality assurance program recognizes three (3) quality status levels for P2PE Assessors. The quality status level of a P2PE Assessor is determined by PCI SSC based on review of submissions, feedback from clients and/or Participating Payment Brands and compliance with P2PE Program requirements.

These levels are not progressive. A P2PE Assessor may move directly from “In Good Standing” to “Revocation” if warranted.

At any of these status levels, PCI SSC may require an onsite visit with the P2PE Assessor to audit their internal Quality Assurance program, at the expense of the P2PE Assessor.

Note: if a P2PE Solution included on the PCI SSC *List of Validated P2PE Solutions* is compromised due to P2PE Assessor error, then that P2PE Assessor may immediately be placed into Remediation.

The P2PE Assessor quality status levels used by the Council are as follows:

6.4.4.1 P2PE Assessor In Good Standing

This is the “normal” status that most P2PE Assessors are expected to hold for the majority of their time participating in the P2PE Program. A P2PE Assessor that is "In Good Standing” will usually have full reviews completed on their P-ROV submissions and will be subject to periodic audit by PCI SSC.

6.4.4.2 Remediation

PCI SSC may place a P2PE Assessor into Remediation if significant quality problems are detected. Remediation is a mandatory program. If the Council determines that Remediation is warranted, the P2PE Assessor must participate in Remediation in order to continue to participate in the P2PE Program. A P2PE Assessor that is in Remediation is required to submit its Quality Assurance Manual to PCI SSC for review and may be asked to submit other documentation such as work papers for some or all of its P-ROV submissions.

A P2PE Assessor in Remediation must also submit a Remediation plan to PCI SSC, detailing how the P2PE Assessor plans to improve quality of its P-ROVs.

Additional detail is communicated to the P2PE Assessor as to what corrective actions need to be taken to improve the overall quality of submissions, and a PCI SSC representative will provide support on a case management basis. PCI SSC will also require each P2PE Assessor in Remediation to evidence lessons learned from Remediation by submitting an updated Quality Assurance Manual to PCI SSC.

So long as the P2PE Assessor participates in Remediation, and complies with the requirements thereof, the P2PE Assessor may continue to participate in the P2PE Program as a P2PE Assessor (subject to the terms of its Remediation).

If PCI SSC determines that the P2PE Assessor has made sufficient improvement during the Remediation process, its In Good Standing status will be reinstated. If PCI SSC determines that the P2PE Assessor has failed to meet applicable requirements or quality standards during Remediation, then the P2PE Assessor will be subject to Revocation.

P2PE Assessors are expected to complete Remediation within 90 days. In the event that the goals of the Remediation program cannot be achieved within this period, Remediation may be extended once by an additional 90 days, but only if the P2PE QSA has been able to demonstrate sufficient positive progress.

PCI SSC will charge a P2PE Assessor Remediation Program Fee for entry into the Remediation Program and a Detailed P-ROV Review Fee for all reports submitted and resubmitted during Remediation. Please refer to the PCI SSC website for pricing information.

The PCI SSC website will be updated to show that the P2PE Assessor is in Remediation status.

6.4.4.3 Revocation

Serious quality problems may result in revocation of P2PE Assessor qualification. When a P2PE Assessor qualification is revoked, the P2PE Assessor is removed from the List of approved P2PE Assessors and is no longer eligible to perform P2PE Assessments, process P-ROVs, or otherwise participate in the P2PE Program; provided, that if and to the extent approved by PCI SSC in writing, the P2PE Assessor will be required to complete any P2PE Solution Assessments for which it was engaged prior to the effective date of the Revocation. The P2PE Assessor may appeal the Revocation, but unless otherwise approved by PCI SSC in writing in each instance, will not be permitted to perform P2PE Solution Assessments, process P-ROVs, or otherwise participate in the P2PE Program until it has demonstrated to PCI SSC's satisfaction that it meets all applicable QSA, P2PE Assessor, and, if applicable, PA-QSA requirements as documented in *QSA Qualification Requirements – Supplement for Point-to-Point Encryption Security Assessors* and relevant PCI SSC program documents.

Appendix A: P2PE Solutions and Acceptance

Acceptance of a given P2PE Solution by the PCI Security Standards Council, LLC (PCI SSC) only applies to the specific P2PE Solution, all of the components of which have been reviewed by a P2PE Assessor and subsequently accepted by PCI SSC (the "Accepted Version"). If any aspect of a P2PE Solution is different from that which was reviewed by the P2PE Assessor and accepted by PCI SSC—even if the different P2PE Solution (the "Alternate Version") conforms to the basic product description of the Accepted Version—then the Alternate Version should not be considered accepted by PCI SSC, nor promoted as accepted by PCI SSC.

No P2PE Solution Provider or other third party may refer to a P2PE Solution as "PCI Approved," or "PCI SSC Approved" nor otherwise state or imply that PCI SSC has, in whole or part, approved any aspect of a P2PE Solution Provider or its P2PE Solution, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with PCI SSC, or in a P2PE Solution AOV provided by PCI SSC. All other references to PCI SSC's acceptance of a P2PE Solution are strictly and actively prohibited by PCI SSC.

When granted, PCI SSC acceptance is provided to ensure certain security and operational characteristics important to the achievement of PCI SSC's goals, but such acceptance does not under any circumstances include or imply any endorsement or warranty regarding the P2PE Solution Provider or the functionality, quality, or performance of the P2PE Solution or any other product or service. PCI SSC does not warrant any products or services provided by third parties. PCI SSC acceptance does not, under any circumstances, include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services that have received acceptance from PCI SSC shall be provided by the party providing such products or services, and not by PCI SSC or any Participating Payment Brand.

Appendix B: Elements for the *List of Validated P2PE Solutions*

P2PE Solution Vendor

This entry denotes the **P2PE Solution Vendor** for the validated P2PE Solution.

P2PE Solution Identifier

The **P2PE Solution Identifier** is used by PCI SSC to denote relevant information for each Validated P2PE Solution, consisting of the following fields (fields are explained in detail below):

- P2PE Solution Name
- Reference Number

Example of a P2PE Solution Identifier:

Component	Description
Solution Name	Acme Payment 600
Reference #	2012-00021.002

P2PE Solution Identifier: Detail

- **P2PE Solution Name**

  P2PE Solution Name is provided by the P2PE Solution Provider, and is the name by which the P2PE Solution is sold.

- **Reference Number**

  PCI SSC assigns the Reference number once the Validated P2PE Solution is posted to the PCI SSC website; this number is unique per P2PE Solution and will remain the same for the life of the listing.

  An example reference number is 2012-XXXXX.XXX consisting of the following:

Field	Format
Year of listing	4 digits + hyphen
Solution Provider #	5 digits + period (assigned alphabetically initially, then as received)
Individual Solution Number #	3 digits

Validated According To

"Validated According To" is used by PCI SSC to denote what standard, and the specific version thereof, that was used to assess the compliance of a Validated P2PE Solution.

P2PE Assessor

This entry denotes the name of qualified **P2PE Assessor** that performed the validation and determined that the P2PE Solution is compliant with the P2PE Standard.

Revalidation Date

The **Revalidation Date** is used by PCI SSC to indicate when the P2PE Solution Provider's annual Solution AOV is due. The Annual Revalidation is part of the Solution AOV form, located on the PCI SSC website.

Expiry Date

The **Expiry Date** for Validated P2PE Solution is the date by which the P2PE Solution Provider must have the P2PE Solution re-evaluated against the current P2PE Standard in order to maintain the acceptance.

Description Provided by Vendor

This section allows for the submission of a description of the P2PE Solution that is to be used in the List of Validated P2PE Solutions should the P-ROV be accepted.

PCI-approved POI Devices

This section identifies the PCI-approved POI devices validated for use with this P2PE Solution. Identification must include specific version/firmware and/or hardware identifiers and any relevant PCI PTS reference numbers.

The Expiry Date shown is the expiry date of the PTS approval for this device. If the expiry date is in the past this will be denoted by a color change. A website link will be provided to the appropriate entry on the List of Approved PIN Transaction Security Devices.

P2PE Applications

This section provides a list of all software applications used in the P2PE Solution which have been evaluated per all P2PE Domain 2 Requirements i.e. those which have access to clear text account data.

For those applications which are separately validated to Domain 2 per Appendix D:

- A website link will be provided to the appropriate entry on the List of P2PE Validated Applications
- The Revalidation Date shown is the annual revalidation date of the Application P-ROV acceptance for this application. If the expiry date is in the past this will be denoted by a color change
- The Expiry Date shown is the expiry date of the Application P-ROV acceptance for this application. If the expiry date is in the past this will be denoted by a color change

For those applications evaluated only as part of the P2PE Solution, the Revalidation Date and Expiry Date are the same as for the P2PE Solution.

Other Validated Applications

This section provides a list of all software applications used in the P2PE Solution that have been assessed against P2PE Domain 2 Requirements to confirm they do not have access to clear-text account data within the P2PE Solution.

These applications do not have Revalidation Date and Expiry Date shown separately as they are evaluated only as part of the overall P2PE Solution Assessment.

Appendix C: Listing of Applications Used In Validated P2PE Solutions

All applications used in P2PE Solutions must be evaluated by a PA-QSA (P2PE).

C.1 Applications without Access to Clear Text Account Data

For applications which do not have access to clear text account data, only Requirement 2A-3 is applicable. These tests are completed as part of each P2PE Solution Assessment by a PA-QSA (P2PE) and validate that these applications are not accessing clear-text account data, and are not bypassing or overriding any security features provided by the other approved components of the P2PE Solution. Such applications are listed only as components of validated P2PE Solutions and are not eligible for inclusion in the List of Validated P2PE Applications.

C.2 Applications with Access to Clear Text Account Data

Applications which have access to clear-text account data must be evaluated against all P2PE Domain 2 Requirements.

Domain 2 testing procedures falls into two categories; Application Developer and Solution Provider.

Application Developer testing procedures can be validated by a PA-QSA (P2PE) outside of a full P2PE Solution.

P2PE Solution Provider testing procedures validate that the application is correctly configured and integrated into a P2PE Solution. These procedures cannot therefore be validated standalone and must be tested by a PA-QSA (P2PE) for each application in each P2PE Solution.

An Application Vendor may choose to:

a) Include the application in the List of Validated P2PE Applications.

This is subject to acceptance by PCI SSC of an Application P-ROV completed by a PA-QSA (P2PE) validating the Domain 2 Application Developer testing procedures, an Application AOV, and all applicable fees.

OR

b) Include the application only as part of a Validated P2PE Solution.

This may be appropriate if the application is used only in one P2PE Solution. The application is still subject to full validation per all P2PE Domain 2 Requirements and this must be documented in a P-ROV submitted as part of the overall P2PE Solution submission. The application must undergo full re-assessment by a PA-QSA (P2PE) every two years as part of the P2PE Solution re-assessment described in Section 5.2 of this document.

C.3 List of Validated P2PE Applications

PCI SSC website has a List of Validated P2PE Applications; an entry on this list indicates that Domain 2; Application Developer testing procedures have been validated by a PA-QSA (P2PE) and a P-ROV confirming this has been accepted by PCI SSC. Appendix D shows the elements for the *List of Validated P2PE Applications.* The application listing entry shows the devices and firmware the application was tested on as part of the validation process.

C.3.1 Managing an Application included in the List of Validated P2PE Application

C.3.1.1 Annual Revalidation

Annually, by the revalidation date noted on the List of Validated P2PE Applications, the application vendor is **required** to submit an updated Application AOV, performing the "Annual Revalidation" steps.

This annual process has been adopted to encourage vendors to not only reaffirm that there have been no updates to the application (if applicable), but also to encourage vendors to periodically consider whether updates are necessary to address changes to the external threat environment in which the application operates. If changes to the threat environment do necessitate changes to the payment application, the product should be updated accordingly and reassessed by a PA-QSA (P2PE), preferably the PA-QSA (P2PE) that originally validated the application for P2PE compliance.

If an updated Application AOV is not submitted for a listed application, that application will be subject to an early administrative expiry. As such, the List of Validated P2PE Applications will be updated to identify this by showing the application in **Orange** color for up to 60 days. If the updated Application AOV is received within this 60 day period PCI SSC will, providing it is completed as above, update the List of Validated P2PE Applications with the new revalidation date and remove the **Orange** status. If the updated Application AOV is not received within 60 days the List of P2PE Validated Applications will be updated to show the application in **Red**. A fee may be levied if the vendor wishes to revalidate the applications more than 60 days later than the Revalidation Date.

As there are no specific fees associated with Annual Revalidations, PCI SSC will upon receipt of the updated Attestation of Validation:

(i) review the submission for completeness;
(ii) once completeness is established, update the List of Validated P2PE Applications with the new revalidation date; and
(iii) sign and return a copy of the updated Application AOV to both the vendor and the PA-QSA (P2PE).

C.3.1.2 Changes to Listed P2PE Applications

Changes may be submitted at any time during an application's current listing. Changes cannot be submitted for expired application listings. For listed P2PE applications there are essentially two types of change scenarios.

(i) **No impact changes** are minor changes (either administrative or software) made to a listed P2PE application that have no impact on compliance with the P2PE Standard. Examples of no-impact updates include, but are not limited to, corporate identify changes or software changes to a graphical user interface or to parts of the application that have no impact to any P2PE functionality.

For the new version to be listed, the application vendor documents the change for the P2PE (PA-QSA)'s review in an Application Vendor Change Analysis. Following review and concurrence by the PA-QSA (P2PE) this is submitted together with an updated Application AOV and, if appropriate, revised *Implementation Guide*, for review and acceptance by PCI SSC quality assurance.

The applicable fee will be invoiced immediately prior to Acceptance, and must be received by PCI SSC for the change to be Accepted and added to PCI SSC's List of Validated P2PE Applications. Upon Acceptance, PCI SSC will sign and return a copy of the Application AOV to both the application vendor and the P2PE Assessor.

The application validation and expiry dates are not affected by this type of change.

(ii) **Changes which have an impact on compliance with requirements of the P2PE Standard or P2PE functionality** require a full re-assessment against P2PE Domain 2 Requirements. This requires preparation and submission to PCI SSC of an Application P-ROV. Essentially this scenario is treated as a new P2PE application. Upon acceptance by PCI SSC of an appropriate Application P-ROV and Application AOV, and receipt of all applicable fees the Listing of Validated P2PE Applications will be updated with new application validation and expiry dates.

C.3.1.3 Renewing Expired P2PE Applications

As an application approaches its expiration date, PCI SSC will notify the vendor of the pending expiration. The two options available for application vendor consideration are full review or expiry:

(i) **Full Review**: If the vendor intends to continue to sell the application then the vendor contacts a PA-QSA (P2PE) and has the application fully re-evaluated against the then current version of the P2PE Standard.

(ii) **Expiry**: In all other situations (e.g. the vendor indicates that it does not intend to continue selling the application or has gone out of business, or otherwise fails to submit the application for full re-assessment by the expiration date), PCI SSC will update the List of Validated P2PE Applications to identify this by showing the application in **Orange** color for up to 60 days. If a new assessment documented in an Application P-ROV is received within this 60-day period PCI SSC will, providing the P-ROV is accepted, update the List of Validated P2PE Applications with the new expiry date and revalidation dates and remove the **Orange** status. If the new assessment documented in an Application P-ROV is not received within 60 days the List of P2PE Validated Applications will be updated to show the application in **Red.** A fee may be levied if the vendor wishes to revalidate the applications more than 60 days later than the Expiry Date.

Appendix D: Elements for the *List of Validated P2PE Applications*

P2PE Application Vendor

This entry denotes the Application Vendor for the validated P2PE application.

P2PE Application Identifier

The **P2PE Application Identifier** is used by PCI SSC to denote relevant information for each validated P2PE application, consisting of the following fields (fields are explained in detail below):

- P2PE Application Name
- P2PE Application Version #
- Reference Number

Example of a P2PE Application Identifier:

Component	Description
Application Name	Acme Payment 600
Application Version #	PCI 4.53
Reference #	2012-00111.001

P2PE Application Identifier: Detail

- **P2PE Application Name**

  P2PE Application Name is provided by the Application Vendor, and is the name by which the application is sold.

- **P2PE Application Version #**

  P2PE Application Version # represents the specific application version reviewed in the P2PE Assessment against P2PE Domain 2 Requirements. The format is set by the vendor and may consist of a combination of fixed and variable alphanumeric characters.

- **Reference Number**

  PCI SSC assigns the Reference number once the Validated P2PE Application is posted to the PCI SSC website; this number is unique per Application and will remain the same for the life of the listing.

  An example reference number is 2012-XXXXX.XXX.AAA, consisting of the following:

Field	Format
Year of listing	4 digits + hyphen
Application Vendor #	5 digits + period (assigned alphabetically initially, then as received)
Application Vendor App #	3 digits (assigned as received)
Minor version	3 alpha characters (assigned as received)

- **Description Provided by Vendor**

  This section allows for the submission of a description of the P2PE Application that is to be used in the List of Validated P2PE Applications should the P-ROV be accepted.

- **Tested Platforms/Operating Systems** This section identifies the PCI-approved POI devices validated for use with this P2PE Application. Identification must include specific version/firmware and/or hardware identifiers and any relevant PCI PTS reference numbers.

Validated According To

"Validated According To" is used by PCI SSC to denote what standard, and the specific version thereof, that was used to assess the compliance of a Validated P2PE Application.

Revalidation Date

The **Revalidation Date** is used by PCI SSC to indicate when the Application Vendor's annual Application AOV is due. The Annual Revalidation is part of the Application AOV form, located on the PCI SSC website.

Expiry Date

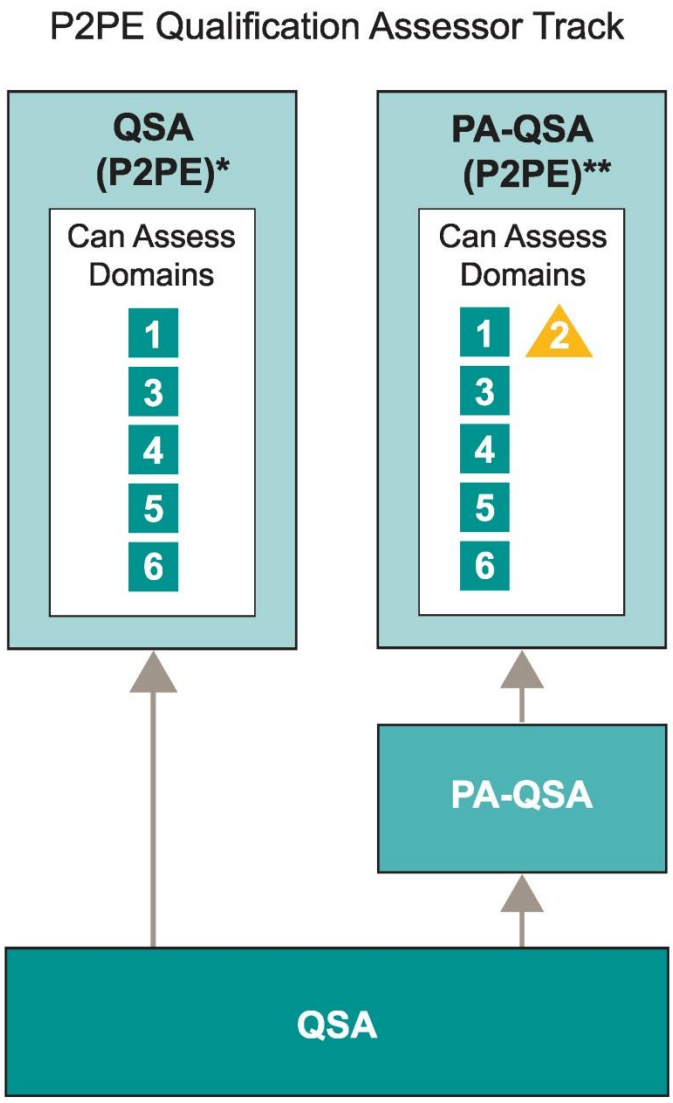
The **Expiry Date** for Validated P2PE Application is the date by which the Application Vendor must have the application re-evaluated against the then current P2PE Standard in order to maintain Acceptance.

PCI SSC will endeavor to update the P2PE Standard on a 36-month cycle. Acceptance for P2PE Validated Applications expires three years past the effective date of a subsequent update of the P2PE Standard. The objective is a three-year minimum approval life expectancy, barring a severe threat that may require immediate changes.

PA-QSA (P2PE)

This entry denotes the name of qualified P2PE Assessor that performed the validation and determined that the application is compliant with the P2PE Standard.

Appendix E: Types of QSAs and Applicability to the P2PE Standard



* P2PE Assessor must be a QSA, and P2PE Assessor employee must be a QSA employee.

** P2PE Assessor must be a PA-QSA, and P2PE Assessor employee must be a PA-QSA employee.