Payment Card Industry (PCI)

Point-to-Point Encryption (P2PE)

Program Guide

Version 2.0

September 2015

Document Changes

Date	Version	Description
June 2012	1.0	Initial Release of the *PCI P2PE Program Guide*
February 2013	1.1	Updated to reflect changes to Domain 2 assessments and changes to the evolving P2PE Program.
September 2015	2.0	Align to v2.0 of the P2PE Standard.

Table of Contents

1 Introduction

This document provides an overview of the PCI SSC Point-to-Point Encryption Standard program ("P2PE Program" or "Program") operated and managed by the PCI Security Standards Council, LLC ("PCI SSC"), and should be read in conjunction with the *P2PE Qualification Requirements* as well as those documents referenced in Section 1.2, "Related Publications," below. This Program Guide describes the following:

- Program Background (Section 1.1)
- P2PE Initiative and Overview (Section 1.4)
- Program Roles and Responsibilities (Section 2)
- Overview of the Validation Process (Section 3)
- Preparation for the Review (Section 4)
- Managing a Validated P2PE Listing (Section 5)
- Reporting Considerations (Section 6)
- Assessor Quality Management Program (Section 6.3)

1.1 Program Background

In response to requests from merchants and other members of the Payment Card Industry (PCI) for a unified set of point-to-point encryption security requirements, PCI SSC has adopted and maintains the *Point-to-Point Encryption Standard* (P2PE), the current version of which is available on the PCI SSC Website. When implemented appropriately, a P2PE Solution provides a rigorous defense against data exposure and compromise.

PCI SSC manages the Program, including the development, implementation, and maintenance of validated P2PE Products (P2PE Application, P2PE Component, or P2PE Solution).

Organizations qualified by PCI SSC to validate P2PE Solutions and P2PE Components on behalf of P2PE Vendors are referred to as Qualified Security Assessor P2PE Companies (QSA (P2PE) Companies), further described below. Organizations qualified by PCI SSC to validate P2PE Applications on behalf of Vendors are referred to as Payment Application Qualified Security Assessor P2PE Companies (PA-QSA (P2PE) Companies), further described below. The quality, reliability, and consistency of a QSA (P2PE) Company and/or PA-QSA (P2PE) Company's work provide confidence that the P2PE Solution, P2PE Component, and/or P2PE Application has been validated for P2PE compliance in accordance with the PCI P2PE Program.

1.2 Related Publications

The P2PE Program Guide should be used in conjunction with the latest versions of (or successor documents to) the following PCI SSC publications, each as available through the Website:

Document name	Description
Payment Card Industry (PCI) Point-to-Point Encryption Glossary of Terms, Abbreviations, and Acronyms (the "P2PE Glossary")	Separate glossary for specific use with the P2PE Standard.
PCI Point-to-Point Encryption Solution Requirements and Testing Procedures ("P2PE Standard")	The P2PE Standard lists and defines the specific technical requirements and assessment procedures.
PCI P2PE Report on Validation Reporting Template ("P-ROV Reporting Template")	The P-ROV Reporting Template is mandatory for completing a P2PE Report on Validation and includes detail on how to document the findings of a P2PE Assessment. There are several versions covering P2PE Solutions, P2PE Components, and P2PE Applications.
PCI P2PE Attestation of Validation ("P-AOV")	The P-AOV is a form for QSA (P2PE) and/or PA-QSA (P2PE) Companies to attest to the results of a P2PE Assessment, as documented in the P2PE Report on Validation. There are several versions covering P2PE Solutions, P2PE Components, and P2PE Applications.
PCI Qualification Requirements for Point-to-Point Encryption (P2PE) Qualified Security Assessors, QSA (P2PE) and PA-QSA (P2PE) (or "P2PE Qualification Requirements")	The P2PE Qualification Requirements are a baseline set of requirements that must be met by a QSA (P2PE) and/or PA-QSA (P2PE) Company and QSA (P2PE) and/or PA-QSA (P2PE) Employees in order to perform P2PE Assessments.
Vendor Release Agreement ("VRA")	The VRA establishes the terms and conditions under which validated P2PE Solutions, P2PE Components, and P2PE Applications are accepted and listed by PCI SSC.

The most current versions of the following additional documents are used in conjunction with the aforementioned:

- *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures* (PCI DSS)
- *Payment Card Industry (PCI) Payment Application Data Security Standard Requirements and Security Assessment Procedures* (PA-DSS)
- *Payment Card Industry (PCI) PIN Security Requirements*
- *Payment Card Industry (PCI) PTS Hardware Security Module (HSM) Security Requirements*
- *Payment Card Industry (PCI) PTS POI Modular Security Requirements*
- *Payment Card Industry (PCI) PTS Device Testing and Approval Program Guide*

- *Payment Card Industry (PCI) Data Security Standard and Payment Application Data Security Standard Glossary of Terms, Abbreviations, and Acronyms* (the "Glossary")

1.3 Updates to Documents and Security Requirements

It is necessary to regularly review, update, and improve the security requirements used to evaluate P2PE Solutions, P2PE Components, and P2PE Applications. PCI SSC provides interim updates to the PCI community through a variety of means including required training, e-mail bulletins, frequently asked questions (which may include technical/normative FAQs), 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, P2PE Component Providers, P2PE Application Providers, and P2PE Assessor Companies to help minimize the impact of any changes.

1.4 Terminology

Throughout this document the following terms have the meanings shown in the chart below.

Term	Meaning
Accepted, or listed	A P2PE Product is deemed to have been "Accepted" or "listed" (and "Acceptance" is deemed to have occurred) when PCI SSC has: (i) received the corresponding P-ROV from the P2PE Assessor Company; (ii) received the corresponding fee and all documentation required with respect to that P2PE Product as part of the Program; (iii) confirmed that the P-ROV is correct as to form (all applicable documents completed appropriately/sufficiently), the P2PE Assessor Company properly determined that the P2PE Solution, P2PE Component, or P2PE Application is eligible to be a P2PE Validated Solution, a P2PE Validated Component, or a P2PE Validated Application, the P2PE Assessor Company adequately reported the P2PE compliance of the P2PE Solution, P2PE Component, or P2PE Application in accordance with Program requirements, and the detail provided in the P-ROV meets PCI SSC's reporting requirements; and (iv) listed the P2PE Solution, P2PE Component, or P2PE Application on the List of Validated P2PE Solutions, List of Validated P2PE Components, or List of Validated P2PE Applications; provided that PCI SSC may suspend, withdraw, revoke, cancel, or place conditions upon (including without limitation, complying with remediation requirements) Acceptance of any P2PE Solution, P2PE Component, or P2PE Application in accordance with applicable P2PE Program procedures.
Application P-ROV	P-ROV covering a P2PE Application Assessment relating to a P2PE Application.
Component P-ROV	P-ROV covering a P2PE Component Assessment relating to a P2PE Component.

Term	Meaning
Delta Assessment	Partial P2PE Assessment performed against applicable P2PE Requirements when changes to a listed P2PE Application are eligible for review under the "Delta Assessment" change-review process described herein.
List of Validated P2PE Applications	The Council's authoritative List of Validated P2PE Applications appearing on the PCI SSC website.
List of Validated P2PE Components	The Council's authoritative List of Validated P2PE Components 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.
Listing	Refers to the listing and related information regarding a P2PE Solution on the List of Validated P2PE Solutions, a P2PE Component on the List of Validated P2PE Components, or a P2PE Application on the List of Validated P2PE Applications.
Merchant-managed Solution (or MMS)	A P2PE solution managed by a merchant rather than by a Third-Party Solution Provider. These merchant solutions are typically for large retail organizations who centrally manage the solution on behalf of their own encryption environments. In a merchant-managed solution, part of the merchant business plays the role of a P2PE solution provider (managing POIs, decryption environment, etc.), and part of the business plays the role of a "merchant" that has no access to clear-text account data, etc. Merchant-managed solutions are not eligible for PCI listing.
P-AOV	A P2PE Program *"Attestation of Validation"* declaring the P2PE Solution, P2PE Component, or P2PE Application's validation status against the P2PE Standard. ▪ The P2PE Solution AOV, signed by a QSA (P2PE) Company and the P2PE Solution Provider, is used when validating, revalidating, or submitting changes to a P2PE Solution. ▪ The P2PE Component AOV, signed by a QSA (P2PE) Company and the P2PE Component Provider, is used when validating, revalidating, or submitting changes to a P2PE Component. ▪ The P2PE Application AOV, signed by a PA-QSA (P2PE) Company and the P2PE Application Vendor, is used when validating, revalidating, or submitting changes to a P2PE Application.
P-ROV	A "P2PE Report on Validation" completed by a P2PE Assessor Company and (except with respect to Merchant-managed Solutions) submitted directly to PCI SSC for review and Acceptance (defined in the P2PE Program Guide). For a P2PE Solution, P2PE Component, or P2PE Application to be included on the corresponding list of validated solutions, components, or applications on the Website, a corresponding P-ROV must be submitted directly to PCI SSC for review and Acceptance.

Term	Meaning
P-ROV (MMS)	A "P2PE Report on Validation" completed by a P2PE Assessor Company for a Merchant-managed Solution.
P2PE Application	Refer to definition in P2PE Glossary.
P2PE Application Assessment	Assessment of a P2PE Application against P2PE Domain 2 in isolation of any point-to-point solution in order to validate compliance with the P2PE Standard as part of the P2PE Program.
P2PE Application Vendor	Refer to definition in P2PE Glossary.
P2PE Assessment	A P2PE Solution Assessment, P2PE Component Assessment, or P2PE Application Assessment.
P2PE Assessor Company	A company qualified by PCI SSC as either a QSA (P2PE) Company or PA-QSA (P2PE) Company.
P2PE Assessor Employee	A QSA (P2PE) Employee or PA-QSA (P2PE) Employee.
P2PE Components	A P2PE service (such as encryption management, decryption management, or key injection) that is eligible for validation and Acceptance on a standalone basis as part of the P2PE Program and may be incorporated into and/or referenced as part of a P2PE Solution.
P2PE Component Assessment	Assessment of a P2PE Component against applicable P2PE Domains in order to validate compliance with the P2PE Standard as part of the P2PE Program.
P2PE Component Provider	Refer to definition in P2PE Glossary.
P2PE Domain or Domain	Any of the six control domains of the P2PE Standard, which together represent the core areas where security controls may need to be applied and validated.
P2PE Glossary	Refers to the then-current version of (or successor document to) the *PCI Point-to-Point Encryption Glossary of Terms, Abbreviations, and Acronyms*, as from time to time amended and made available on the 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 Non-payment Software	Refer to definition in P2PE Glossary.
P2PE Product	A P2PE Application, P2PE Component, or P2PE Solution

Term	Meaning
P2PE Program (or Program)	Refers to PCI SSC's program and requirements for qualification of QSA (P2PE) Companies and QSA (P2PE) Employees and PA-QSA (P2PE) Companies and PA-QSA (P2PE) Employees, and validation and Acceptance of P2PE Solutions, P2PE Components, and P2PE Applications, as further described in this document and related PCI SSC documents, policies, and procedures.
P2PE Program Guide	The then-current version of (or successor documents to) this document—the *Payment Card Industry (PCI) Point-to-Point Encryption P2PE Program Guide*, as from time to time amended and made available on the Website.
P2PE Solution	A combination of secure devices, applications, and processes that encrypt cardholder data from a PCI SSC-approved point-of-interaction (POI) device through to decryption and that is eligible for validation and Acceptance as part of the P2PE Program.
P2PE Solution Assessment	Assessment of a P2PE Solution against applicable P2PE Domains in order to validate compliance with the P2PE Standard as part of the P2PE Program.
P2PE Solution Provider	Refer to definition in P2PE Glossary.
P2PE Standard	The then-current version of (or successor document(s) to) the *Payment Card Industry (PCI) Point-to-Point Encryption Solution Requirements and Testing Procedures*, any and all appendices, exhibits, schedules, and attachments to the foregoing and all materials incorporated therein, in each case, as from time to time amended and made available on the Website.
P2PE Vendor	A P2PE Solution Provider, or P2PE Component Provider, or P2PE Application Vendor.
PA-QSA (P2PE) Company	A Payment Application Qualified Security Assessor (PA-QSA) Company that: (a) Is qualified by PCI SSC to provide services to P2PE Solution Providers, P2PE Component Providers, and/or P2PE Application Vendors in order to validate that such providers' or vendors' P2PE Solutions, P2PE Components, 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 (defined in Section 1.3 of the *P2PE Qualification Requirements*) or in remediation as a PA-QSA (P2PE) Company.

Term	Meaning
PA-QSA (P2PE) Employee	An individual employed by a PA-QSA (P2PE) Company who has satisfied, and continues to satisfy, all PA-QSA (P2PE) Requirements (defined in the *P2PE Qualification Requirements*) applicable to employees of PA-QSA (P2PE) Companies who will conduct P2PE Application Assessments, as described in further detail herein.
Participating Payment Brand	A global payment card brand or scheme that is also a limited liability company member of PCI SSC (or affiliate thereof).
PCI SSC or the Council	Refers to the PCI Security Standards Council, LLC.
PCI-approved POI device	Refer to definition in P2PE Glossary.
QSA (P2PE) Company	A Qualified Security Assessor (QSA) Company that: (a) Is qualified by PCI SSC to provide services to P2PE Solution Providers and/or P2PE Component Providers in order to validate that such providers' P2PE Solutions and/or P2PE Components adhere to all applicable aspects of the P2PE Standard, and (b) Remains in Good Standing (defined in Section 1.3 of the *P2PE Qualification Requirements*) or in remediation as a QSA (P2PE) Company. QSA (P2PE) Company qualification, alone, does not qualify a company to conduct P2PE Application Assessments. P2PE Application Assessments may only be performed by PA-QSA (P2PE) Companies.
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) Companies who will conduct P2PE Solution Assessments and/or P2PE Component Assessments, as described in further detail herein.
Secure Cryptographic Device (SCD)	Refer to definition in P2PE Glossary.
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 payment gateway or data center. A Third-Party Service Provider is only considered a P2PE Component Provider for eligible P2PE Component services if the applicable service is separately PCI-listed on the List of Validated P2PE Components. A Third-Party Service Provider that is not also a PCI-listed P2PE Component Provider for those services must have its services reviewed during the course of each of its solution-provider customers' P2PE Assessments.

Term	Meaning
Validated P2PE Application	A P2PE Application that has been assessed and validated by a PA-QSA (P2PE) Company 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 Component	A P2PE Component that has been assessed and validated by a QSA (P2PE) Company to be in scope for the P2PE Program and to have met all necessary P2PE Requirements and then Accepted by PCI SSC, so long as such Acceptance has not been revoked, suspended, withdrawn, or terminated.
Validated P2PE Product	A Validated P2PE Application, Validated P2PE Component, or Validated P2PE Solution
Validated P2PE Solution	A P2PE Solution that has been assessed by a QSA (P2PE) Company or PA-QSA (P2PE) Company 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.
Vendor Release Agreement (or VRA)	The then-current and applicable form of release agreement that PCI SSC: (a) Requires to be executed by P2PE Solution Providers, P2PE Component Providers and/or P2PE Application Vendors (as applicable) in connection with the P2PE Assessor Program, and (b) Makes available on the Website.
Versioning Methodology	Refer to definition in P2PE Glossary.
Website	The then-current PCI SSC Website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org.
Wildcard	Refer to definition in P2PE Glossary.

1.5 About the P2PE Standard

The P2PE Standard reflects a desire among constituents of the Payment Card Industry for a single, standardized set of security requirements, security assessment procedures, and processes for recognizing P2PE Products validated by P2PE Assessors. The P2PE Standard 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 the P2PE Standard in a variety of ways, including the following:

- Customers benefit from a broader selection of validated P2PE Solutions, the possibility of implementing Validated P2PE Solutions to reduce the scope of PCI DSS assessments, and assurance from using P2PE Products validated by a QSA (P2PE) and/or PA-QSA (P2PE) Companies to be P2PE Standard compliant.

- P2PE Solution Providers benefit from a broader selection and recognition of P2PE Components and P2PE Applications.
- P2PE Solutions validated and listed by the Council are currently recognized by all Participating Payment Brands.

Note: *each brand independently develops and manages its own compliance programs and decisions regarding recognition of P2PE Products.*

For more information regarding PCI SSC, see the Website.

1.6 P2PE Initiative and Overview

This P2PE Program Guide reflects a single set of requirements currently recognized by each of the Participating Payment Brands regarding:

- P2PE security requirements and assessment procedures
- Processes for recognizing P2PE Assessor-validated P2PE Solutions, P2PE Components, and P2PE Applications
- Quality assurance processes for P2PE Assessor Companies

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.

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 and Application Management	The secure management of the PCI-approved POI devices and the resident software.
Domain 2: Application Security	The secure development of payment applications designed to have access to clear-text account data intended solely for installation on PCI-approved POI devices.
Domain 3: P2PE Solution Management	Overall management of the P2PE solution by the solution provider, including third-party relationships, incident response, and the *P2PE Instruction Manual* (PIM).
Domain 4: Merchant-managed Solutions	Separate duties and functions between merchant encryption and decryption environments.
Domain 5: Decryption Environment	The secure management of the environment that receives encrypted account data and decrypts it.
Domain 6: P2PE Cryptographic Key Operations and Device Management	Establish and administer key-management operations for account data encryption POI devices and decryption HSMs.

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

Note: 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.

2 Roles and Responsibilities

This section provides an overview of the roles and responsibilities of the various P2PE stakeholder groups.

2.1 P2PE Vendors

P2PE Vendors (P2PE Solution Providers, P2PE Component Providers, and P2PE Application Vendors) seeking Acceptance as part of the Program provide access to their P2PE Products and supporting documentation to the P2PE Assessor Company for validation, and authorize their P2PE Assessor Company to submit resulting P-ROVs and related information to PCI SSC.

2.1.1 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 applicable requirements of the P2PE Standard.

2.1.2 P2PE Application (Software) Vendors

As part of establishing the P2PE compliance of its applications, an application vendor that develops applications with access to clear-text account data on a POI device (i.e., P2PE Applications) must have those applications assessed for secure operation within the applicable POI devices, and must provide corresponding *Implementation Guides* that describe the secure installation and administration of such applications on the corresponding POI devices.

Where a P2PE Application is to be used in a P2PE Solution, 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. P2PE Applications must be assessed by a PA-QSA (P2PE) Company. For P2PE Applications intended for use in multiple P2PE Solutions, validation and Acceptance as a Validated P2PE Application eliminates the need for the application to be separately reviewed as part of each P2PE Solution in which is it used.

2.1.3 P2PE Component Providers

P2PE Component Providers provide any of the following component services that are assessed and intended for listing by PCI SSC, and subsequently, for use in P2PE Solutions:

- Encryption-management services – Assessed per Domains 1 and 6 including Annex A as applicable.
- Decryption-management services – Assessed per Domains 5 and 6 including Annex A as applicable.
- Key-Injection Facility services – Assessed per Annex B of Domain 6 including Annex A as applicable.
- Certification Authority/Registration Authority services – Assessed per Domain 6 Annex A, Part A2, including Part A1 as applicable.

While an entity may provide more than one of the above component services, only component services that have been validated by a P2PE Assessor and Accepted on a stand-alone basis by PCI SSC are separately listed on the Website. “Stand-alone basis” here refers to the requirement for each component service’s individual PCI SSC submission in the Portal—including the corresponding P-AOV, P-ROV, and applicable fees—for each individual component service. While each component service requires its own PCI SSC submission, the actual validation may be part of a larger P2PE assessment and a separate assessment solely for the individual component service may not be required.

If a component service described above is assessed as part of a P2PE Solution but is not on the List of Validated P2PE Components, the entity is not considered a P2PE Component Provider for purposes of that component and is simply referred to as a Third-Party Service Provider with respect to that component. A Third-Party Service Provider must have its services reviewed during the course of each of its solution provider customers’ P2PE Assessments.

All QSA (P2PE) Companies are qualified to assess P2PE Components for Listing on the List of Validated P2PE Components.

2.1.3.1 Encryption-management Entity

An “Encryption-management Entity” is an entity that manages and deploys POI devices and any resident P2PE applications and/or P2PE non-payment software. Specific requirements for Encryption-management Entities are set out in Domain 1 and 6 (including Annex A as applicable) of the P2PE Standard and need only be concerned up to the point of initial key loading. The requirements in Domains 1 and 6 apply to all Encryption-management Entities whether the entity is a P2PE Component Provider, a P2PE Solution Provider, or a Third-Party Service Provider performing functions on behalf of a P2PE Solution Provider.

2.1.3.2 Decryption-management Entity

A “Decryption-management Entity” is an entity that performs decryption management functions for the secure management of the environment that receives encrypted account data and decrypts such account data.

Specific requirements for Decryption-management Entities are set out in Domains 5 and 6 (including Annex A as applicable) of the P2PE Standard. The requirements in Domains 5 and 6 apply to all Decryption-management Entities whether the entity is a P2PE Component Provider, a P2PE Solution Provider, or a Third-Party Service Provider performing functions on behalf of a P2PE Solution Provider.

2.1.3.3 Key-Injection Facilities

The term “Key-Injection Facility” (KIF) describes an entity performing key injection into POI devices.

Specific requirements for KIFs are set out in Annex B of Domain 6 (including Annex A) of the P2PE Standard. The requirements apply to all KIFs, whether the entity is a P2PE Component Provider, a P2PE Solution Provider, or a Third-Party Service Provider performing functions on behalf of a P2PE Solution Provider.

2.1.3.4 Certification/Registration Authorities

A Certification Authority (CA)/Registration Authority (RA), as defined in the P2PE Standard, is an entity that signs public keys, whether in X.509 certificate-based schemes or other designs for use in connection with the remote distribution of symmetric keys using asymmetric techniques. A Registration Authority (RA) performs registration services on behalf of a CA to vet requests for certificates that will be issued by the CA.

Specific requirements for CAs/RAs are set out in Domain 6 Annex A, Part A2 (and Part A1, as applicable) of the P2PE Standard. These requirements apply to all CAs/RAs, whether the entity is a P2PE Component Provider, a P2PE Solution Provider, or a Third-Party Service Provider performing functions on behalf of a P2PE Solution Provider.

2.1.4 Third-Party Service Providers

As noted in Section 1.4 "Terminology," a Third-Party Service Provider may provide services or functions on behalf of a P2PE Vendor, but Third-Party Service Provider must have its services or functions reviewed during the course of each of its P2PE Vendor customers' P2PE Assessments. There is no listing of Third-Party Service Providers on the Website, including within the listing of the P2PE Product with which the third party's services or functions were assessed for use.

Refer to Section 2.1.3, "P2PE Component Providers," to understand how to address Third-Party Service Providers whose services may be eligible for consideration as a P2PE Component. Without such applicable services being separately PCI-listed on the List of Validated P2PE Components, those services (such as KIF, CA/RA, etc.) are not considered P2PE Components but simply a third-party service provider with respect to the P2PE Solution it is used within.

2.2 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.

2.3 PCI Security Standards Council

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

- Maintains a centralized repository for all P-ROVs for P2PE Products listed on the Website;
- Hosts the List of Validated P2PE Solutions, the List of Validated P2PE Components, and the List of Validated P2PE Applications on the Website;
- Provides required training for and qualifies QSA (P2PE) and PA-QSA (P2PE) Companies and Employees to assess and validate P2PE Products for P2PE compliance;
- Maintains and updates the P2PE Standard and related documentation according to a standards lifecycle management process; and
- Reviews all P-ROVs submitted to PCI SSC and related change submissions for compliance with baseline quality standards, including but not limited to, confirmation that:
    - Submissions (including P-ROVs, updates and Interim Self Assessments/Annual Revalidations) are correct as to form;
    - QSA (P2PE) and PA-QSA (P2PE) Companies properly determine whether candidate P2PE Products meet baseline eligibility criteria for validation under the P2PE Program (PCI SSC reserves the right to reject or de-list any P2PE Solution, P2PE Component, and/or P2PE Application determined to be ineligible for the P2PE Program);
    - QSA (P2PE) and PA-QSA (P2PE) Companies adequately report the P2PE compliance of candidate Products in their associated submissions; and
    - Detail provided in such submissions meets PCI SSC's reporting requirements.

As part of the PCI SSC quality assurance (QA) process, PCI SSC assesses whether overall, QSA (P2PE) and PA-QSA (P2PE) Company operations appear to conform to PCI SSC's quality assurance and qualification requirements.

***Note**: PCI SSC does not assess or validate P2PE Solutions, P2PE Components, and/or P2PE Applications for P2PE compliance; assessment and validation is the role of the QSA (P2PE) and/or PA-QSA (P2PE) Company, as applicable. Listing of a P2PE Solution, P2PE Component, and/or P2PE Application on the List of Validated P2PE Solutions, List of Validated P2PE Components, and/or List of Validated P2PE Applications signifies only that the applicable P2PE Assessor Company has determined that the application complies with the P2PE Standard, that the P2PE Assessor Company has submitted a corresponding P-ROV to PCI SSC, and that the P-ROV, as submitted to PCI SSC, has satisfied all requirements of the PCI SSC for P-ROVs as of the time of PCI SSC's review.*

2.4 P2PE Assessor Companies

There are two types of P2PE Assessor Companies:

- **QSA (P2PE):** QSA (P2PE) Companies are QSA companies that have been additionally qualified by PCI SSC to perform P2PE Assessments of P2PE Solutions and P2PE Components. QSA (P2PE) Companies are not qualified by PCI SSC to perform P2PE Application Assessments.
- **PA-QSA (P2PE):** PA-QSA (P2PE) Companies are PA-QSA companies that have been additionally qualified by PCI SSC to perform P2PE Assessments of P2PE Solutions, P2PE Components, and P2PE Applications.

Note:

- *Not all QSA Companies are PA-QSA Companies—there are additional qualification requirements that must be met for a QSA Company to become a PA-QSA Company.*
- *Not all QSA Companies are QSA (P2PE) Companies—there are additional qualification requirements that must be met for a QSA Company to become a QSA (P2PE) Company.*
- *Not all PA-QSA Companies are PA-QSA (P2PE) Companies—there are additional qualification requirements that must be met for a PA-QSA Company to become a PA-QSA (P2PE) Company.*

P2PE Assessor Companies are responsible for:

- Performing assessments of P2PE Solutions and P2PE Components (and P2PE Applications for PA-QSA (P2PE) Assessor Companies) in accordance with the P2PE Standard and the *P2PE Qualification Requirements.*
- Providing an opinion regarding whether the P2PE Solution or P2PE Component (or P2PE Application for PA-QSA (P2PE) Assessor Companies) meets the P2PE Standard.
- Documenting each P2PE Assessment in a P-ROV using the applicable P2PE P-ROV Reporting Template.
- Providing adequate documentation within the applicable P-ROV to demonstrate the P2PE Solution's or P2PE Component's (or P2PE Application's for PA-QSA (P2PE) Assessor Companies) P2PE compliance.
- Where applicable, submitting the applicable P-ROV and/or any change submission to PCI SSC, along with the applicable P-AOV signed by both the P2PE Assessor Company and P2PE Vendor;
- Maintaining an internal quality assurance process for their P2PE Assessment efforts.
- Staying up-to-date with Council statements and guidance, P2PE Technical FAQs, industry trends and best practices.
- Determining the scope and applicability of the P2PE Standard as it applies to a given P2PE Solution Assessment, in accordance with the P2PE Standard.

It is the QSA (P2PE) Employee's responsibility to assess a P2PE Solution's or P2PE Component's P2PE compliance (and the PA-QSA (P2PE) Employee's responsibility to assess a P2PE Application's P2PE compliance) as of the date of the P2PE Assessment, and document their findings and opinions on compliance. As indicated above, PCI SSC does not approve P-ROVs from a technical compliance perspective but performs quality assurance to confirm that the P-ROVs adequately document the demonstration of compliance.

2.5 Integrators and Resellers

Integrators and Resellers are those entities that sell, install, and/or service P2PE Solutions on behalf of P2PE Vendors or others. Integrators and Resellers performing 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 POI devices used in a P2PE Solution—for example, troubleshooting, delivering remote updates, and providing remote support—according to the validated processes in the *P2PE Instruction Manual.*
- Ensuring that customers are provided (either directly from the Vendor or from the reseller or integrator) with a current copy of the *P2PE Instruction Manual.*

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

2.6 Qualified Integrators and Resellers (QIRs)

PCI Qualified Integrators and Resellers (QIRs) are trained by the Council in PCI DSS and PA-DSS in order to help ensure that they securely implement Payment Applications. However, the QIR Program does not apply to the P2PE Program at this time.

2.7 Customers

Merchants are the P2PE Solution customers and users. Customers using a Validated P2PE Solution to facilitate their PCI DSS compliance are responsible for:

- 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 and/or integrator/reseller.
- Ensuring—if the merchant has other non-P2PE payment channels—that the P2PE environment is adequately segmented (isolated) from any non-P2PE payment channels.
- Removing any legacy cardholder data or systems from the P2PE environment.
- Ensuring that their payment environments are validated against applicable PCI DSS requirements in accordance with applicable payment card brand requirements.

2.8 PCI-Recognized Laboratories

Security laboratories qualified by PCI SSC under the PCI SSC laboratory program ("PCI-recognized 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-recognized Laboratories to PCI SSC for approval; and if approved, the device is listed on PCI SSC's "List of Approved PTS Devices" on the PCI SSC website.

Note: *Device evaluation by a PCI-recognized Laboratory is a separate process from the validation of a P2PE Solution Assessment; the P2PE Solution Assessment validates whether or not a given P2PE Solution (which may include multiple POI devices) is in compliance with the P2PE Standard.*

2.9 Payment Device (Hardware) Vendors

A POI device vendor submits a POI device for evaluation to an independent PCI-recognized Laboratory. Per PTS requirements, device vendors must develop a supplement document describing the secure operation and administration of such devices.

3 Overview of Validation Processes

3.1 Validation Processes for P2PE Solutions, P2PE Components, and P2PE Applications to be listed on the Website

The P2PE Assessment process is initiated by the P2PE Vendor. The Website has all the associated documents needed to navigate the P2PE Assessment process. The following is a high-level overview of the process (other than for Merchant-managed Solutions):

1) The P2PE Vendor selects a P2PE Assessor Company from the Council's List of P2PE Qualified Security Assessor Companies and negotiates the cost and any associated P2PE Assessor Company confidentiality and non-disclosure agreements with the P2PE Assessor Company.

2) The P2PE Vendor then provides to the P2PE Assessor Company access to the Solution, Component, or Application to be assessed, POI device types, corresponding *Implementation Guides* for P2PE Applications*, P2PE Instruction Manual* for P2PE Solutions, and all associated manuals and other required documentation, including but not limited to the P2PE Vendor's signed *Vendor Release Agreement*.

Refer to the sections "P2PE Solutions and Use of Third Parties and/or P2PE Component Providers" and "P2PE Solutions and Use of P2PE Applications and/or P2PE Non-payment Software" in the P2PE Standard to understand options for validating Third-Party Service Providers, P2PE Component Providers and P2PE Applications to be used in P2PE Solutions.

3) The P2PE Assessor Company then assesses the Solution, Component, or Application, including its security functions and features, to determine whether it complies with the P2PE Standard.

4) If the P2PE Assessor Company determines that the Solution, Component, or Application is in compliance with the P2PE Standard, the P2PE Assessor Company submits a corresponding P-ROV to PCI SSC, attesting to compliance and setting forth the results, opinions, and conclusions of the P2PE Assessor Company on all test procedures along with the P2PE Vendor's signed VRA and the corresponding P-AOV.

Note: *If the P2PE Solution being assessed includes a P2PE Component and/or P2PE Application intended for PCI SSC Listing (but not yet Listed), each such P2PE Product must be individually submitted to PCI SSC via the Portal – including the corresponding P-AOV, P-ROV, and applicable fees – to achieve PCI SSC Listing for each P2PE Product. This submission must be Accepted by PCI SSC before review of the P2PE Solution can occur, though all can be submitted to PCI SSC and invoiced at the same time. The review of the paid P2PE Solution will remain on hold until the Listing of any related pending P2PE Component and/or P2PE Application.*

Note: *Only one P2PE Component service can be included in each submission to PCI SSC for Listing, even if an entity conducts more than one component service and they were assessed together. As noted above, this may not require separate assessments, but each such component service must be individually submitted to PCI SSC via the Portal – including the corresponding P-AOV, P-ROV, and applicable fees – to achieve PCI SSC Listing.*

Note: *While each P2PE Component service or P2PE Application requires its own PCI SSC submission for review and Acceptance, the actual validation may be part of a larger P2PE assessment and a separate assessment solely for the individual component service may not be required.*

5) PCI SSC issues an invoice to the P2PE Vendor for the applicable P2PE Acceptance Fee. After the P2PE Vendor has paid the invoice, PCI SSC reviews the P-ROV to confirm that it meets the P2PE Program requirements and if confirmed, PCI SSC notifies the P2PE Assessor Company and P2PE Vendor that the Solution, Component, or Application has successfully completed the process.

6) Once the Solution, Component, or Application completes the above process, the Council signs the corresponding P-AOV and adds the P2PE Solution, P2PE Component, or P2PE Application to the corresponding List on the Website.

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

The illustrations and descriptions on the following pages explain in further detail processes for the P2PE Program:

Process	Illustration
P2PE Product Assessment for Products Intended for PCI SSC Listing	Figure 1
P2PE Product Submission and PCI SSC Review	Figure 2

Figure 1: P2PE Product Assessment for Products Intended for PCI SSC Listing

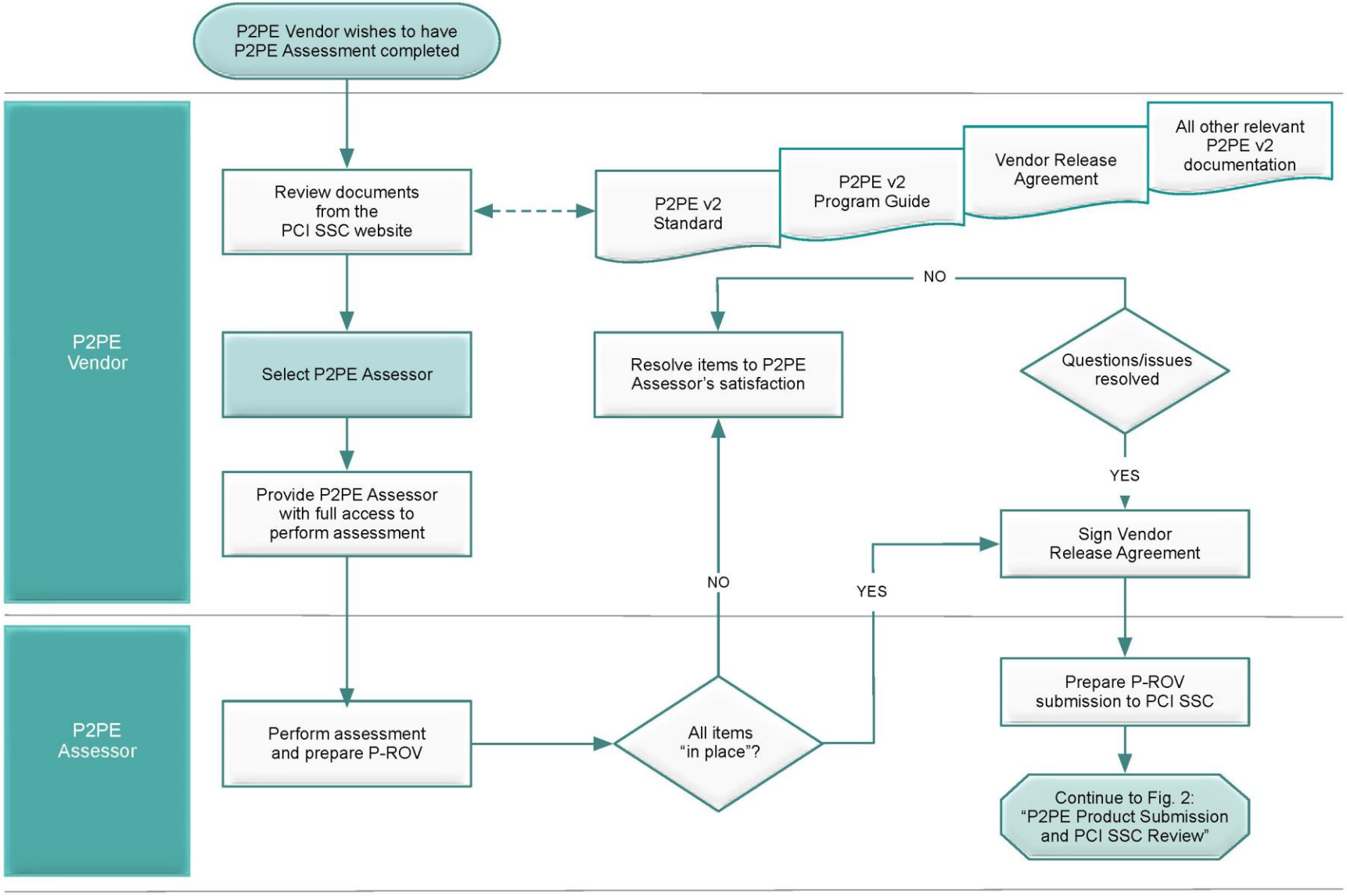
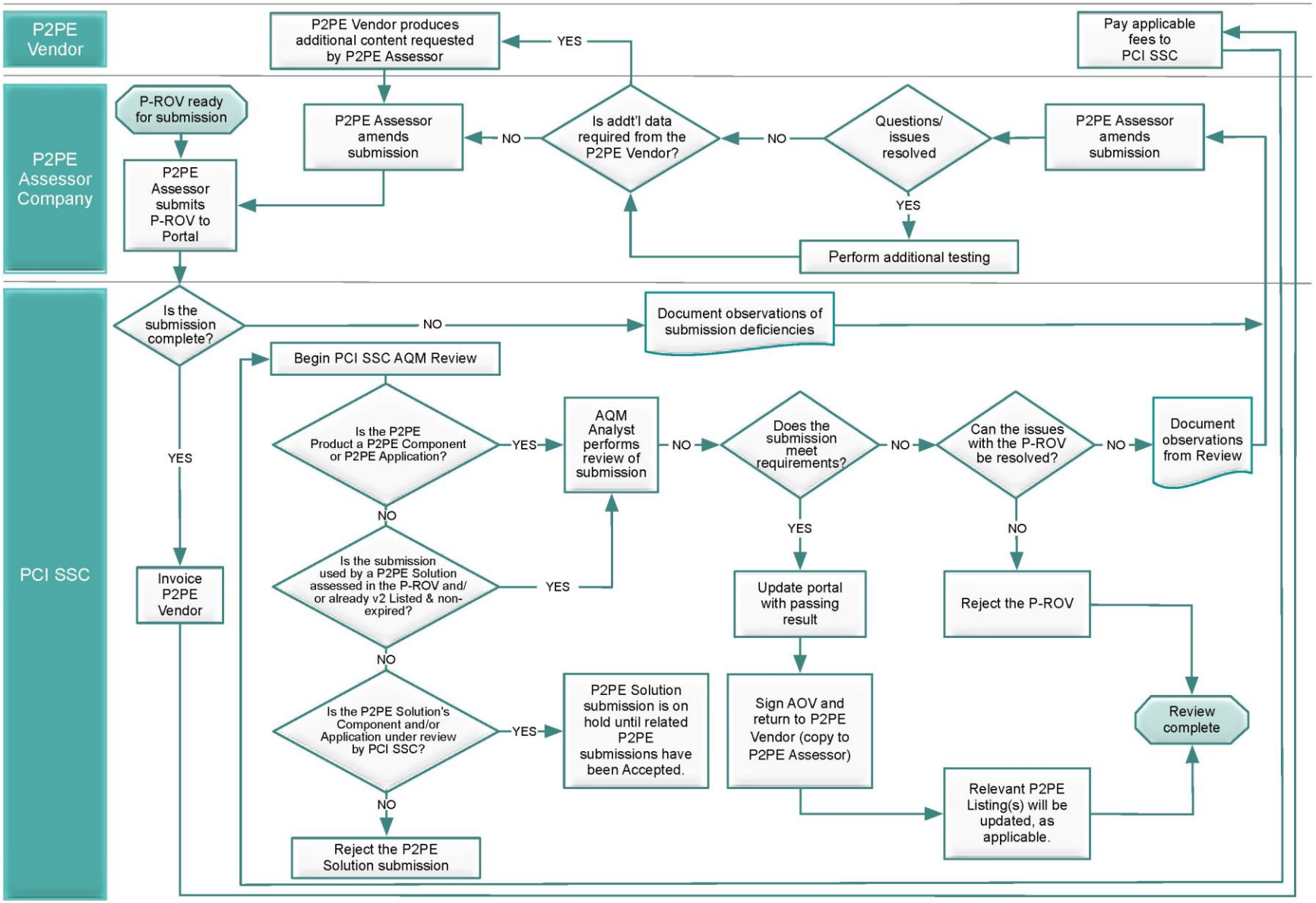


Figure 2: P2PE Product Submission and PCI SSC Review



3.2 Overview of Validation Processes for Merchant-managed Solutions

The P2PE Assessment process for Merchant-managed Solutions (MMS) is initiated by the Merchant. The Website has all the associated documents needed to navigate the assessment process for MMS. The following is a high-level overview of the process:

1) The Merchant selects a P2PE Assessor Company from the Council's List of P2PE Qualified Security Assessor Companies and negotiates the cost and any associated P2PE Assessor Company confidentiality and non-disclosure agreements with the P2PE Assessor Company.
2) The Merchant then provides to the P2PE Assessor Company access to the MMS to be assessed, POI device types, corresponding *Implementation Guides* for P2PE Applications, *P2PE Instruction Manual* for MMS, and all associated manuals and other required documentation.
3) The P2PE Assessor Company then assesses the MMS, including its security functions and features, to determine whether the MMS complies with the P2PE Standard.
4) If the P2PE Assessor Company determines that the MMS, is in compliance with the P2PE Standard, the P2PE Assessor Company prepares and submits to the Merchant a corresponding Solution P-ROV attesting to compliance and setting forth the results, opinions and conclusions of the P2PE Assessor Company on all test procedures.

Refer to the sections "P2PE Solutions and Use of Third Parties and/or P2PE Component Providers" and "P2PE Solutions and Use of P2PE Applications and/or P2PE Non-payment Software" in the P2PE Standard to understand options for validating Third-Party Service Providers, P2PE Component Providers, and P2PE Applications.

Note: *Merchant-managed Solutions are not eligible for listing on the Website, and the P-ROV is not submitted to PCI SSC. A Merchant-managed Solution may utilize third-party service providers, listed P2PE Applications and/or listed P2PE Components.*

4 Preparation for the Review

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

4.1 Considerations for Secure Cryptographic Devices (SCDs), Vendors of P2PE Applications and Non-payment Software, and Providers of P2PE Components for use in P2PE Solutions

Note: *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.*

Note: *A PA-DSS assessment is not required or necessary for a P2PE Application or Non-payment Software to be used in a P2PE Solution.*

The following table should be used to determine requirements and eligibility, along with the relevant reference sections of the P2PE Standard:

Table 4.1

Possible Element	Program Guidance
SCDs	Validated P2PE Solutions require the use of various types of SCDs. To assist in evaluating these device types for use in a P2PE Solution: ▪ Refer to "Definition of Secure Cryptographic Devices (SCDs) to be used in P2PE Solutions" in the Introduction section of the P2PE Standard for requirements for these devices; ▪ Use the "SCD Domain Applicability" matrix in the Introduction section of the P2PE Standard. Obtaining and maintaining PTS device approval (for those SCDs that require approval) is the responsibility of the secure cryptographic device vendor. For those SCDs required to be approved, such approval is a prerequisite for the devices being assessed as part of a P2PE Solution Assessment. P2PE Assessors will request evidence of device approvals being in place and current as part of performing a P2PE Solution Assessment. Device vendors wishing to obtain PTS approval should consult the Website for further information. Obtaining PTS approval does not replace or supersede any payment card brand-specific device-approval processes.

Possible Element	Program Guidance
P2PE Applications	▪ Refer to definition in P2PE Glossary. ▪ Refer to "P2PE Solutions and Use of P2PE Applications and/or P2PE Non-payment Software" in the Introduction section of the P2PE Standard. ▪ Must undergo validation per all P2PE Domain 2 Requirements by a PA-QSA (P2PE), and will be either: • Independently listed on the List of Validated P2PE Applications **OR** • Not listed on the List of Validated P2PE Applications and therefore only considered an element of the specific Validated P2PE Solution for which it has been submitted. ▪ If a P2PE Application is currently listed on the List of Validated P2PE Applications AND was assessed against the same major version of the P2PE standard, only the applicable Domain 1 Testing Procedures must be assessed and evidenced in the Solution P-ROV for each P2PE Solution Assessment in which the application is used. ▪ If a P2PE Application is not already on the List of Validated P2PE Applications, both the Application P-ROV and the Solution P-ROV must be submitted before the P2PE Solution can be Accepted. This applies for **each** P2PE Solution in which the application is used.
P2PE Non-payment Software	▪ Refer to definition in P2PE Glossary. ▪ Refer to "P2PE Solutions and Use of P2PE Applications and/or P2PE Non-payment Software" in the Introduction section of the P2PE Standard. ▪ Assessed only per designated P2PE Domain 1 Requirements as noted in the above referenced section of the P2PE Standard, by a P2PE Assessor Company. ▪ Not eligible for PCI-listing.

Possible Element	Program Guidance
P2PE Components	There are four P2PE Component products or services that can be separately assessed and PCI-listed in isolation of any P2PE Solution defined in the P2PE Standard. ▪ Refer to definition in P2PE Glossary. ▪ Refer to "P2PE Solutions and Use of Third Parties and/or P2PE Component Providers" in the Introduction section of the P2PE Standard. Independent PCI SSC listing of Third-Party Service Provider component services depends on eligibility and is optional. However, such independent listing is required for a given component service to be recognized as a Validated P2PE Component that can be used in multiple P2PE Solutions without the need for full P2PE Assessment of those services each time it is used with a different P2PE Solution. ▪ If a P2PE Component is currently listed on the List of Validated P2PE Components, the Component P-ROV has already been Accepted by PCI SSC. As a result, only the applicable Testing Procedures must be assessed and evidenced in the Solution P-ROV for each Validated P2PE Component included in the applicable P2PE Solution ▪ If a P2PE Component is not already on the List of Validated P2PE Components but is being added to the List of Validated P2PE Components, the Component P-ROV must be submitted and Accepted before the Solution P-ROV can be Accepted. If independent listing is not being pursued for a P2PE Component, this is instead considered a Third-Party Service Provider's service offering and it is only an element of the specific Validated P2PE Solution within which it is assessed.
Third-Party Service Provider	Refer to "P2PE Solutions and Use of Third Parties and/or P2PE Component Providers" in the Introduction section of the P2PE Standard.

4.2 Prior to the Review

Note: *The process for developing and validating P2PE Solutions—including responsibilities for implementing requirements and validating compliance with each Domain—is defined within the P2PE Standard.*

Prior to commencing a P2PE review with a P2PE Assessor Company, all parties involved are encouraged to take the following preparatory actions:

- Review the requirements of both the PCI DSS and the P2PE Standard and all related documentation located at the Website.
- Determine/assess the Solution's, Component's, or Application's readiness to comply with P2PE:
  - Perform a gap analysis between the Solution's, Component's, or Application's security functionality and the P2PE Standard;
  - Correct any gaps; and
  - If desired, the P2PE Assessor Company may perform a pre-assessment or gap analysis of a P2PE Solution, Component, or Application. If the P2PE Assessor Company notes deficiencies that would prevent a compliant result, the P2PE Assessor Company will provide a list of P2PE features to be addressed before the formal review process begins.
- Determine whether the P2PE Application Provider's *Implementation Guide* meets P2PE Standard requirements and correct any gaps.
- Determine whether the P2PE Solution Provider's *P2PE Instruction Manual* meets P2PE Standard requirements and correct any gaps.
- P2PE Solution Providers are responsible for ensuring that the various components and applications (including those provided by Third-Party Service Providers, P2PE Application Vendors, and/or P2PE Component Providers) used as part of their P2PE Solutions are all compliant with all applicable requirements of the P2PE Standard, and that appropriate agreements are in place with such providers and vendors to ensure proper information disclosures if required under the *Vendor Release Agreement*.

4.3 Required Documentation and Materials

All completed P2PE Assessment-related materials such as manuals, the *P2PE Instruction Manual*, *P2PE Application Implementation Guide*, the *Vendor Release Agreement* and all other materials related to the P2PE Assessment and participation in the P2PE Program must be delivered to the P2PE Assessor Company performing the assessment, not to PCI SSC.

4.4 P2PE Review Timeframes

The amount of time necessary for a P2PE Assessment can vary widely depending on factors such as:

- How close the P2PE Product is to being P2PE-compliant at the start of the Assessment
  - Corrections to the P2PE Product to achieve compliance will delay validation.
- For P2PE Solutions that use P2PE Applications and/or P2PE Components
  - Those that are being listed on the Website separately must be Listed before the P2PE Solution can be reviewed.

- Whether the P2PE Application's *Implementation Guide* and/or *P2PE Implementation Manual* meets all P2PE Requirements at the start of the Assessment
  - Extensive rewrites will delay validation.
- Prompt payment of the fees due to PCI SSC
  - PCI SSC will not commence review of the P-ROV until the applicable fee has been paid.
- Quality of the P2PE Assessor Company's submission to PCI SSC
  - Incomplete submissions or those containing errors—for example, missing or unsigned documents, incomplete or inconsistent submissions—will result in delays in the review process.
  - If PCI SSC reviews the P-ROV more than once, providing comments back to the P2PE Assessor Company to address each time, this will increase the length of time for the review process.

Any P2PE Assessment timeframes provided by a P2PE Assessor Company should be considered estimates, since they may be based on the assumption that the P2PE Product is able to successfully meet all P2PE requirements quickly. If problems are found during the review or acceptance processes, discussions between the P2PE Assessor Company, the P2PE Vendor, and/or PCI SSC may be required. Such discussions may significantly impact review times and cause delays and/or may even cause the review to end prematurely (for example, if the P2PE Vendor decides they do not want to make the necessary changes to achieve compliance).

4.5 P2PE Assessors

PCI SSC qualifies and provides required training for P2PE Assessor Companies (QSA (P2PE) and PA-QSA (P2PE)) to assess and validate P2PE Products for adherence to the P2PE Standard. In order to perform P2PE Solution Assessments and/or P2PE Component Assessments, a P2PE Assessor Company must have been qualified by PCI SSC and remain in Good Standing (as defined in the *QSA Qualification Requirements* and *P2PE Qualification Requirements*, as applicable) or in remediation as both a QSA Company and QSA (P2PE) Company. In order to perform P2PE Application Assessments, a P2PE Assessor Company must have been additionally qualified by PCI SSC and remain in Good Standing (as defined in the *QSA Qualification Requirements* and *P2PE Qualification Requirements*, as applicable) or in remediation as both a PA-QSA Company and PA-QSA (P2PE) Company. All recognized P2PE Assessor Companies are listed on the Website. These are the only assessors recognized by PCI SSC as qualified to perform P2PE Assessments.

- For each P2PE Assessment, the resulting P2PE Assessor report must follow the P2PE Report on Validation (P-ROV) template and instructions, as outlined in the corresponding P2PE Solution, P2PE Component, and P2PE Application *P2PE P-ROV Reporting Template.*
- The P2PE Assessor Company must prepare each P-ROV based on evidence obtained by following the P2PE Standard.
- Each P-ROV submitted to PCI SSC must be accompanied by a corresponding P2PE Attestation on Validation (P-AOV) in the form available through the Website, signed by a duly authorized officer of the P2PE Assessor Company, that summarizes whether the entity is in compliance or is not in compliance with PCI P2PE and any related findings, as well as the *P2PE Application Implementation Guide* (as applicable) and *P2PE Implementation Manual.*

4.5.1 P2PE Assessor Company Fees

The prices and fees charged by P2PE Assessor Companies are not set by PCI SSC. These fees are negotiated between the P2PE Assessor Company and their customers. Before deciding on a P2PE Assessor Company, it is recommended that a prospective customer check the list of P2PE Qualified Assessor Companies, talk to several P2PE Assessor Companies, and follow their own vendor-selection processes.

4.5.2 Non-P2PE assessment services that may be offered by P2PE Assessor Companies

The list below provides examples of non-P2PE Assessment services that may be offered by P2PE Assessor Companies. These services are neither required nor recommended by PCI SSC. If these services are of interest to your company, please contact the P2PE Assessor Companies for availability and pricing. Examples of non-P2PE Assessment services include, but are not limited to:

- 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* and/or *P2PE Application Implementation Guide*
- Pre-assessment (gap analysis) services prior to beginning formal P2PE Assessment
- Guidance for bringing the Solution, Component, or Application into compliance with the P2PE Standard if gaps or areas of non-compliance are noted during the assessment

Note: *When arranging for non-P2PE Assessment services with a P2PE Assessor Company, care should be taken by both the P2PE Assessor Company and its customer to ensure that the P2PE Assessor Company satisfies all independence requirements as set forth in the* QSA Qualification Requirements*—for example, that a P2PE Assessor Employee does not assess its own work product as part of the actual P2PE Assessment. Conflicts of interest may result in the P-ROV being rejected by PCI SSC.*

4.6 Technical Support throughout Testing

It is recommended that the P2PE Vendor (or in the case of a Merchant-managed Solution, the Merchant) make available a technical resource person to assist with any questions that may arise during the assessment. During the review, and to expedite the process, a technical contact should be on call to discuss issues and respond to questions from the P2PE Assessor Company.

4.7 *Vendor Release Agreement* (VRA)

For any P2PE Product to be listed on the Website, the P2PE Vendor's signed copy of the most-current version of the *Vendor Release Agreement* available on the Website must be provided to the P2PE Assessor Company along with access to the P2PE Product and other documents and materials at the beginning of each P2PE Assessment process

Among other things, the VRA:

- Covers confidentiality issues;
- Covers the P2PE Vendor's agreement to P2PE Program requirements, policies and procedures;

- Gives permission to the P2PE Vendor's P2PE Assessor Company to release P-ROVs and related materials to PCI SSC for review; and
- Requires P2PE Vendors to adopt and comply with industry standard Vulnerability Handling Policies.

For PCI SSC review of a P-ROV to take place:

- The P2PE Assessor Company must provide to PCI SSC the P2PE Vendor's signed copy of the then-current VRA, along with the initial P-ROV submitted to PCI SSC in connection with that P2PE Assessment.
- So long as an executed copy of the current VRA is on file with PCI SSC for the relevant P2PE Vendor, the P2PE Assessor is not required to re-submit the same VRA with each subsequent P-ROV for the same P2PE Vendor.

4.8 The Portal

For any P2PE Solution, P2PE Component, or P2PE Application to be listed on the Website all documents relating to the P2PE validation process are to be submitted by the applicable P2PE Assessors, on behalf of the P2PE Vendor, 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.

4.9 P2PE Acceptance Fees

For each P2PE Product to be listed on the Website, the P2PE Vendor is also required to pay a *P2PE Acceptance Fee* to PCI SSC. For each new P2PE Product submission, the corresponding P2PE Acceptance Fee will be invoiced and must be received by PCI SSC before the P2PE submission will be reviewed, Accepted, and added to the corresponding List of Validated P2PE Solutions, List of Validated P2PE Components, or List of Validated P2PE Applications. Upon Acceptance, PCI SSC will sign and return a copy of the corresponding P-AOV to both the P2PE Vendor and the P2PE Assessor Company.

Note:

All P2PE Assessment-related fees are payable directly to the P2PE Assessor Company (these fees are negotiated between the P2PE Assessor Company and their customers).

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

There are no annual recurring PCI SSC fees associated with the Acceptance of a P2PE Product. There are, however, PCI SSC fees associated with P2PE Vendor delays in annual revalidation of P2PE Validated Products. Please see the Website for more information.

All Program fees are non-refundable and are subject to change upon posting of revised fees on the Website.

5 Managing a Validated P2PE Listing

5.1 Annual Revalidation

Annually, by the Interim Assessment Due date (i.e., the anniversary date of the P2PE Product's Acceptance), the P2PE Vendor is required to submit an updated *P2PE Attestation of Validation*, performing the Interim Self-Assessment steps (as indicated in the P-AOV). PCI SSC will provide notification via email to the P2PE Vendor Contact (listed on the P-AOV) within 90 days of revalidation/reassessment, but it is the sole responsibility of the P2PE Vendor to maintain the listing regardless of the successful receipt of the courtesy reminder(s).

As part of this annual process, P2PE Vendors are required to confirm whether any changes have been made to the P2PE Solution, P2PE Component, or P2PE Application, and that:

a) Changes have been applied in a way that is consistent with the P2PE Standard;

b) The P2PE Solution, P2PE Component, or P2PE Application continues to meet the requirements of the P2PE Standard;

c) The PCI SSC has been advised of any change that necessitates a change to the listing on the Website, in accordance with this Program Guide.

The P2PE Vendor is required to give consideration to the impact of external threats and whether updates to the P2PE Solution, P2PE Component, or P2PE Application are necessary to address changes to the external threat environment.The updated P-AOV should be submitted via email to the P2PE Program Manager. If an updated P-AOV is not submitted in a timely manner, the P2PE Listing will be subject to early administrative expiry, as follows:

- On the Interim Assessment Due Date, the corresponding List will be updated to show the P2PE Listing in **Orange** for a period of 90 days.
- If the updated and complete P-AOV is received within this 90-day period, PCI SSC will update the corresponding List with the new Interim Assessment Due Date and remove the **Orange** status.
- If the updated and complete P-AOV is not received within this 90-day period, the corresponding List will be updated to show the P2PE Listing in **Red.**
- Once in **Red**, a full assessment (including applicable fees) is required to return the P2PE Listing status to good standing.

PCI SSC will, upon receipt of the updated *P2PE Attestation of Validation*: (i) review the submission for completeness; (ii) once completeness is established, update the List of Validated P2PE Solutions, List of Validated P2PE Components, or List of Validated P2PE Applications with the new Interim Assessment Due Date; and (iii) sign and return a copy of the updated *P2PE Attestation of Validation* to the P2PE Vendor.

5.2 Changes to P2PE Listings

P2PE Vendors may update listed P2PE Solutions, P2PE Components, or P2PE Applications for various reasons—for example, adding additional software applications. Changes do not have any impact on Interim Assessment Due Date or Reassessment Dates of P2PE Listings. Changes are categorized as follows:

Table 5.2.a – Changes to P2PE Listings for Solutions and Components

Change Type	Description
Designated	Designated Changes to P2PE Solutions or P2PE Components are limited to the following: ▪ Add/Remove P2PE Component; ▪ Add/Remove PCI-approved POI Device Type; ▪ Add/Remove P2PE Application. *See Section 5.2.2, "Designated Changes for P2PE Solutions and P2PE Components," for details.*
Interim	Interim Changes are not reported in detail but are addressed by the P2PE Vendor during the Annual Revalidation process via the Interim Self-Assessment. These changes will include: ▪ Any change that impacts compliance with the requirements of the P2PE Standard for a P2PE Solution or P2PE Component, but is not considered a "Designated Change." ▪ Any other change that does not impact compliance with the requirements of the P2PE standard for a given P2PE Product.
Administrative	Changes made to a listed P2PE Solution or P2PE Component that have no impact on the compliance of the P2PE Listing with any requirements of the P2PE Standard, but where the List of Validated P2PE Solutions or List of Validated P2PE Components is updated to reflect the change. Examples of administrative changes include, but are not limited to, corporate identify changes, P2PE Solution name changes, changes to listing details such as "Regions Served" (P2PE Solutions only) or "Description Provided by," etc. *See Section 5.2.1, "Administrative Changes for P2PE Listings," for details.*

Table 5.2.b – Changes to P2PE Listings for Applications

Change Type	Description
Delta (low impact)	Delta Changes are applicable only to P2PE Applications and are limited to the following: ▪ Changes where less than half of the P2PE Application's functionality is affected; ***and*** ▪ Changes where less than half of the Domain 2 Requirements/sub-Requirements are affected; ***and*** ▪ Changes where less than half the P2PE Application's code-base is changed. *See Section 5.2.4, "Delta Changes for P2PE Applications," for details.*
No Impact Change	Any other change that does not impact compliance with the requirements of the P2PE standard for a given P2PE Product. No Impact Changes are not reported in detail, but are addressed by the P2PE Vendor during the Annual Revalidation process.
Administrative	Changes made to a P2PE Application that have no impact on the compliance of the P2PE Listing with any requirements of the P2PE Standard, but where the List of Validated P2PE Applications is updated to reflect the change. Examples of administrative changes include, but are not limited to, corporate identify changes, P2PE Application name changes, and changes to listing details such as "Description Provided By Application Vendor," etc. *See Section 5.2.1, "Administrative Changes for P2PE Listings," for details.*

5.2.1 Administrative Changes for P2PE Listings

Administrative Changes are limited to updates where no changes to a listed P2PE Solution, P2PE Component, or P2PE Application have occurred but the P2PE Vendor wishes to request a change to the way the P2PE Solution, P2PE Component, or P2PE Application is currently listed on the corresponding List on the Website.

See Section 5.3, "Change Documentation," for specifics on the below:

The P2PE Vendor prepares a *Vendor Change Analysis* (for example, using the corresponding *P2PE Change Impact Template* in the Appendices) and submits it to the P2PE Assessor Company for review, along with the updated *P2PE Application Implementation Guide* or *P2PE Implementation Manual*. The change analysis must contain the following information at a minimum:

- Name and reference number of the Validated P2PE Listing
- Description of the change
- Description of why the change is necessary

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

Note:
Administrative Changes are only permissible to already-listed P2PE Solutions, P2PE Components, and P2PE Applications that have not expired.

If the P2PE Assessor Company agrees that the change as documented by the P2PE Vendor is eligible as an Administrative Change:

1) The P2PE Assessor Company must notify the P2PE Vendor that they agree;
2) The P2PE Vendor prepares and signs the corresponding P-AOV, and sends it to the P2PE Assessor Company;
3) If applicable, the P2PE Vendor modifies the *P2PE Instruction Manual* and/or *P2PE Application Implementation Guide* and/or completes a new VRA;
4) The P2PE Assessor Company completes the corresponding *P2PE Change Impact Template* in the Appendix;
5) The P2PE Assessor signs their concurrence on the P-AOV and forwards it, along with the corresponding P2PE Change Impact report, to PCI SSC;
6) PCI SSC will then issue an invoice to the P2PE vendor for the applicable change fee; and
7) Upon payment of the invoice, PCI SSC will review Administrative Change submission for quality assurance purposes.

If the P2PE Assessor Company does not agree with the P2PE Vendor that the change as documented in the *Vendor Change Analysis* is eligible as an Administrative Change, the P2PE Assessor Company returns the *Vendor Change Analysis* to the P2PE Vendor and works with the P2PE Vendor to consider the actions necessary to address the P2PE Assessor Company's observations.

Following successful PCI SSC quality assurance review of the change, PCI SSC will:

1) Amend the corresponding List of Validated P2PE Solutions, List of Validated P2PE Components, or List of Validated P2PE Applications on the Website accordingly with the new information; and
2) Sign and return a copy of the corresponding *P2PE Attestation of Validation* to both the P2PE Vendor and the P2PE Assessor Company. The Revalidation date of the updated listing will be the same as that of the parent listing.

For quality issues associated with any aspect of the submission, PCI SSC communicates those issues to the P2PE Assessor Company. PCI SSC reserves the right to reject any P2PE Change Impact document if it determines that a change described therein and purported to be an Administrative Change by the P2PE Assessor Company or P2PE Vendor is ineligible for treatment as an Administrative Change.

5.2.2 Designated Changes for P2PE Solutions and P2PE Components

Designated Changes are changes made to a listed P2PE Solution or P2PE Component (where applicable) to:

- Add/remove a validated POI device; ***or***
- Add/remove a validated P2PE Application ; ***or***
- Add/remove a validated P2PE Component used in a P2PE Solution

Designated Changes result in an amendment to a P2PE Solution or P2PE Component as currently listed on the corresponding List on the Website.

See Section 5.3, "Change Documentation," for specifics on the below.

The P2PE Vendor prepares a *Vendor Change Analysis* (for example, using the corresponding *P2PE Change Impact Template* in the Appendices) and submits it to the P2PE Assessor Company for review, along with the updated *P2PE Implementation Manual*, as applicable. The change analysis must contain the following information at a minimum:

- Name and reference number of the Validated P2PE Listing
- Description of the change
- Description of why the change is necessary

It is recommended that the P2PE Vendor submit the *Vendor Change Analysis* to the same P2PE Assessor Company used for the original assessment.

If the P2PE Assessor Company agrees that the change as documented by the P2PE Vendor is eligible as a Designated Change:

1) The P2PE Assessor Company must notify the P2PE Vendor that they agree;
2) If applicable, the P2PE Vendor modifies the *P2PE Instruction Manual* and/or completes a new VRA and submits this to the P2PE Assessor Company;
3) The P2PE Assessor Company must perform an assessment of the requirements of the P2PE Standard that are affected by the change. Details of the tests that must be performed are available within the "Designated Changes" sections of the corresponding *P2PE Change Impact Template* in the Appendices.
4) The P2PE Assessor Company completes the corresponding *P2PE Change Impact Template in the Appendices* and must produce a red-lined P-ROV and document the testing completed per PCI SSC requirements;
5) The P2PE Vendor prepares and signs the corresponding P-AOV and sends it to the P2PE Assessor Company;
6) The P2PE Assessor signs its concurrence on the P-AOV and forwards it along with the completed *P2PE Change Impact Template,* the P2PE Solution's updated *P2PE Instruction Manual* (as applicable), VRA (as applicable), and the red-lined P-ROV to PCI SSC;
7) PCI SSC will then issue an invoice to the P2PE Vendor for the applicable change fee; and
8) Upon payment of the invoice, PCI SSC will review the Designated Change submission for quality assurance purposes.

If the P2PE Assessor Company does not agree with the P2PE Vendor that the change as documented in the *Vendor Change Analysis* is eligible as a Designated Change, the P2PE Assessor Company returns the *Vendor Change Analysis* to the P2PE Vendor and works with the P2PE Vendor to consider the actions necessary to address the P2PE Assessor Company's observations.

Following successful PCI SSC quality assurance review of the change, PCI SSC will:

1) Amend the corresponding List of Validated P2PE Solutions or List of Validated P2PE Components on the Website accordingly with the new information; and
2) Sign and return a copy of the corresponding *P2PE Attestation of Validation* to both the P2PE Vendor and the P2PE Assessor Company. The Revalidation date of the updated listing will be the same as that of the parent listing.

For quality issues associated with any aspect of the submission, PCI SSC communicates those issues to the P2PE Assessor Company. PCI SSC reserves the right to reject any *P2PE Change Impact* document if it determines that a change described therein and purported to be a Designated Change by the P2PE Assessor Company or P2PE Vendor is ineligible for treatment as a Designated Change.

5.2.3 Wildcards for P2PE Applications

All P2PE Application changes must result in a new application version number; however, whether this affects the version number listed on the Website depends on the nature of the change and the Vendor's defined, documented versioning methodology. The use of wildcards may be permitted for managing the versioning methodology for No Impact changes only.

Note: *Wildcards may only be substituted for elements of the version number that represent non-security-impacting changes; the use of wildcards for any change that has an impact on security or any P2PE Requirements is prohibited.*

Only those P2PE applications that have had the P2PE Vendor's wildcard versioning methodology assessed to P2PE v2 by a PA-QSA (P2PE) Assessor Company are eligible for wildcard usage and listing on the Website with wildcards. Changes falling within the scope of wildcard usage are not required to be advised to PCI SSC; therefore, any such changes will not result in an update to the P2PE Application listing on the Website. See Appendix H, "P2PE Application Software Version Methodology," for additional information regarding the use of wildcards.

5.2.4 Delta Changes for P2PE Applications

Delta Changes are changes made to a listed P2PE Application and are limited to the following:

- Changes where less than half of the P2PE Application's functionality is affected; ***and***
- Changes where less than half of the Domain 2 Requirements/sub-Requirements are affected; ***and***
- Changes where less than half the P2PE Application's code-base is changed.

Since the number of possible P2PE Application changes and their impact cannot be determined in advance, the type of assessment required must be considered on a per-case basis. P2PE Application Vendors are encouraged to contact the P2PE Assessor Company that performed the last full validation of the P2PE Application for guidance. The P2PE Assessor Company engaged by the P2PE Vendor for this purpose then determines whether a full P2PE Application Assessment or Delta Assessment of the P2PE Application is required, based on the degree to which the changes impact the security and/or P2PE-related functions of the P2PE Application, the impact to P2PE Requirements, and/or the scope of the changes being made.

See Section 5.3, "Change Documentation," for specifics on the below.

The P2PE Application Vendor prepares a *Vendor Change Analysis* (for example, using the corresponding *P2PE Change Impact Template* in the Appendices) and submits it to the P2PE Assessor Company for review, along with the updated *P2PE Application Implementation Guide*. The change analysis must contain the following information at a minimum:

- Name and reference number of the Validated P2PE Application Listing
- Description of the change
- Description of why the change is necessary

It is highly recommended that the P2PE Application Vendor submit the *Vendor Change Analysis* to the same P2PE Assessor Company used for the original assessment. If the P2PE Assessor Company does not agree with the P2PE Application Vendor that the change as documented in the *Vendor Change Analysis* is eligible as a Delta Change, the P2PE Assessor Company returns the *Vendor Change Analysis* to the P2PE Application Vendor and works with the P2PE Application Vendor to consider the actions necessary to address the P2PE Assessor Company's observations.

If the P2PE Assessor Company agrees that the change as documented by the P2PE Application Vendor is eligible as a Delta Change:

1) The P2PE Assessor Company must notify the P2PE Application Vendor that they agree;
2) The P2PE Application Vendor modifies the *P2PE Application Implementation Guide* and/or completes a new VRA (if applicable) and sends it to the P2PE Assessor Company;
3) The P2PE Assessor Company performs a Delta Assessment of the P2PE Application for the P2PE Requirements affected by the changes;
4) The P2PE Assessor Company tests the P2PE Application's affected functionality;
5) The P2PE Assessor Company completes the appropriate *P2PE Change Impact Template* in the Appendices, providing the detail of the changes to the P2PE Application, and must produce a red-lined P-ROV and document the testing completed per PCI SSC requirements;
6) The P2PE Application Vendor prepares and signs the corresponding P-AOV and sends it to the P2PE Assessor Company;
7) The P2PE Assessor signs its concurrence on the P-AOV and forwards it, along with the completed *P2PE Change Impact* document, the P2PE Application's updated *P2PE Implementation Guide*, the P2PE Vendor's signed current VRA (if not already on file with PCI SSC), and the red-lined Application P-ROV to PCI SSC;
8) PCI SSC will then issue an invoice to the P2PE Application Vendor for the applicable change fee; and

Upon payment of the invoice, PCI SSC will review the Delta Change submission for quality assurance purposes.Following successful PCI SSC quality assurance review of the change, PCI SSC will:

1) Amend the corresponding List of Validated P2PE Applications on the Website accordingly with the new information; and
2) Sign and return a copy of the corresponding *P2PE Attestation of Validation* to both the P2PE Application Vendor and the P2PE Assessor Company. The expiry date of this newly listed P2PE Application will be the same as that of the parent P2PE Application.

For quality issues associated with any aspect of the submission, PCI SSC communicates those issues to the P2PE Assessor Company. PCI SSC reserves the right to reject any *P2PE Change Impact* document if it determines that a change described therein and purported to be a Delta Change by the P2PE Assessor Company or P2PE Application Vendor is ineligible for treatment as a Delta Change.

Delta assessment example:

Assuming the above defined criteria for a delta assessment is met, examples of low-impact changes to a Validated P2PE application that could be included in a delta assessment may include, but are not limited to:

- Addition of a POI device type to be supported by the P2PE Application
- Discontinuing support of a POI device currently supported by the P2PE Application
- Inclusion of updates or patches
- Recompilation of unchanged code-base

5.3 Change Documentation

Administrative Change (All P2PE Products)	Interim Self-Assessment (All P2PE Products)	Delta Change (Application)	Designated Change (Solution or Component)
▪ *P2PE Attestation Of Validation* ▪ P2PE Change Impact document** ▪ *P2PE Implementation Guide ** ▪ *P2PE Instruction Manual ** ▪ Current VRA* ▪ Fee	▪ *P2PE Attestation Of Validation*	▪ *P2PE Attestation Of Validation* ▪ P2PE Change Impact document*** ▪ Red-lined P-ROV ▪ *P2PE Implementation Guide* ▪ Current VRA* ▪ Fee	▪ *P2PE Attestation Of Validation* ▪ P2PE Change Impact document ** ▪ Red-lined P-ROV ▪ *P2PE Implementation Guide ** ▪ *P2PE Instruction Manual ** ▪ Current VRA* ▪ Fee

***** *If applicable*

****** ***Note:*** *The P2PE Change Impact – P2PE Solutions and P2PE Components documents in the Appendix are mandatory for the P2PE Assessor Company for submitting Administrative and Designated Changes to PCI SSC on behalf of P2PE Solution Providers and P2PE Component Service Providers*.

******* ***Note:*** *The P2PE Change Impact – P2PE Applications document in the Appendix is mandatory for the P2PE Assessor Company for submitting Administrative and Delta Changes to PCI SSC on behalf of the P2PE Application Vendor, but may also be used by Vendors as a* Vendor Change Analysis.

5.4 Renewing Expiring Listings

As a P2PE Product listing approaches its reassessment date, PCI SSC will notify the P2PE Vendor of the pending expiration. The two options available for Vendor consideration are either new validation or expiry:

- **New Validation**: If the P2PE Vendor wishes the P2PE Product listing to remain on the corresponding P2PE Product list on the Website, the P2PE Vendor must contact a P2PE Assessor Company to have the P2PE Product fully re-evaluated against the then-current version of the P2PE Standard, resulting in a new Acceptance, on or before the applicable Reassessment Date. This reassessment must follow the same process as an initial P2PE Assessment of the applicable P2PE Product.
- **Expiry:** Listings of P2PE Products for which a new Acceptance has not occurred on or before the applicable expiration date/reassessment date, will appear in **Orange** for the first 90 days, and in **Red** thereafter.

5.5 Validation Maintenance Fees

If a listed P2PE Solution, P2PE Component, or P2PE Application is revised, the P2PE Vendor is required to pay the applicable change fee to PCI SSC.

For any change affecting the listing of a validated P2PE Solution, P2PE Component, or P2PE Application, the applicable fee will be invoiced and must be received by PCI SSC for the changes to be Accepted and added to the corresponding P2PE List. Upon Acceptance, PCI SSC will sign and return a copy of the P-AOV to both the P2PE Vendor and the P2PE Assessor Company.

There is no PCI SSC fee associated with the processing of Interim Self-Assessments.

All P2PE Program fees are posted on the Website. Program fees are non-refundable and are subject to change upon posting of revised fees on the Website.

Note:

The P2PE Vendor pays all P2PE Assessment-related fees directly to the P2PE Assessor. (These fees are negotiated between the P2PE Vendor and the P2PE Assessor Company.)

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

A parent P2PE listing must already exist on the corresponding List and not yet have expired in order to have a change Accepted and Listed.

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

In the event of a Security Issue (defined in the VRA) relating to a Validated P2PE Product, the VRA requires the applicable P2PE Vendor to notify PCI SSC.

5.6.1 Notification and Timing

Notwithstanding any other legal obligations, pursuant to the VRA, the P2PE Vendors are required to notify PCI SSC of all such Security Issues within the period of time specified in the VRA, including the related information pursuant to the VRA, and to provide follow-up information which may include (without limitation) an assessment of any impact (possible or actual) that the Security Issue has had or may or will have.

5.6.2 Notification Format

The P2PE Vendor's Security Issue notification to PCI SSC must be in writing in accordance with the VRA, and should be preceded by a phone call to the PCI P2PE Program Manager at (781) 876-8855.

5.6.3 Notification Details

Information provided pursuant to such written notice and to the PCI P2PE Program Manager should include (but is not limited to) the following:

- The name, PCI SSC approval number, and any other relevant identifiers of each of the P2PE Vendor's P2PE Product(s) affected by the Security Issue;
- A description of the general nature of the Security Issue;
- The P2PE Vendor's good-faith assessment, to its knowledge at the time, as to the scope and severity of the vulnerability or vulnerabilities associated with the Security Issue (using CVSS or other industry-accepted standard scoring); and
- Assurance that the P2PE Vendor is following its Vulnerability Handling Policies.

5.6.4 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 Product, PCI SSC may take the actions specified in the VRA and additionally, may:

- Notify Participating Payment Brands that a Security Issue has occurred.
- Request a copy of the latest version of the P2PE Vendor's Vulnerability Handling Policies.
- Communicate with the P2PE Vendor about the Security Issue and, where possible and permitted, share information relating to the Security Issue.
- Support the P2PE Vendor's efforts to mitigate or prevent further Security Issues.
- Support the P2PE Vendor's efforts to correct any Security Issues.
- Work with the P2PE Vendor to communicate and cooperate with appropriate law enforcement agencies to help mitigate or prevent further Security Issues.

5.6.5 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, List of Validated P2PE Components, or List of Validated P2PE Applications) any P2PE Product in accordance with the VRA, in instances including but not limited to, if PCI SSC reasonably determines that (a) the P2PE Product does not provide sufficient protection against current threats and conform to the requirements of the P2PE Program, (b) the continued Acceptance of the P2PE Product represents a significant and imminent security threat to its users, or (c) such action is necessary in light of a related Security Issue.

6 P2PE Assessor Reporting Considerations

6.1 P-ROV Acceptance Process Overview

The P2PE Assessor Company performs the P2PE Assessment in accordance with the P2PE Standard and produces a P-ROV that is shared with the P2PE Vendor.

When the P-ROV has all items in place, and where the P2PE Vendor seeks to have the P2PE Product listed on the Website, the P2PE Assessor Company submits the P-ROV and all other required materials to PCI SSC. If the P-ROV does not have all items in place, the P2PE Vendor must address those items, and the P2PE Assessor must update the P-ROV prior to submission to PCI SSC.. Once the P2PE Assessor Company is satisfied that all documented issues have been resolved by the P2PE Vendor, the P2PE Assessor Company submits the P-ROV and all other required materials to PCI SSC.

Note:

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

Once PCI SSC receives the P-ROV and all other required materials and applicable fees, PCI SSC reviews the submission from a quality assurance perspective and determines whether it is acceptable. Subsequent iterations will also be responded to, typically within 30 calendar days of receipt. If the P-ROV meets all applicable quality assurance requirements (as documented in the *QSA Qualification Requirements* and related P2PE Program materials), PCI SSC sends a countersigned P-AOV to both the P2PE Vendor and the P2PE Assessor Company and adds the product to the List of Validated P2PE Solutions, List of Validated P2PE Components, or List of Validated P2PE Applications, as applicable.

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

P-ROVs that have been returned to the P2PE Assessor Company for correction must be resubmitted to the PCI SSC within 30 days of the preceding submission. If this is not possible, the P2PE Assessor Company must inform the PCI SSC of the timeline for response. Lack of response on P-ROVs returned to the P2PE Assessor Company 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.

6.2 Delivery of the P-ROV and Related Materials

For P2PE Solutions, P2PE Components, and P2PE Applications to be listed on the Website, all documents required in connection with the P2PE validation process must be submitted to PCI SSC by the P2PE Assessor Company, through a secure submissions website designated by PCI SSC (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 be rejected by PCI SSC.

6.2.1 Access to the Portal

Once a P2PE Assessor Company has had its first employee successfully complete the individual P2PE Assessor qualification 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 Assessor Employees.

6.2.2 Resubmissions

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

6.3 Assessor Quality Management Program

As stated in the *Qualification Requirements – For Point-to-Point Qualified Security Assessors* and the *P2PE Assessor Addendum*, 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.

6.3.1 P-ROV Submission Review

PCI SSC's Assessor Quality Management Team ("AQM") reviews each P-ROV submission after the invoice for the P2PE Acceptance Fee has been paid by the P2PE Vendor. Administrative review will be performed in "pre-screening" to ensure that the submission is complete; then an AQM Analyst will review the submission in its entirety

The AQM Analyst will review the P2PE submission first to determine whether the candidate P2PE Product is eligible for validation as described in the *P2PE Program Guide*. If there is question as to eligibility, the AQM Analyst will contact the P2PE Assessor Company for additional information. If the P2PE submission is determined to be ineligible for validation under the P2PE Program, the P-ROV will be rejected. The P2PE Assessor Company will receive a letter of rejection with optional instructions for appealing this rejection.

If the P2PE submission is determined to be eligible for validation under the P2PE Program and the submission is complete, the AQM Analyst will conduct a complete review of the P-ROV submissions and supporting documentation provided or subsequently requested by PCI SSC. Any comments or feedback from the AQM Analyst will be made via the Portal, and the P2PE Assessor Company is expected to address all comments and feedback in a timely manner. The AQM Analyst's role is to ensure sufficient evidence and detail are present in the P2PE Assessor Company's submission to provide reasonable assurance that the P2PE Assessment was performed in accordance with Program requirements and quality standards.

6.3.2 P2PE Assessor Quality Audit

The purpose of the P2PE Assessor Company audit process is to provide reasonable assurance that the assessment of P2PE Solutions, P2PE Components, and P2PE Applications and overall quality of report submissions remain at a level that is consistent with the objectives of the *P2PE Program Guide* and supporting PCI SSC documentation.

QSA Company audits are provided for in the *QSA Qualification Requirements*, and P2PE Assessor Companies are subject to audits of their work as P2PE Assessor Companies under the *QSA Qualification Requirements* at any time. This may include, but not be limited to, review of completed reports, work papers, and onsite visits with P2PE Assessor Companies to audit internal QA programs, at the expense of the P2PE Assessor Company. Refer to the *QSA Qualification Requirements* for information on PCI SSC's audit process.

6.3.3 P2PE Assessor Company Status

The P2PE Program recognizes several status designations for P2PE Assessor Companies: "In Good Standing," "Remediation," and "Revocation." The status of a P2PE Assessor Company is initially "In Good Standing" but may change based on quality concerns, feedback from clients and/or Participating Payment Brands, administrative issues, or other factors. These status designations are described further below.

Note: *These status designations are not necessarily progressive: Any P2PE Assessor Company's status may be revoked or its P2PE Assessor Addendum (defined in the P2PE Qualification Requirements) terminated in accordance with the P2PE Assessor Addendum; and accordingly, if warranted, a P2PE Assessor Company may move directly from "In Good Standing" to "Revocation."*

Nonetheless, in the absence of severe quality concerns, P2PE Assessor Companies with quality issues are generally first addressed through the Remediation process in order to promote improved performance.

6.3.3.1 In Good Standing

P2PE Assessor Companies are expected to maintain a status of In Good Standing while participating in the P2PE Program. Reviews of each submission and the overall quality of submissions are conducted by PCI SSC to detect any deterioration of quality levels over time. P2PE Assessor Companies may also be subject to periodic audit by PCI SSC at any time.

6.3.3.2 Remediation

A P2PE Assessor Company and/or P2PE Assessor Employee may be placed into Remediation for various reasons, including quality concerns or administrative issues—such as failure to meet any requalification requirements, failure to submit required information, etc. P2PE Assessor Companies in Remediation are listed on the Website in **Red**, indicating their remediation status without further explanation as to why the designation is warranted.

If administrative or non-severe quality problems are detected, PCI SSC will typically recommend participation in the Remediation program. Remediation provides an opportunity for P2PE Assessor Companies and/or Employees to improve performance by working closely with PCI SSC staff; and in the absence of participation, quality issues may increase. Additionally, Remediation helps to assure that the baseline standard of quality for P2PE Assessor Companies and/or Employees is upheld. Refer to the *QSA Qualification Requirements* for further detail on the Remediation Process.

6.3.3.3 Revocation

Serious quality concerns may result in revocation of P2PE Assessor Company and/or P2PE Assessor Employee qualification and/or termination of the P2PE Assessor Addendum. When a P2PE Assessor Company and/or P2PE Assessor Employee qualification is revoked, the 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 Assessments for which it was engaged prior to the effective date of the Revocation.

Note:

If a P2PE Solution, P2PE Component, or P2PE Application included on the List of Validated Solutions, List of Validated Components, or List of Validated Applications is compromised due to P2PE Assessor Company and/or Employee error, that P2PE Assessor Company and/or Employee may immediately be placed into Remediation or its P2PE qualification status revoked.

The P2PE Assessor Company and/or P2PE Assessor Employee may appeal the Revocation but, unless otherwise approved by PCI SSC in writing in each instance, will not be permitted to perform P2PE Assessments, process P-ROVs, or otherwise participate in the P2PE Program. The P2PE Assessor Company and/or P2PE Assessor Employee may reapply at a later date of two years after revocation, so long as 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 the relevant PCI SSC program documents.

Appendix A: P2PE Products and Acceptance

Acceptance of a given P2PE Product by the PCI SSC only applies to the specific P2PE Solution, P2PE Component, or P2PE Application that has been validated by a P2PE Assessor and subsequently Accepted by PCI SSC (the "Accepted Product"). If any aspect of a P2PE Product is different from that which was validated by the P2PE Assessor and Accepted by PCI SSC—even if the different P2PE Product (the "Alternate Product") conforms to the basic product description of the Accepted Product— the Alternate Product should not be considered Accepted by PCI SSC, nor promoted as Accepted by PCI SSC.

No P2PE Vendor or other third party may refer to a P2PE Product as "PCI Approved," or "PCI SSC Approved" or otherwise state or imply that PCI SSC has, in whole or part, approved any aspect of a P2PE Vendor or its P2PE Product, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with PCI SSC, or in a corresponding P-AOV provided by PCI SSC. All other references to PCI SSC's acceptance of a P2PE Product 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 Product 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*

Company

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

P2PE Solution Identifier

P2PE Solution Identifiers refers to a subset of fields in the listing below the "Company" entry 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
- Solution Details

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 Website; this number is unique per P2PE Solution Provider and will remain the same for the life of the listing.

  An example reference number is 2015-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

- **Solution Details**

  Clicking on this link brings up a list of details specific to this Solution consisting of the following fields (fields are explained in detail below):

  - PTS Devices Supported
  - P2PE Application(s) Supported
  - P2PE Components

Solution Details: Detail

- **PTS Devices Supported**

  This section identifies the PCI-approved POI devices validated for use with this P2PE Solution and will include relevant PCI PTS reference numbers and 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 Supported**

  This section identifies the P2PE Applications validated for use with this P2PE Solution and listed on the List of Validated P2PE Applications, and will include the expiry date of the P2PE Application's approval.

  While a P2PE Solution may include applications that were evaluated per relevant requirements in the P2PE Standard, those are not listed within the P2PE Solution or within the List of Validated P2PE Applications. Any use of such an application in another P2PE Product would require either independent listing as a P2PE Application, if eligible, or assessment as part of each P2PE Solution the application is part of.

- **P2PE Components**

  This section identifies the P2PE Components validated for use with this P2PE Solution and listed on the List of Validated P2PE Components, and will include the expiry date of the P2PE Component's approval.

  While a P2PE Solution may include third-party services (including services potentially eligible for Listing as a P2PE Component, such as CA/RA or KIF), those are not listed within the P2PE Solution or within the List of Validated P2PE Components. Any use of such a component in another P2PE Product would require either independent listing as a P2PE Component, if eligible, or assessment as part of each P2PE Solution the application is part of.

P2PE Version

"P2PE Version" is used by PCI SSC to denote the standard, and the specific version thereof, used to assess the compliance of a Validated P2PE Solution.

P2PE Assessor

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

Regions Served

This section allows for the submission of a description of geographic regions in which this P2PE Solution is available—e.g., Europe, Asia-Pacific.

Reassessment Date

The **Reassessment 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 Solution Provider

This section allows for the Solution Provider's submission in the Portal via the QSA (P2PE) of a description for the P2PE Solution to be used in the List of Validated P2PE Solutions, should the Solution P-ROV be Accepted.

Appendix C: Elements for the *List of Validated P2PE Components*

There are four recognized types of Component Providers for the List of Validated Components, which are represented across the top of the List of Validated Components – Encryption-management services ("Encryption Mgmt"), Decryption-management services ("Decryption Mgmt"), Certification Authority/Registration Authority Services (CAs/RAs), and Key-Injection facility services ("KIFs"). Each contain the same listing elements below:

Company

This entry denotes the **P2PE Component Provider** for the Validated P2PE Component.

P2PE Component Identifiers

P2PE Component Identifier refers to a subset of fields in the listing below the "Company" entry used by PCI SSC to denote relevant information for each Validated P2PE Component, consisting of the following fields (fields are explained in detail below):

- P2PE Component Name
- Reference Number
- Component Details

P2PE Component Identifier: Detail

- **P2PE Component Name**

  P2PE Component Name is provided by the P2PE Component Provider, and is the name by which the P2PE Component Provider's services are known.

- **Reference Number**

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

  An example reference number is 2015-XXXXX.XXX consisting of the following:

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

- **Component Details**

Clicking on this link brings up a list of details specific to this Component consisting of the following fields (fields are explained in detail below):

- PTS Devices Supported
- P2PE Application(s) Supported
- P2PE Components

Note:

Not all component details will apply, as each component service is different. For example, Encryption-management services may have PTS Devices Supported, others likely will not.

Component Details: Detail

- **PTS Devices Supported**

  This section identifies the PCI-approved POI devices validated for use with this P2PE Component and will include relevant PCI PTS reference numbers and 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 Supported**

  This section identifies the P2PE Applications validated for use with this P2PE Component and listed on the List of Validated P2PE Applications, and will include the expiry date of the P2PE Application's approval.

- **P2PE Components**

  This section identifies the P2PE Components validated for use with this P2PE Component and listed on the List of Validated P2PE Components, and will include the expiry date of the P2PE Component's approval.

  While a P2PE Component may include third-party services (including those offering services potentially eligible for Listing as a P2PE Component, such as CA/RA or KIF), those are not listed within the P2PE Component or within the List of Validated P2PE Components. Any use of such a component in another P2PE Product would require either independent listing as a P2PE Component, if eligible, or assessment as part of each P2PE Solution the application is part of.

P2PE Version

"P2PE Version" is used by PCI SSC to denote the standard, and the specific version thereof, used to assess the compliance of a Validated P2PE Component.

P2PE Assessor

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

Reassessment Date

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

Description Provided by Component Provider

This section allows for the Component Provider's submission in the Portal via the QSA (P2PE) of a description of the P2PE Component to be used in the List of Validated P2PE Components, should the Component P-ROV be Accepted.

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

Company

This entry denotes the P2PE Application Vendor for the Validated P2PE Application.

P2PE Application Identifiers

P2PE Application Identifiers refers to a subset of fields in the listing below the Company entry 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
- Application Details

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. The Application Name cannot contain any variable characters.

- **P2PE Application Version #**

  P2PE Application Version # represents the specific application version reviewed in the P2PE Application Assessment. The format of the version number:

  - Is set by the vendor,
  - May consist of a combination of alphanumeric characters and
  - Must be consistent with the Application Vendor's published versioning methodology for this product as documented in the *P2PE Application Implementation Guide*.

  Note:
  See Appendix H: P2PE Application Software Versioning Methodology for details about content to include in the Application P-ROV and P2PE Application Implementation Guide for the Application Vendor's versioning methods.

- **Reference Number**

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

  An example reference number is 2015-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)

- **Application Details**

  Clicking on this link brings up a list of details specific to this Component consisting of the following fields (fields are explained in detail below):

  - PTS Devices Supported

Application Details: Detail

- **PTS Devices Supported**

  This section identifies the PCI-approved POI devices validated for use with this P2PE Application and will include relevant PCI PTS reference numbers and 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 Version

"P2PE Version" is used by PCI SSC to denote the standard, and the specific version thereof, used to assess the compliance of a Validated P2PE Application.

P2PE Assessor

This entry denotes the name of qualified **PA-QSA (P2PE) Assessor Company** that performed the validation and determined that the application is compliant with the P2PE Standard.

Reassessment Date

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

Description Provided by Application Vendor

This section allows for the Application Vendor's submission in the Portal via the PA-QSA (P2PE) of a description of the P2PE Application that is to be used in the List of Validated P2PE Applications should the Application P-ROV be Accepted. This must be a factual description of the application functionality. The description must not:

- Contradict any PCI SSC program or requirement.
- Make misleading claims about the application.
- Claim the application is valid under another PCI SSC program or standard.

PCI SSC recommends keeping the description concise and including only pertinent information about the application. All descriptions must be acceptable to PCI SSC, which reserves the right to modify any description at any time.

Appendix E: Change Impact Template for P2PE Solutions

This *P2PE Change Impact Template* is required for Administrative Change and Designated Change submissions for P2PE Solution listings. Always refer to the applicable *P2PE Program Guide* for information on any P2PE listing changes.

The P2PE Vendor and/or P2PE Assessor Company must complete each section of this document and all other required documents based on the type of change. The P2PE Assessor Company is required to submit this P2PE Change Impact along with supporting documentation to PCI SSC for review.

Part 1. P2PE Listing Details, Contact Information, and Change Type

P2PE Listing Details			
P2PE Solution Name		Validated Listing Reference #	
Type of Change *(Please check)*	☐ Administrative *(Complete Part 2)*	☐ Delta *(Complete Part 3)*	
Submission Date			

P2PE Vendor Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	
QSA (P2PE) Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	

Part 2. Details for Administrative Change (if indicated at Part 1)

Administrative Change Revision			
Current Company Name		Revised Company Name *(if applicable)*	
Current P2PE Solution Name		Revised P2PE Solution Name *(if applicable)*	
Additional details, as applicable			

Part 3. Details for Designated Change (if indicated at Part 1)

Designated Change Revision		
Identify the type of designated changes applicable to this submission and complete the appropriate sections of this P2PE Change Impact Template (check all that apply). *Please refer to the* P2PE Program Guide *for details about each type of designated change.*		
Add/Remove POI Device Type *(Complete Part 3a)*	☐ Add	☐ Remove
Add/Remove P2PE Application *(Complete Part 3b)*	☐ Add	☐ Remove
	Application Version Number:	
Add/Remove P2PE Component *(Complete Part 3c)*	☐ Add	☐ Remove
Description of changes to the P2PE Solution or P2PE Component:		
Description of how Designated Change impacts the P2PE Solution's functionality		
Additional details, as applicable		

Part 3a. Add/Remove POI Device Type (if indicated at Part 3)

POI Device Type		
Adding for inclusion in listing or removal from listing?	☐ Addition/Inclusion in listing *(Red-lined P-ROV review required, see details below)*	☐ Removal from listing *(No Red-lined P-ROV review required)*
POI Device type name/identifier		
POI Device manufacturer, model, and number		
PTS approval number for POI Device		
POI Device Hardware version #		
POI Device Firmware version #		

Perform a red-lined P-ROV review for the added Device using the table below as a minimum set of testing procedures.

P2PE Requirements (including all testing procedures)
☐ All of 1A-1.1
☐ 1B -1.1
☐ 1B-2.2
☐ 1B-2.3
☐ 1C-2
☐ 3C-1

Part 3b. Add/Remove P2PE Application (if indicated at Part 3)

P2PE Applications					
Adding for inclusion in listing or removal from listing?			☐ Addition/Inclusion in listing *(Red-lined P-ROV review required, see details below)*	☐ Removal from listing *(No Red-lined P-ROV review required)*	
Application Name	Application version #	Application vendor name	Application reference #	Brief description of Application function/purpose	POI Device type name/identifier Application is installed on

Perform a red-lined P-ROV review for the added Application using the table below as a minimum set of testing procedures.

P2PE Requirements (including all testing procedures)
☐ 1A-2.1
☐ 1A-2.2
☐ 1B-1.1.1
☐ 1B-3.2
☐ 1C-1.1
☐ 1C-1.2
☐ All of 1D-1
☐ 1D-2.1

Part 3c. Add/Remove P2PE Component (if indicated at Part 3)

P2PE Component					
Adding for inclusion in listing or removal from listing?	☐ Addition/Inclusion in listing *(Red-lined P-ROV review required, see details below)*		☐ Removal from listing *(No Red-lined P-ROV review required)*		
P2PE Component Provider Name	Type of P2PE Component (select only one)				SSC Listing Number
	KIF	CA/RA	Encryption Mgmt.	Decryption Mgmt.	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	

Perform a red-lined P-ROV review for the added P2PE Component using the table below as a minimum set of testing procedures.

P2PE Requirements (including all testing procedures)
☐ All of 3A-1
☐ 3A-2 (as applicable)
☐ All of 3B-1
☐ 3C-1 (as applicable)

Appendix F: Change Impact Template for P2PE Components

This *P2PE Change Impact Template* is required for Administrative Change and Designated Change submissions for P2PE Component listings. Always refer to the applicable *P2PE Program Guide* for information on any P2PE listing changes.

The P2PE Vendor and/or P2PE Assessor Company must complete each section of this document and all other required documents based on the type of change. The P2PE Assessor Company is required to submit this *P2PE Change Impact* along with supporting documentation to PCI SSC for review.

Part 1. P2PE Listing Details, Contact Information, and Change type

P2PE Listing Details					
P2PE Component Provider Name	Type of P2PE Component (select only one)				SSC Listing Number
	KIF	CA/RA	Encryption Mgmt.	Decryption Mgmt.	
	☐	☐	☐	☐	
Type of Change *(Please check)*	☐ Administrative *(Complete Part 2)*		☐ Delta *(Complete Part 3)*		
Submission Date					

P2PE Vendor Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	
QSA (P2PE) Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	

Part 2. Details for Administrative Change (if indicated at Part 1)

Administrative Change Revision			
Current Company Name		Revised Company Name *(if applicable)*	
Current P2PE Component Name		Revised P2PE Component Name *(if applicable)*	
Additional details, as applicable			

Part 3. Details for Designated Change (if indicated at Part 1)

Designated Change Revision		
Identify the type of designated changes applicable to this submission and complete the appropriate sections of this *P2PE Change Impact Template* (check all that apply). *Please refer to the* P2PE Program Guide *for details about each type of designated change.*		
Add/Remove POI Device Type *(Complete Part 3a)*	☐ Add	☐ Remove
Add/Remove P2PE Application * *(Complete Part 3b)*	☐ Add	☐ Remove
	Version Number of the Application:	
Add/Remove P2PE Component *(Complete Part 3c)*	☐ Add	☐ Remove
Description of changes to the P2PE Component:		
Description of real or potential impact to the P2PE Solution(s) it is used in		
Additional details, as applicable		

Part 3a. Add/Remove POI Device Type (if indicated at Part 3)

POI Device Type		
Adding for inclusion in listing or removal from listing?	☐ Addition/Inclusion in listing *(Red-lined P-ROV review required, see details below)*	☐ Removal from listing *(No Red-lined P-ROV review required)*
POI Device type name/identifier		
POI Device manufacturer, model, and number		
PTS approval number for POI Device		
POI Device Hardware version #		
POI Device Firmware version #		

Perform a red-lined P-ROV review for the added Device using the table below as a minimum set of testing procedures.

P2PE Requirements (including all testing procedures)
☐ All of 1A-1.1
☐ 1B -1.1
☐ 1B-2.2
☐ 1B-2.3
☐ 1C-2

Part 3b. Add/Remove P2PE Application (if indicated at Part 3)

P2PE Applications					
Adding for inclusion in listing or removal from listing?			☐ Addition/Inclusion in listing *(Red-lined P-ROV review required, see details below)*	☐ Removal from listing *(No Red-lined P-ROV review required)*	
Application Name	Application version #	Application vendor name	Application reference #	Brief description of Application function/purpose	POI Device type name/identifier Application is installed on

Perform a red-lined P-ROV review for the added Application using the table below as a minimum set of testing procedures.

P2PE Requirements (including all testing procedures)
☐ 1A-2.1
☐ 1A-2.2
☐ 1B-1.1.1
☐ 1B-3.2
☐ 1C-1.1
☐ 1C-1.2
☐ All of 1D-1
☐ 1D-2.1

Part 3c. Add/Remove P2PE Component (if indicated at Part 3)

P2PE Component					
Adding for inclusion in listing or removal from listing?	☐ Addition/Inclusion in listing *(Red-lined P-ROV review required, see details below)*		☐ Removal from listing *(No Red-lined P-ROV review required)*		
P2PE Component Provider Name	Type of P2PE Component (select only one)				SSC Listing Number
	KIF	CA/RA	Encryption Mgmt.	Decryption Mgmt.	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	

Perform a red-lined P-ROV review for the added P2PE Component using the table below as a minimum set of testing procedures.

P2PE Requirements (including all testing procedures)
☐ All of 3A-1
☐ 3A-2 (as applicable)
☐ All of 3B-1
☐ 3C-1 (as applicable)

Appendix G: Change Impact Template for P2PE Applications

This *P2PE Change Impact Template* is required for Administrative Change and Delta Change submissions for P2PE Application listings. Always refer to the applicable *P2PE Program Guide* for information on any P2PE listing changes.

The P2PE Application Vendor and/or P2PE Assessor Company must complete each section of this document and all other required documents based on the type of change (see Table 5.2.b – Changes to P2PE Listings for Applications). The P2PE Assessor Company is required to submit this *P2PE Change Impact* along with supporting documentation to PCI SSC for review.

Part 1. P2PE Application Details, Contact Information, and Change type

P2PE Application Details			
P2PE Application Name		Validated Listing Reference #	
P2PE Application Version #:		Revised P2PE Application Version *(if applicable)*	
Type of Change *(Please check)*	☐ Administrative *(Complete Part 2)*	☐ Delta *(Complete Part 3)*	
Submission Date			

P2PE Application Vendor Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	
PA-QSA (P2PE) Contact Information			
Contact Name		Title/Role	
Contact E-mail		Contact Phone	

Part 2. Details for Administrative Change (if indicated at Part 1)

Administrative Change Revision			
Current Company Name		Revised Company Name *(if applicable)*	
Current P2PE Application Name		Revised P2PE Application Name *(if applicable)*	
Current P2PE Application Version		Revised P2PE Application Version *(if applicable)*	
Description of how this change is reflected in the Vendor's versioning methodology, including how this version number indicates the type of change			
Additional details, as applicable:			

Part 3. Details for Delta Change (if indicated at Part 1)

For **each** change eligible for Delta Assessment, provide the following information. Any that impact P2PE Requirements must be reflected in the red-lined P-ROV submitted. Use additional pages and/or add rows if needed.

Delta Change – Change Summary				
Add/Remove POI Device Type *(Complete Part 3a)*		☐ Add	☐ Remove	☐ Not Applicable
Additional details, as applicable:				
Change Number	Detailed description of the change	Description of why the change is necessary	Description of how P2PE functionality is impacted	Description of how P2PE Domain 2 Requirements/sub-Requirements are impacted

Part 3a. Add/Remove POI Device Type (if indicated at Part 3)

POI Device Type		
Adding for inclusion in listing or removal from listing?	☐ Addition/Inclusion in listing *(Red-lined P-ROV review required, see details below)*	☐ Removal from listing *(No Red-lined P-ROV review required)*
POI Device type name/identifier		
POI Device manufacturer, model, and number		
PTS approval number for POI Device		
POI Device Hardware version #		
POI Device Firmware version #		

Perform a red-lined P-ROV review for the added Device using the table below as a minimum set of testing procedures.

P2PE Requirements (including all testing procedures)
☐ All of 1A-1.1
☐ 1B -1.1
☐ 1B-2.2
☐ 1B-2.3
☐ 1C-2

Appendix H: P2PE Application Software Versioning Methodology

P2PE Application Vendors are required to document and follow a software versioning methodology as part of their system development lifecycle. Additionally, P2PE Application Vendors must communicate the versioning methodology to their customers and integrators/resellers in the *P2PE Application Implementation Guide*. Customers and integrators/resellers require this information to understand which version of the application they are using and the types of changes that have been made to each version of the application. P2PE Assessor Companies are required to verify the P2PE Application Vendor is adhering to the documented versioning methodology and the requirements of the *P2PE Program Guide* as part of the P2PE Assessment. Note that if a separate version-numbering scheme is maintained internally by the P2PE Application Vendor, a method to accurately map the internal version numbers to the publically listed version number(s) must be documented and maintained by the P2PE Application Vendor.

H.1 Version Number Format

The format of the application version number is set by the P2PE Application Vendor and may be comprised of several elements. The versioning methodology and the *P2PE Application Implementation Guide* must fully describe the format of the application version number including the following:

- The format of the version scheme, including:
  - Number of elements
  - Numbers of digits used for each element
  - Format of separators used between elements
  - Character set used for each element (consisting of alphabetic, numeric, and/or alphanumeric characters)
- The hierarchy of the elements
  - Definition of what each element represents in the version scheme
  - Type of change: major, minor, maintenance release, wildcard, etc.
- The definition of elements that indicate any use of wildcards
- The specific details of how wildcards are used in the versioning methodology

H.2 Version Number Usage

All changes to the P2PE Application must result in a new application version number. However, whether this affects the version number listed on the Website depends on the nature of the change and the P2PE Application Vendor's published versioning methodology (see Section H.3, "Wildcards," below). All changes that impact security functionality and/or any P2PE Requirements must result in a change to the version number listed on the Website; wildcards are not permitted for changes impacting security functionality and/or any P2PE Requirements.

The P2PE Application Vendor must document how elements of the application version number are used to identify:

- Types of changes made to the application—e.g., major release, minor release, maintenance release, wildcard, etc.
- Changes that have no impact on the functionality of the application or its dependencies

- Changes that have impact on the application functionality but no impact on security or P2PE Requirements
- Changes that impact any security functionality or P2PE Requirement

Elements of the version number used for non-security-impacting changes must never be used for security-impacting changes.

If the P2PE Application Vendor uses a versioning scheme that involves mapping of internal version numbers to external, published version numbers, all security-impacting changes must result in an update to the external, published version number.

Any version number that is accessible to customers and integrator/resellers must be consistent with the versioning methodology described in the *P2PE Application Implementation Guide*.

P2PE Application Vendors must ensure traceability between application changes and version numbers such that a customer or integrator/reseller may determine which changes are included in the specific version of the application they are running.

H.3 Wildcards

A "wildcard" element is a variable character that may be substituted for a defined subset of possible characters in an application versioning scheme. In the context of P2PE Applications, wildcards can optionally be used to represent non-security-impacting changes between each version represented by the wildcard element. A wildcard is the only variable element of the P2PE Application Vendor's version scheme. Use of a wildcard element in the versioning scheme is optional and is not required in order for the P2PE Application to be P2PE validated. The use of wildcard elements is permitted subject to the following:

a. Wildcard elements may only be used for No Impact changes, which have no impact on security and/or any P2PE requirements.

b. The use of wildcard elements is limited to the rightmost (least significant) portion of the version number. For example, *1.1.x* represents acceptable usage. A version methodology that includes a wildcard element followed by a non-wildcard element is not permitted. For example, *1.x.1* and *1.1.y.1* represent usage that is not permitted.

c. All security-impacting changes must result in a change to the non-wildcard portion of the application version number and will therefore result in an update to the version number listed on the Website.

d. Wildcard elements must not precede version elements that could represent security-impacting changes; version elements reflecting a security-impacting change must appear "to the left of" the first wildcard element.

e. All wildcard usage must be pre-defined and documented in the P2PE Application Vendor's versioning methodology and the *P2PE Application Implementation Guide*.

f. All wildcard usage must be consistent with that validated by the P2PE Assessor Company as part of the P2PE Assessment of the P2PE Application.