Payment Card Industry (PCI)

Point-to-Point Encryption (P2PE)®

Program Guide

Version 3.0

December 2019

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
December 2019	3.0	Align to v3.0 of the P2PE Standard

Contents

1 Introduction

This document provides information on the PCI SSC Point-to-Point Encryption (P2PE) Standard program ("P2PE Program" or "Program") and is intended for P2PE Assessor Companies and vendors of P2PE Products (P2PE Solutions, P2PE Components, and P2PE Applications). Information regarding the qualification of P2PE Assessor Companies and their employees can be found in the *PCI P2PE® Qualification Requirements* on the Website. Capitalized terms used but not otherwise defined herein have the meanings set forth in Section 1.4 below or in the P2PE Glossary, as applicable.

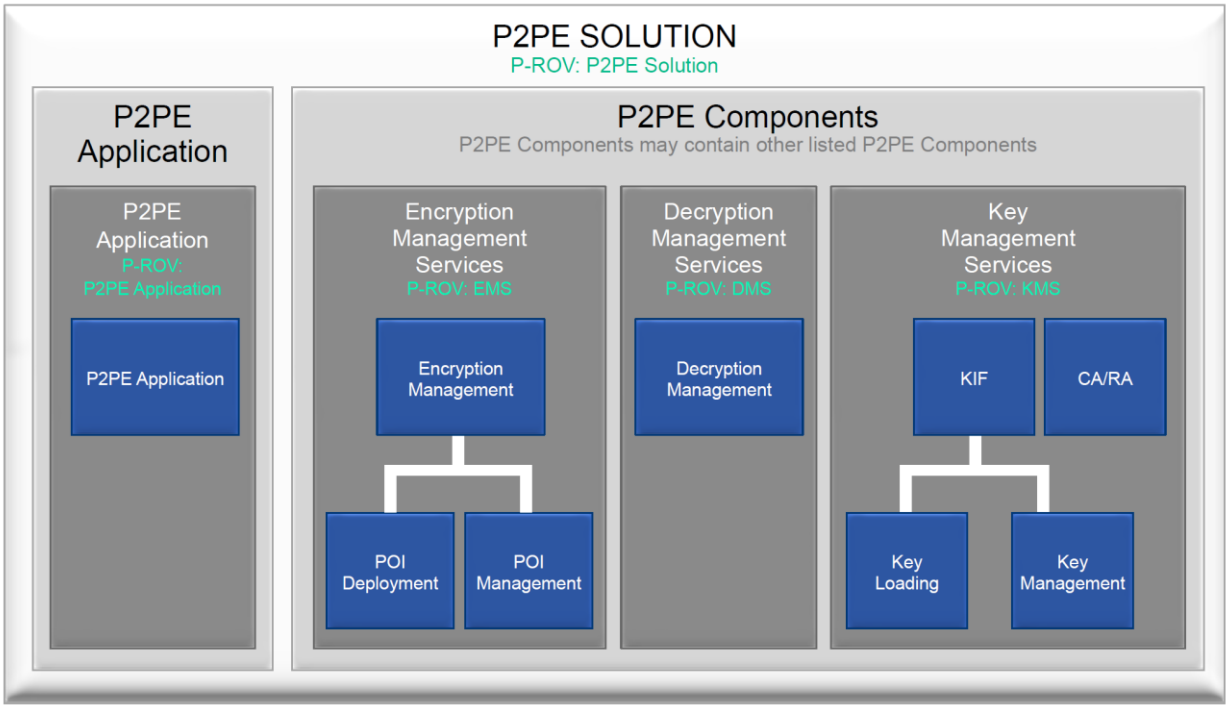
1.1 P2PE Program Overview

A P2PE Vendor may choose to have its P2PE Products validated for compliance with the P2PE Standard in order to have those P2PE Products included in the applicable list of validated P2PE Solutions, P2PE Applications, or P2PE Components on the Website.

- A P2PE Solution can be made up of Validated P2PE Applications and Validated P2PE Components (see Figure 1.1) or can be validated as a standalone solution.
- P2PE Applications and P2PE Components (all the boxes in blue in Figure 1.1) can be validated and Listed on the Website on a standalone basis and made available for Validated P2PE Solutions. See Section 2.1.3, "P2PE Component Providers" for details on P2PE Components.
- The P2PE requirements and test procedures for validating P2PE Products can be found in the corresponding P-ROV indicated by green text in Figure 1.1. P-ROVs can be found on the Website.
- For each P2PE Product to be Listed on the Website, Vendors must also submit P2PE Attestations of Validation (P-AOVs), Acceptance fees, Vendor Release Agreements (VRAs), and other supporting documents such as P2PE Application Implementation Guides and Instruction Manuals, as applicable.
- Once Listed, P2PE Products must be revalidated on an annual basis. See Section 5.1, "Annual Revalidation of P2PE Products," for further details.
- A complete P2PE Assessment of each Listed P2PE Solution (and its components), P2PE Component, and P2PE Application in accordance with the P2PE Standard (a "Full Assessment") is required on all P2PE Products every three years based on its Acceptance date.
- Any changes made to a Listed P2PE Product must be assessed as to the impact of the change on the ability of that P2PE Product to continue to satisfy applicable P2PE Requirements. See Section 5.2, "Changes to P2PE Products," for further details.
- For a mapping of the P2PE Requirements to all P2PE Products, refer to the matrix in Appendix I, "P2PE Applicability of Requirements."

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 Products.*

Figure 1.1 P2PE Program Overview



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 Security Requirements and Testing Procedures ("P2PE Standard")	The P2PE Standard contains the requisite security requirements and associated test procedures for the assessment of P2PE Solutions, Components, and Applications.
PCI P2PE Report on Validation Reporting Template ("P-ROV Reporting Template")	The P-ROV Reporting Templates are mandatory for completing a P2PE Assessment and include details on how to document the findings of a P2PE Assessment. See Table 6.1 below for specific P-ROV types.
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.

Document name	Description
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 supporting documents are used with the aforementioned documents:

- *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures* (PCI 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*

1.3 Updates to Documents and Security Requirements

It is necessary to regularly review, update, and improve the security requirements and testing procedures used to evaluate P2PE Products. 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 or testing procedures 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, validated P2PE Application Vendors, and P2PE Assessor Companies to help minimize the impact of any changes.

1.4 Terminology

Throughout this document the following terms have the meanings set forth in this Section 1.4 or in the *PCI P2PE Glossary of Terms, Abbreviations, and Acronyms* (available on the Website), as applicable:

Term	Meaning
Accepted, 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.
Decryption Management Component	A decryption environment that can support a P2PE Solution and is managed by a Decryption Management Component Provider.
Decryption Management Services	The P2PE-related services provided by a Decryption Management Component Provider as more fully described in Section 2.1.3.2.
Delta Assessment	Partial P2PE Assessment performed against applicable P2PE Requirements when changes to a Listed P2PE Solution, P2PE Application, or P2PE Component are eligible for review under the "Delta Assessment" change-review process described herein.
Encryption Management Component	The POI devices and any resident P2PE applications and/or P2PE non-payment software that can support a P2PE Solution and is deployed and managed by an Encryption Management Component Provider.
Encryption Management Services	The P2PE-related services provided by an Encryption Management Component Provider as more fully described in Section 2.1.3.1.
Key Injection Facility (KIF) Component	Key-injection facility (KIF) services managed by a KIF.
Key Loading Component	A Key Loading P2PE Component.

Term	Meaning
Key Management Component	A Key management P2PE Component.
Key Management Services	The P2PE-related services provided by a KIF as more fully described in Section 2.1.3.3.
List of Validated P2PE Applications	The Council's authoritative List of Validated P2PE Applications appearing on the Website.
List of Validated P2PE Components	The Council's authoritative List of Validated P2PE Components appearing on the Website.
List of Validated P2PE Solutions	The Council's authoritative List of Validated P2PE Solutions appearing on the Website.
Listing	Refers to the listing and related information regarding a P2PE Product on the applicable list of Validated P2PE Products on the Website.
P2PE Application Assessment	Assessment of a P2PE Application against applicable P2PE Requirements in order to validate compliance with the P2PE Standard as part of the P2PE Program.
P2PE Application Vendor	A vendor that develops and then sells, distributes, or licenses a P2PE Application for use in a P2PE Solution. A P2PE Solution Provider may also be a P2PE Application Vendor.
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 Attestation of Validation (P-AOV)	A P2PE Program *"Attestation of Validation"* declaring the validation status of a P2PE Solution, P2PE Component, or P2PE Application against the P2PE Standard.
P2PE Component	A P2PE service that is eligible for validation as a "P2PE component" (as defined in the P2PE Glossary) as part of the P2PE Program.
P2PE Component Assessment	Assessment of a P2PE Component against applicable P2PE Requirements in order to validate compliance with the P2PE Standard as part of the P2PE Program.
P2PE Expired Listing (Expired Listing)	The list of P2PE Products on the Website that have an expired status for a period of at least 90 days.
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.

Term	Meaning
P2PE Instruction Manual (PIM)	An instruction manual prepared by a P2PE Solution Provider using the template provided by PCI SSC 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 Product	A P2PE Application, P2PE Component, or P2PE Solution.
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 Report on Validation (P-ROV)	A "P2PE Report on Validation" completed by a P2PE Assessor Company and (except with respect to Merchant-Managed P2PE 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, respectively, on the Website, a corresponding P-ROV must be submitted directly to PCI SSC for review and Acceptance.
P2PE Solution Assessment	Assessment of a P2PE Solution against applicable P2PE Requirements in order to validate compliance with the P2PE Standard as part of the P2PE Program.
P2PE Solution Provider	An entity that designs, implements, and manages a P2PE Solution for one or more merchants, and is ultimately responsible for the design, maintenance, and delivery of that P2PE Solution.
P2PE Standard	The then-current version of (or successor document(s) to) the *Payment Card Industry (PCI) Point-to-Point Encryption Security 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, P2PE Component Provider, or P2PE Application Vendor.

Term	Meaning
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 Vendors in order to validate that such P2PE Vendors or their P2PE Products adhere to all aspects of the P2PE Standard, including but not limited to, validation that P2PE Applications, when incorporated into or used as part of a P2PE Solution, adhere to all applicable P2PE requirements; and (b) Remains in Good Standing (defined in Section 1.3, "Qualification Process Overview," of the *P2PE Qualification Requirements*) or in remediation as a PA-QSA (P2PE) Company.
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.
POI Deployment Component	The POI devices and any resident P2PE applications and/or P2PE non-payment software that can support a P2PE Solution and is prepared and deployed by a POI Deployment Component Provider.
POI Management Component	The POI devices and any resident P2PE applications and/or P2PE non-payment software that can support a P2PE solution and are managed by a POI Management Component Provider once deployed.
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, "Qualification Process Overview," 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.

Term	Meaning
Third-Party Service Provider	An entity that provides a service or function on behalf of a P2PE Solution Provider or P2PE Component Provider, which is incorporated into and/or referenced by the applicable P2PE Solution or P2PE Component, 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 Listed on the List of Validated P2PE Components. A Third-Party Service Provider that is not also a Listed P2PE Component Provider for those services must have its services reviewed during the course of each of its P2PE Solution Provider or P2PE Component Provider customers' P2PE Assessments.
Validated P2PE Application	A P2PE Application that has been assessed and validated by a PA-QSA (P2PE) Company to have met all applicable P2PE 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 or PA-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 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 vendor release agreement that PCI SSC: (a) Requires to be executed by P2PE Vendors in connection with the P2PE Program, and (b) Is available on the Website.
Website	The then-current PCI SSC Website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org.
Wildcard	A character that may be substituted for a defined subset of possible characters in an application version scheme. Wildcards in the context of PCI P2PE are further described in Section 5.2.3, "Wildcards for P2PE Applications."

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 a P2PE Assessor Company for validation, and
- Authorize the 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 manage P2PE Solutions for their customers and/or manage corresponding responsibilities.

A P-ROV using the required P-ROV template specifically for P2PE Solutions (a "Solution P-ROV") (see Table 6.1 below) must be submitted to PCI SSC for each P2PE Solution to be validated (except Merchant-Managed P2PE Solutions).

2.1.2 P2PE Application (Software) Vendors

To comply with the P2PE Standard, 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 against the P2PE Standard for secure operation within the applicable POI devices, and
- Provide corresponding Implementation Guides that describe the secure installation and administration of such applications on the corresponding POI devices.

A P2PE Application may be assessed as part of an overall P2PE Solution or may optionally be validated and Accepted as a standalone, Validated P2PE Application, and Listed on the List of Validated P2PE Applications. Assessment of P2PE Applications for P2PE Program purposes must be performed 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 assessed for P2PE Program purposes as part of each P2PE Solution in which is it used.

A P2PE Application P-ROV (see Table 6.1 below) must be submitted to PCI SSC for each P2PE Application assessed as part of the Program.

2.1.3 P2PE Component Providers

P2PE Component Providers are entities that provide one or more services that:

(a) Require P2PE Assessment for Program purposes, and

(b) Are performed on behalf of a P2PE Solution Provider or Component Provider for use in P2PE Solutions. These services (and their respective P2PE Component Providers) include:

- Encryption Management Services (EMS)
  - Encryption Management Component Provider (EMCP)
  - POI Deployment Component Provider (PDCP)
  - POI Management Component Provider (PMCP)
- Decryption Management Services (DMS)
  - Decryption Management Component Provider (DMCP)
- Key Management Services (KMS)
  - Key Injection Facility (KIF)
  - Key Management Component Provider (KMCP)
  - Key Loading Component Provider (KLCP)
  - Certification Authority/Registration Authority (CA/RA)

Only P2PE Components (i.e., component services) that have been validated by a P2PE Assessor and Accepted on an "Individual basis" by PCI SSC are separately Listed on the Website.

"Individual basis" here refers to the requirements 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.

Each P2PE Component requires its own PCI SSC submission. A separate P-ROV is required for each Listed P2PE Component.

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

P2PE Components may, in turn, use Validated P2PE Components or component services provided by Third-Party Service Providers.

All QSA (P2PE) Assessors are qualified to perform P2PE Assessments of P2PE Components for potential listing on the List of Validated P2PE Components.

2.1.3.1 Encryption Management Services (EMS)

"Encryption Management Services" relates to the distribution, management, and use of POI devices in a P2PE Solution or Component.

Encryption Management Component Provider is an entity that deploys and manages POI devices and any resident P2PE applications and/or P2PE non-payment software that can support a P2PE solution.

- **POI Deployment Component Provider** is an entity that prepares and deploys POI devices and any resident P2PE applications and/or P2PE non-payment software that can support a P2PE solution.
- **POI Management Component Provider** is an entity that maintains the POI devices and any resident P2PE applications and/or P2PE non-payment software, once deployed. that can support a P2PE solution.

The EMS P-ROV (see Table 6.1, "P-ROVs to be used for P2PE v3.0 Assessments") must be submitted in order to validate P2PE Components of the types provided by each of the above providers.

2.1.3.2 Decryption Management Services (DMS)

"Decryption Management Services" relates to the management of a decryption environment, including applicable devices (for example, HSMs) used to support a P2PE Solution.

- Decryption Management Component Provider is an entity that manages the decryption environment that can support a P2PE solution.

The DMS P-ROV must be submitted in order to validate P2PE Components of the type provided by the Decryption-Management Component Provider.

2.1.3.3 Key Management Services (KMS)

"Key Management Services" relates to the generation, conveyance, management, and loading of cryptographic keys including the management of associated devices.

- **Key Injection Facility** is an entity that performs cryptographic key services for POI devices and HSMs (including, but not limited to, key generation, conveyance, and/or key loading).
- **Key Loading Component Provider** is an entity that manages the cryptographic key loading for POI devices and HSMs that can support a P2PE solution.
- **Key Management Component Provider** is an entity that manages cryptographic key generation and key conveyance for POI devices and HSMs that can support a P2PE Solution.
- **Certification/Registration Authorities** (CA/RA) is an entity that signs public keys such as X.509 or other non-X.509 certificates 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.

The KMS P-ROV (see Table 6.1 below) must be submitted in order to validate P2PE Components of the type provided by this provider type.

Listings will indicate whether the P2PE Component Provider offers local or remote key-injection services and will show whether Certification Authority/Registration Authority (CA/RA) services are provided.

The KMS P-ROV must be submitted in order to validate P2PE Components of the types provided by the above provider types.

2.1.4 Use of Third-Party Service Providers

A given P2PE Solution or P2PE Component:

1) May be entirely performed and managed by a single P2PE Solution Provider or by a merchant acting as its own P2PE Solution Provider (in the case of a MMS); or
2) Certain services that are part of the applicable P2PE Solution may be outsourced to Third-Party Service Providers who perform these functions on behalf of the P2PE Solution Provider or P2PE Component Provider.

All P2PE services and functions performed by Third-Party Service Providers on behalf of a P2PE Solution Provider or P2PE Component Provider must be validated per applicable P2PE Solution or P2PE Component requirements, and Third-Party Service Providers have the option of having their P2PE Component services validated under the Program.

There are two validation options for third-party entities performing P2PE functions on behalf of P2PE Solution Providers or P2PE Component Providers:

1) Undergo a P2PE Assessment of the applicable P2PE Component services and functions against relevant P2PE Requirements, and have their P2PE Assessor submit the applicable P2PE Report of Validation (P-ROV) to PCI SSC for review and Acceptance. Upon Acceptance, the corresponding P2PE Component is Listed on PCI SSC's List of Validated P2PE Components. Or:
2) Have their P2PE Component functions or services reviewed during and as part of each of their customers' corresponding P2PE Assessments.

Accordingly, a P2PE Solution or P2PE Component can be reviewed via one of the following scenarios:

1) A P2PE Solution Provider or P2PE Component Provider (or a merchant as a P2PE Solution Provider in the case of a Merchant-Managed Solution (MMS)) can outsource functions and have them assessed as part of the overall P2PE Assessment of that P2PE Solution or P2PE Component.
2) A P2PE Solution Provider or P2PE Component Provider (or a merchant as a P2PE Solution Provider in the case of a MMS) can outsource certain P2PE Component service functions to Listed P2PE Component Providers and report use of those PCI-Listed P2PE Component(s) in its P2PE Solution P-ROV.

P2PE Solution Providers (or merchants as P2PE Solution Providers in the case of a MMS) must manage the overall P2PE Solution and any third-party services (and corresponding Third-Party Service Providers) used to perform P2PE Component services or functions on their behalf, whether those Third-Party Service Providers are separately Listed by PCI SSC as P2PE Component Providers or are assessed as part of the P2PE Assessment of the corresponding P2PE Solution or P2PE Component.

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. In relation to the P2PE Standard, PCI SSC:

- 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 against the P2PE Standard;
- Maintains and updates the P2PE Standard and related documentation; 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 Annual Revalidations are correct as to form;
  - QSA (P2PE) and PA-QSA (P2PE) Companies properly determine whether candidate P2PE Products are eligible 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 Products 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 P2PE Product complies with the P2PE Standard, that the P2PE Assessor Company has submitted the corresponding P-ROV(s) 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.

P2PE Assessor Companies are responsible for:

- Performing P2PE 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.*
- Determining the scope of their P2PE Assessments and applicability of the P2PE Standard to each of those P2PE Assessments.
- Assessing the compliance of P2PE Solutions and P2PE Components (and P2PE Application for PA-QSA (P2PE) Assessor Companies) against the P2PE Standard.
- Documenting each P2PE Assessment in a P-ROV using the applicable P2PE P-ROV Reporting Templates.
- Submitting the applicable P-ROV(s) 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 PCI SSC statements and guidance, P2PE Technical and General FAQs, industry trends, and best practices.

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 on compliance.

As indicated above, PCI SSC does not approve P-ROVs from a technical compliance perspective but performs quality assurance to confirm that P-ROVs adequately document the demonstration of compliance.

2.5 Customers

Customers using a Validated P2PE Solution to facilitate their PCI DSS compliance are responsible for:

- Determining which solutions and devices to implement.
- Adhering to the *P2PE Instruction Manual* (PIM), provided to the merchant by the P2PE Solution Provider.

2.6 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 and HSMs against PCI SSC's PTS Standards ("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 that occurs as part of a P2PE Assessment; the P2PE Assessment validates whether or not a given P2PE Product (which may include multiple POI/HSM devices) is in compliance with the P2PE Standard.*

2.7 Payment Device (Hardware) Vendors

A POI device vendor submits a POI device for evaluation to a PCI-recognized Laboratory. Only eligible POI devices listed on the List of Approved PTS Devices may be used as part of a P2PE Solution.

3 Overview of Validation Processes

3.1 Validation Processes for P2PE Products 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.

Note: *The results of Merchant-Managed P2PE Solution assessments are not submitted to PCI SSC for validation, and Merchant-Managed P2PE Solutions are not Listed.*

1) The P2PE Vendor selects a P2PE Assessor Company from PCI SSC'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 its executed VRA and access to the applicable P2PE Solution, P2PE Component(s), and/or P2PE Application(s) 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.
3) Refer to Section 2.1.4, "Use of Third-Party Service Providers," in this document to understand options for validating P2PE Component functions and services provided by Third-Party Service Providers. The P2PE Assessor Company then assesses the P2PE Solution, P2PE Component(s), and/or P2PE Application(s), including its security functions and features, using the appropriate P-ROV(s), to determine whether it complies with the P2PE Standard.
4) If the P2PE Assessor Company determines that the P2PE Solution, P2PE Component(s), and/or P2PE Application is in compliance with the P2PE Standard, the P2PE Assessor Company submits the corresponding P-ROV(s) 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. See Appendix A, "P2PE Products and Acceptance," for more details on Acceptance.
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 submission to confirm that it meets the P2PE Program requirements and if confirmed, PCI SSC notifies the P2PE Assessor Company and P2PE Vendor that the P2PE Solution, P2PE Component(s), and/or P2PE Application(s) have completed the process.
6) Once the above process is complete for the submitted P2PE Solution, P2PE Component(s), and/or P2PE Application(s), PCI SSC signs the corresponding P-AOV and adds the P2PE Solution, P2PE Component(s), and/or P2PE Application(s) to the corresponding list of Validated P2PE Products on the Website.

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

Process	Illustration
P2PE Assessment for P2PE Products Intended for v3 PCI SSC Listing	Figure 1
P2PE Product Submission and PCI SSC Review	Figure 2

Figure 1: P2PE Assessment for Products Intended for v3 PCI SSC Listing

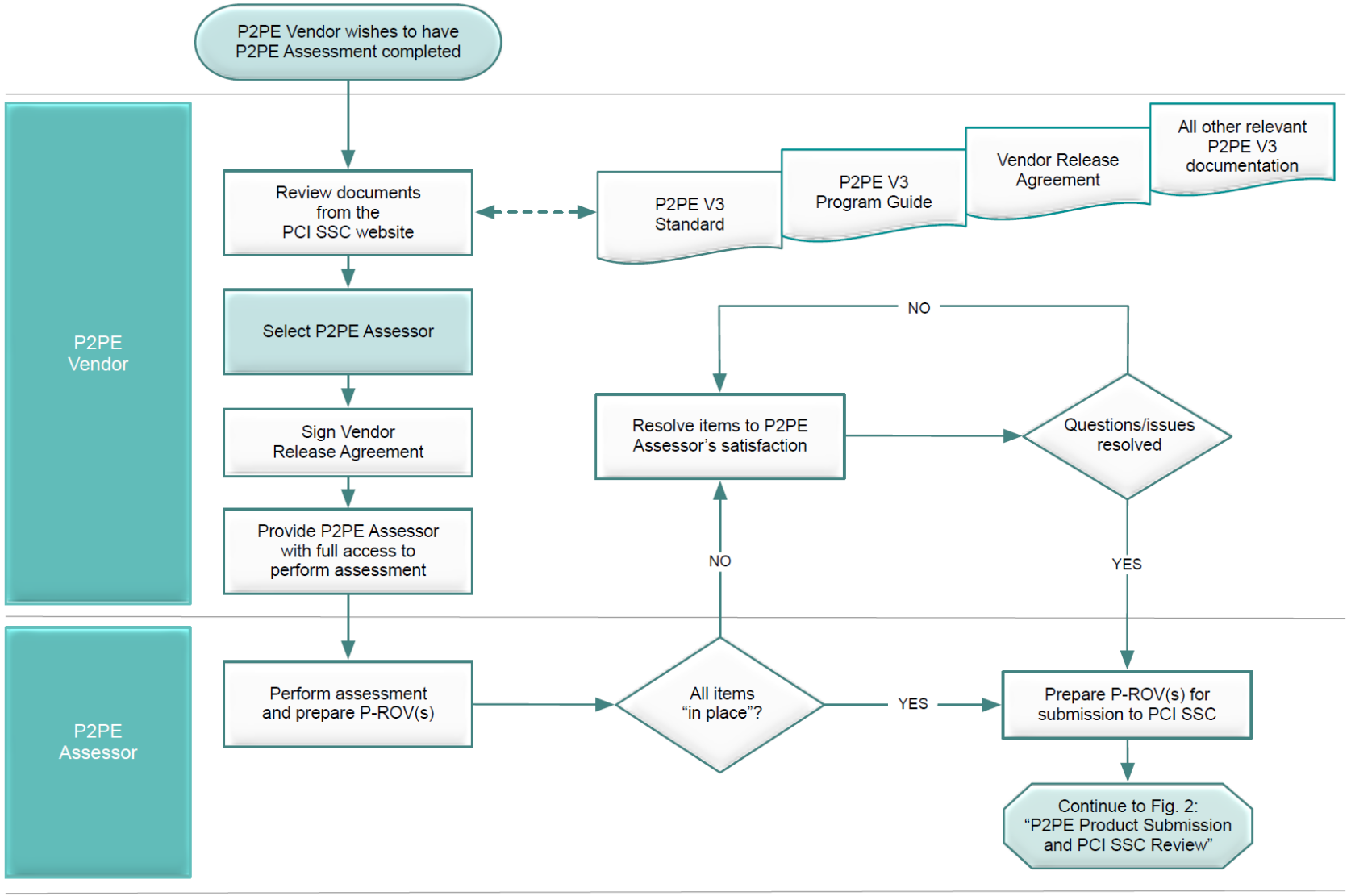
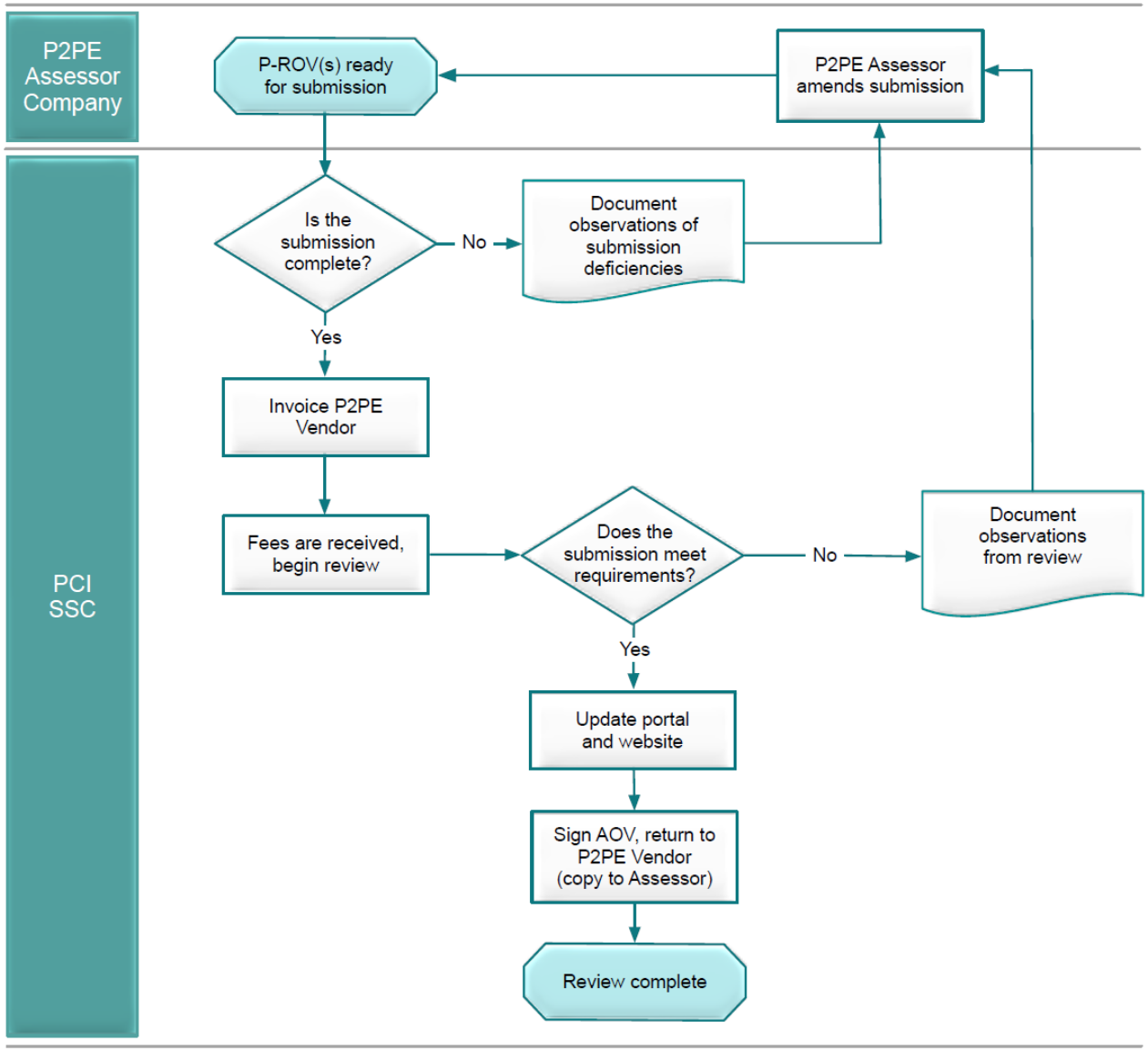


Figure 2: P2PE Product Submission and PCI SSC Review



3.2 Overview of Validation Processes for Merchant-Managed P2PE Solutions

The P2PE Assessment process for P2PE Solutions that are managed by the merchant that uses that P2PE Solution (each a "Merchant-Managed P2PE Solution" or "MMS") is initiated by the applicable 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 PCI SSC 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.

Note: *Refer to Section 2.1.4, "Use of Third-Party Service Providers" in this document to understand options for validating Third-Party Service Providers.*

2) The Merchant provides 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 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 Merchant-Managed P2PE Solution P-ROV attesting to compliance and setting forth the results, opinions and conclusions of the P2PE Assessor Company on all test procedures.

Note: *Merchant-Managed P2PE Solutions are not eligible for listing on the Website, and the corresponding P-ROV is not submitted to PCI SSC. A Merchant-Managed P2PE Solution may utilize Third-Party Service Providers, Validated P2PE Applications, and/or Validated P2PE Components.*

4 Program Guidance

4.1 Requirements and Eligibility

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

Table 4.1

<table>
<tr><th>Possible Element</th><th>Program Guidance</th></tr>
<tr><td>SCDs</td><td>Validated P2PE Solutions and P2PE Components require the use of various types of Secure Cryptographic Devices (SCDs). To assist in evaluating these device types for use in a P2PE Solution, note the following:
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.
Obtaining and maintaining PTS or FIPS 140 device approval is the responsibility of the secure cryptographic device vendor. P2PE Assessors will request evidence of device approvals being in place and current as part of performing a P2PE Assessment.
An <u>existing</u> P2PE Program approval of a Listed P2PE Solution or P2PE Component may be reassessed up to but not exceeding three years past the expiry date of any PCI-listed HSMs already included in the corresponding P2PE Solution or P2PE Component approval. This will be checked as part of the reassessment and submittal process to PCI SSC. As the reassessment (provided it results in an updated P2PE listing) is valid for three years, this will allow vendors to continue to use the expired HSMs for up to a total of six years after any associated PTS HSM listings have expired, depending on their reassessment date.
The following table provides the current PTS HSM expiry dates and the corresponding reassessment window for P2PE Solutions and applicable P2PE Components using these devices:<table><tr><th>PCI PTS HSM version</th><th>PCI PTS HSM Approval Expiry Date</th><th>P2PE Reassessment End-date for Expired HSM Devices*</th><th>Expired PCI HSMs End of Life**</th></tr><tr><td>1.x</td><td>EXPIRED April 2019</td><td>29 April 2022</td><td>29 April 2025</td></tr><tr><td>2.x</td><td>30 April 2022</td><td>29 April 2025</td><td>29 April 2028</td></tr><tr><td>3.x</td><td>30 April 2026</td><td>29 April 2029</td><td>29 April 2032</td></tr></table></td></tr>
</table>

<table>
<tr><th>Possible Element</th><th>Program Guidance</th></tr>
<tr><td></td><td>
* Existing Listed P2PE Solutions and applicable P2PE Components are prohibited from reassessment with any expired HSMs that exceed the reassessment date shown relative to the associated PCI PTS HSM version. For example, Any PCI-Listed P2PE Solution or P2PE Component using a v1.x PCI HSM will be prohibited from reassessment after April 29, 2022.
** P2PE Solutions and applicable P2PE Components must have replaced any expired HSMs with current (non-expired) HSMs by this date.
For additional detail, refer to Appendix J, “PCI-Listed PTS HSM Expiry Flowchart.”
</td></tr>
<tr><td>SCDs
(continued)</td><td>

Existing PCI P2PE approvals of Validated P2PE Products with expired PTS POI devices may be revalidated and reassessed for up to, but not exceeding, five years past the PTS POI device expiry dates (as appearing on the PCI SSC List of Approved PTS Devices) used in the corresponding P2PE Product. A POI device may not be used in a Listed P2PE Solution more than five years past the corresponding PTS POI device expiry date. A Validated P2PE Solution will be delisted if all of its associated POI device types have exceeded the five-year window (as shown in the table below).
The following table provides the current POI device expiry dates and the corresponding revalidation/reassessment window for P2PE Solutions using these devices.

<table>
<tr><th>PCI PTS POI version</th><th>PTS POI Expiry Date</th><th>P2PE Revalidation/Reassessment End-date for Expired POI Devices*</th></tr>
<tr><td>1.x</td><td>EXPIRED 2014</td><td>N/A – v1.x devices are not P2PE eligible</td></tr>
<tr><td>2.x</td><td>EXPIRED April 2017</td><td>29 April 2022</td></tr>
<tr><td>3.x</td><td>30 April 2020</td><td>29 April 2025</td></tr>
<tr><td>4.x</td><td>30 April 2023</td><td>29 April 2028</td></tr>
<tr><td>5.x</td><td>30 April 2026</td><td>29 April 2031</td></tr>
</table>
* There may be regional variations—check with the respective payment brands to determine any variances in the dates shown above.
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.
</td></tr>
</table>

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 applicable P2PE Application 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 or P2PE Component 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, additional testing/assessment against the P2PE Application P-ROV is not required as part of the P2PE Assessment of the applicable P2PE Solution. ▪ If a P2PE Application is not already on the List of Validated P2PE Applications, both the Solution P-ROV (including Component P-ROVs, if applicable) and the P2PE Application P-ROV must be submitted before the P2PE Solution can be assessed. This applies for **each** P2PE Solution in which the P2PE 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 Requirements by a P2PE Assessor Company. ▪ Not eligible for PCI-listing by PCI SSC.

Possible Element	Program Guidance
P2PE Components	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 and P2PE Components without the need for a Full Assessment of those services each time they are used with a different P2PE Solution or P2PE Component. 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 P2PE Components that the P2PE Solution or P2PE Component uses will need to be identified in the Solution P-ROV and no assessment of that currently listed P2PE Component is needed as part of the P2PE Solution or P2PE Component assessment. ▪ 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 applicable Component P-ROV must be submitted and Accepted before the P2PE Solution or P2PE Component 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 P2PE Solution or P2PE Component within which it is assessed.
Third-Party Service Provider	Refer to the Section 2.1.4, "Use of Third-Party Service Providers," in this document to understand options for validating P2PE Component services or functions provided by Third-Party Service Providers.

4.2 Prior to the Review

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

Prior to commencing a P2PE Assessment 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 P2PE Solution's, P2PE Component's, or P2PE Application's readiness to comply with the P2PE Standard: Select the appropriate P-ROV(s) based on the type of P2PE Assessment.
- Determine whether the P2PE Application Vendor'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.

4.3 Required Documentation

The P2PE Solution Provider must deliver all completed P2PE Assessment-related materials (such as, but not limited to, P-ROVs, 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) to the P2PE Assessor Company performing the P2PE Assessment, not to PCI SSC.

4.4 P2PE Review Timeframes

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

- How close the P2PE Product is compliant with the P2PE Standard at the start of the P2PE Assessment

  Corrections to the P2PE Product to achieve compliance will delay validation.

- For P2PE Solutions and P2PE Components 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 Instruction 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
  - *Submissions that are incomplete or contain 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(s) more than once, providing comments back to the P2PE Assessor Company to address each time 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 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 it does 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 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 P-ROV Reporting Template.*
- The P2PE Assessor Company must prepare each P-ROV based on evidence obtained by following the P2PE Standard.
- Prior to submitting to PCI SSC, the P2PE Assessor Company must perform a review of all documents to ensure they are consistent and meet PCI SSC's requirements and quality standards.
- 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 Instruction 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 the P2PE Vendor. Before deciding on a P2PE Assessor Company, it is recommended that a prospective P2PE Vendor check the list of P2PE Qualified Assessor Companies, talk to several P2PE Assessor Companies, and follow its own vendor-selection processes.

4.6 Technical Support throughout Testing

It is recommended that the P2PE Vendor (or in the case of a Merchant-Managed P2PE Solution, the Merchant) make available a technical resource person to assist with any questions that may arise during the P2PE 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 P-ROV to be reviewed by PCI SSC, PCI SSC must have on file the P2PE Vendor's signed copy of the then-current version of the *Vendor Release Agreement* available on the Website. Generally, the P2PE Vendor provides its signed VRA to the P2PE Assessor Company along with access to the P2PE Product and other documents and materials, at the beginning of the applicable 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 to review a P-ROV, PCI SSC must receive from the P2PE Assessor Company (or already have on file) the P2PE Vendor's signed copy of then-current VRA. At the time of submission of any P-ROV to PCI SSC:

- If PCI SSC **does not** already have the P2PE Vendor's signed copy of the then-current VRA, the P2PE Assessor Company must provide the P2PE Vendor's signed copy of the then-current VRA to PCI SSC, along with the P-ROV(s) submission.
- If PCI SSC **does** already have the P2PE Vendor's signed copy of the then-current VRA, the P2PE Assessor is not required to re-submit the same VRA to PCI SSC at that time.

4.8 The Portal

For any P2PE Product to be Listed on the Website, all documents relating to the P2PE validation process for that P2PE Product are to be submitted by the applicable P2PE Assessor, on behalf of the P2PE Vendor, to PCI SSC through the PCI SSC's secure website ("Portal"). Submissions are pre-screened in the Portal by Council staff to help ensure that all required documentation has been included and the basic submission requirements have been satisfied.

The Portal is also used by PCI SSC to track all communications relating to a 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 its 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. 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 Annual Revalidation and Change

5.1 Annual Revalidation of P2PE Products

Note: *P2PE v3 Products require a Full Assessment every three years based on the date of the P2PE Product's Acceptance.*

Annually, based on the date of the applicable P2PE Product's Acceptance, the P2PE Vendor is required to submit an updated *P2PE Attestation of Validation* for that P2PE Product, covering the time since the last submission for that P2PE Product (i.e., initial P-ROV submission or annual update per this Section) was accepted and listed by PCI SSC (each an "Annual Revalidation")

PCI SSC will generally send a courtesy reminder e-mail to the P2PE Vendor's contact (as identified in the applicable P-AOV) within 90 days prior to the relevant revalidation/reassessment date, but it is the sole responsibility of the P2PE Vendor to maintain the listing regardless of any such courtesy reminder(s).

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

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

b) The P2PE Product continues to meet the requirements of the P2PE Standard;

c) POI devices or HSMs that are part of the P2PE Product continue to be acceptable for use in a P2PE Product. See Table 4.1, "Program Guidance," for SCDs regarding expired POI devices and HSMs.

d) PCI SSC has been advised of any change that necessitates a change to the listing on the Website, in accordance with the P2PE Program Guide.

Note: *Vendors are required to annually submit a P-AOV to confirm their P2PE Product continues to meet the P2PE Standard.*

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

- The corresponding Listing will be updated to show the P2PE Product's Reassessment Date 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 Listing's Reassessment Date with the new date and remove the **Orange** status.
- If the updated and complete P-AOV is not received within this 90-day period, the corresponding Listing's Reassessment Date will be updated to show the date in **Red.**
- Once in **Red**, a Full Assessment (including applicable fees) is required to return the P2PE Product's Listing to good standing.
- If a P2PE Product's Listing has been in a **Red** status for more than 90 days, the P2PE Product will be moved to the P2PE Expired Listing.

- PCI SSC will, following receipt of the updated *P2PE Attestation of Validation*: (i) review the submission for completeness; and (ii) if completeness is established, sign and return a copy of the updated *P2PE Attestation of Validation* to the P2PE Vendor."

5.2 Changes to P2PE Products

P2PE Vendors may update Listed P2PE Products for various reasons. All changes must be assessed for security impact. Delta and Administration changes do not have any impact on Annual Assessment due dates or Reassessment dates in P2PE Product Listings. Changes are categorized as follows:

Table 5.2 – Changes to P2PE Listed Products

Change Type	Description	Action by Vendor/Assessor
Delta[1]	1. Impacts the corresponding P2PE Product Listing; and 2. Is not an "Administrative" change (described below). Delta changes include changes to: ▪ Add/Remove a P2PE Component; ▪ Add/Remove a PCI-approved POI device Type; ▪ Add/Remove a PCI SSC listed or FIPS-approved HSM; ▪ Add/Remove a P2PE Application; and ▪ P2PE Application changes where fewer than half the applicable Requirements/Sub-Requirements are affected. ***Note:*** *P2PE Application changes where at least half of the applicable Requirements/ Sub-Requirements are affected require a full P2PE Assessment.* *See Section 5.2.2, "Delta Changes for P2PE Products" for details.*	▪ Complete change analysis and submit to P2PE Assessor Company for review. ▪ Submit *Change Impact Template* (See Appendices) to PCI SSC for review. ▪ Submit updated P2PE Application Implementation Guide or P2PE Instruction Manual to P2PE Assessor Company for review, if applicable. ▪ Submit red-lined P-ROV to PCI SSC for review, if applicable. ▪ Submit new VRA to P2PE Assessor Company, if applicable. ▪ Pay fee to PCI SSC.
No Impact[2]	1. Does not impact the P2PE Product's compliance with any of the P2PE Requirements; and 2. Does not impact the corresponding Listing.	▪ Not reported at the time of the change. ▪ Addressed by P2PE Vendor during the Annual Revalidation Process. ▪ Submit P-AOV to PCI SSC in accordance with Section 5.1, "Annual Revalidation."

[1] Combining former Designated and Delta change categories

[2] Combining former Interim and No Impact change categories

Change Type	Description	Action by Vendor/Assessor
Administrative	1. Does not impact the P2PE Product's compliance with any of the P2PE Requirements; and 2. Only impacts administrative information in the corresponding Listing. Examples: ▪ Corporate identity changes ▪ P2PE Product name changes ▪ Listing detail changes such as "Regions Served" (P2PE Solutions only) *See Section 5.2.1, "Administrative Changes for P2PE Listings," for details.*	▪ Complete change analysis and submit to P2PE Assessor Company for review. ▪ Complete *P2PE Change Impact Template* (See Appendices) and submit to P2PE Assessor Company for review. ▪ Submit updated P2PE Application Implementation Guide or P2PE Instruction Manual to P2PE Assessor Company for review, if applicable. ▪ Submit new VRA to P2PE Assessor Company, if applicable ▪ Pay fee to PCI SSC.

5.2.1 Administrative Changes for P2PE Listings

"Administrative Changes" are updates to the Listing information of a Listed P2PE Product where no changes to the P2PE Product itself have occurred, but the P2PE Vendor wishes to request a change to the administrative information in the corresponding P2PE Product Listing on the Website.

The P2PE Vendor prepares a change analysis (for example, using the corresponding *P2PE Change Impact Template*) and submits it to the P2PE Assessor Company for review, along with the updated *P2PE Application Implementation Guide* or *P2PE Instruction 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 change analysis to the same P2PE Assessor Company used for the last full P2PE Solution Assessment.

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 it agrees;
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 submits it through the Portal;

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 change analysis is eligible as an Administrative Change, the P2PE Assessor Company returns the 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 Delta Changes for P2PE Products

Delta Changes are changes made to a listed a Listed P2PE Products (where applicable) to:

- Add/remove a PCI-approved POI device; ***or***
- Add/remove a PCI SSC listed and/or FIPS-approved HSM; or
- Add/remove a validated P2PE Application; or
- Add/remove a validated P2PE Component; or
- Address changes to P2PE Application changes where fewer than half of the applicable Requirements/sub-Requirements are affected.

Note: *P2PE Application changes where greater than half the applicable Requirements/Sub-Requirements are affected require a Full Assessment of the application.*

Delta Changes result in an amendment to a P2PE Product as currently Listed on the Website.

The P2PE Vendor prepares a change analysis (for example, using the corresponding *P2PE Change Impact Template*) and submits it to the P2PE Assessor Company for review, along with the updated *P2PE Instruction Manual or P2PE Application Implementation Guide*, 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 change analysis to the same P2PE Assessor Company used for the last Full Assessment as they are familiar with the P2PE Product. If the P2PE Assessor Company agrees that the change as documented by the P2PE Vendor is eligible as a Delta Change:

1) The P2PE Assessor Company must notify the P2PE Vendor that it agrees;
2) If applicable, the P2PE Vendor modifies the *P2PE Instruction Manual* or *P2PE Application Implementation Guide* 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 "Delta Changes" sections of the corresponding *P2PE Change Impact Template*;
4) The P2PE Assessor Company completes the corresponding *P2PE Change Impact Template* and must produce a **red-lined** P-ROV and document the testing completed per PCI SSC requirements. For any changes to P2PE Applications where fewer than half of the security requirements have been impacted, the *Change Impact Template for P2PE Applications* must be completed.
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* or *Implementation Guide, (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 Delta Change submission for quality assurance purposes and consistency.

If the P2PE Assessor Company does not agree with the P2PE Vendor that the change as documented in the change analysis is eligible as a Delta Change, the P2PE Assessor Company returns the 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.

1) Amend the corresponding Listing of Validated P2PE Solutions. P2PE Applications or 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 Delta Change by the P2PE Assessor Company or P2PE Vendor is ineligible for treatment as a Delta 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 specified 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 v3 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.

5.3 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 perform a Full Assessment of the P2PE Product against 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. If the P2PE Product remains in a **Red** status on the listing for 90 days, the P2PE Product will be moved to the P2PE Expired Listing.

5.4 Validation Maintenance Fees

If a Listed P2PE Product 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 Product, the applicable fee will be invoiced and must be received by PCI SSC for the change 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 Annual Revalidation 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.

5.5 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. P2PE Vendors must be aware of and adhere to their obligations under the VRA in the event of a Security Issue.

5.5.1 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.

5.5.2 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 an e-mail to the PCI P2PE Program Manager at P2PE@pcisecuritystandards.org.

5.5.3 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.

5.5.4 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.

5.5.5 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 Standard makes use of different P-ROV templates for P2PE Solutions, P2PE Applications, and P2PE Component types. There is a single Solution P-ROV, in addition to separate P-ROVs based on a P2PE Component or P2PE Application function (or service offering) as it pertains to a P2PE Solution. Each of the separate P-ROVs is used in addition to the Solution P-ROV for P2PE Assessments of P2PE Solutions, as needed. They are also used for individual P2PE Assessments of P2PE Components or P2PE Applications. See Table 6.1, "P-ROVs to be used for P2PE v3.0 Assessments," below.

6.1.1 P2PE Solution Assessments

P2PE Assessment of P2PE Solutions must use the Solution P-ROV template. For every function that is not outsourced to a PCI SSC-listed P2PE Component Provider, EACH applicable P-ROV must be completed and submitted in addition to the Solution P-ROV.

6.1.2 P2PE Component Assessments

P2PE Assessments of P2PE Components must use the P-ROV template associated with the applicable service offering. See Table 6.1, "P-ROVs to be used for P2PE v3.0 Assessments," for description of appropriate P-ROV(s).

6.1.3 P2PE Application Assessments

P2PE Assessments of P2PE Applications must use the P-ROV template specified for P2PE Applications.

6.1.4 P-ROV Submission Process

When the P-ROV(s) have all items in place, and where the P2PE Vendor seeks to have the P2PE Product Listed on the Website, the P2PE Assessor Company performs a quality assurance review and then submits the P-ROV(s) and all other required materials to PCI SSC. If the P-ROV(s) do not have all items in place, the P2PE Vendor must address those items, and the P2PE Assessor must update the P-ROV(s) 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(s) and all other required materials to PCI SSC.

Once PCI SSC receives the completed P-ROV(s) 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(s) meet 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(s) 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-ROV(s) 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-ROV(s) 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.

Table 6.1: P-ROVs to be used for P2PE v3.0 Assessments

P-ROV Name	Used for the Following Assessments	Purpose
Solution	P2PE Solution	The Solution P-ROV is mandatory for all P2PE Assessments of P2PE Solutions. Additional P-ROVs (below) may be required. ***Note:*** *A separate Merchant-Managed Solution P-ROV is used as part of MMS Assessments.*
Encryption Management Services (EMS)	P2PE Solution Encryption Management POI Deployment POI Management	"Encryption Management Services" relates to the distribution, management, and use of POI devices in a P2PE Solution or Component. P2PE Assessment of P2PE Solutions that do not outsource the entirety of their Encryption Management Services to PCI SSC-listed P2PE Component Providers, either to an EMCP or to BOTH a PDCP AND a PMCP, must complete this P-ROV in addition to the Solution P-ROV. P2PE Assessments of P2PE Components provided by an EMCP, PDCP, or a PMCP must use this P-ROV.
P2PE Application	P2PE Application	Any P2PE Assessment for software on the POI devices intended for use in a P2PE Solution that has the potential to access clear-text cardholder data must complete this P-ROV.
Decryption Management Services (DMS)	P2PE Solution Decryption Management	"Decryption Management Services" relates to the management of a decryption environment, including applicable devices (for example, HSMs) used to support a P2PE Solution. P2PE Assessments of P2PE Solutions that do not outsource the entirety of their Decryption Management Services to a PCI SSC-listed DMCP must complete this P-ROV in addition to the Solution P-ROV. P2PE Assessments of P2PE Components provided by a DMCP must use this P-ROV.

P-ROV Name	Used for the Following Assessments	Purpose
Key Management Services (KMS)	P2PE Solution KIF Key Management Key Loading CA/RA	"Key Management Services" relates to the generation, conveyance, management, and loading of cryptographic keys including the management of associated devices. Solution assessments that have not satisfied the key management services requirements (Domain 5) either through the use of PCI-listed Component Providers and/or through the assessment of their Encryption Management Services and/or Decryption Management Services must complete the KMS P-ROV. For example, if the P2PE Solution offers remote key-distribution using asymmetric techniques for the distribution of keys to POI devices for use in connection with account-data encryption, or the operation of an applicable CA/RA, or any other relevant key management service that has not already been assessed as part of the inclusion of a PCI-listed Component Provider, then the Solution assessment must include the use of the KMS P-ROV. Component Provider assessments for a KIF, KMCP, KLCP, or a CA/RA must complete this P-ROV

6.2 Delivery of the P-ROV and Related Materials

For P2PE Products 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 the Portal. PCI SSC 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 the PCI SSC P2PE Program Manager. Portal credentials may be issued to any employee of a P2PE Assessor Company 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 *P2PE Qualification Requirements* 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 prior to AQM review, during which an AQM Analyst reviews 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 are questions 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 instructions for optionally appealing.

If the P2PE submission is complete and is determined to be eligible for validation under the P2PE Program, the AQM Analyst will conduct a complete review of the P-ROV submission 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 must address all inquiries and feedback in a timely manner. The AQM Analyst's role is to ensure sufficient evidence is included to provide reasonable assurance that the P2PE Assessment was performed in accordance with Program requirements and meets 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.

As QSA Company audits are described in the *QSA Qualification Requirements*, P2PE Assessor Companies are also subject to audits of their work as P2PE Assessor Companies under the *QSA Qualification Requirements* at any time. This may include but is not 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 are also 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 requirement, failure to submit required information in a timely manner, etc. P2PE Assessor Companies in Remediation are identified on the Website in **Red**, indicating their remediation status without further explanation of the designation.

If administrative or minor quality problems are detected, PCI SSC will typically recommend participation in Remediation. Remediation provides an opportunity for P2PE Assessor Companies and/or Employees to improve performance by working closely with PCI SSC staff; in the absence of participation, quality issues may persist or 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 Listed P2PE Solution, P2PE Component or P2PE Application 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 pending resolution of the appeal. 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 (Link to Company website)

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

P2PE Solution Identifier

"P2PE Solution 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 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

- **P2PE 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):

  - PCI SSC listed and/or FIPS 140-certified Devices Supported
  - P2PE Application(s) Supported
  - P2PE Components

P2PE Solution Details: Detail

- **PCI SSC Listed and FIPS 140-certified Devices Supported**

  This section identifies:

  – PCI-approved POI devices validated for use with this P2PE Solution and will include

relevant PCI PTS reference numbers and expiry dates of the PTS approval. A website link will be provided to the appropriate entry on the List of Approved PIN Transaction Security Devices

- PCI SSC listed, or FIPS 140-certified HSM reference numbers and expiry date. A website link will be provided to the appropriate entry on the *NIST Cryptographic Module Validation Program* (CMVP) list of FIPS validated HSMs.

- **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 P2PE 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 identified within the P2PE Solution's Listing or on 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 P2PE Component 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—Example, Global or US, Brazil.

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 P2PE Standard in order to maintain the Acceptance.

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

The list of recognized P2PE Component Providers for the List of Validated P2PE Components:

- Encryption-management services (EMS):
  - Encryption Management
  - POI Management
  - POI Deployment
- Decryption-management services (DMS)
  - Decryption Management
- Key Management Services (KMS):
  - Key-Injection Facility (KIF)
  - Key Management
  - Key Loading
  - Certification Authority/Registration Authority (CA/RA)

Each contains the same listing elements below:

Company (link to Company website)

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
- P2PE 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

- **P2PE 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):

  – PCI-approved POI Devices Supported
  – PCI SSC Listed and/or FIPS 140-certified HSMs 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 POI Devices Supported; others likely will not.

P2PE Component Details: Detail

- **PCI-Approved POI Devices Supported**

  This section identifies PCI-approved POI devices validated for use with this P2PE Solution and will include relevant PCI PTS reference numbers and expiry dates of the PTS approval. A website link will be provided to the appropriate entry on the List of Approved PIN Transaction Security Devices.

- **PCI SSC Listed and/or FIPS 140-certified HSMs Supported**

  This section identifies PCI SSC listed, and/or FIPS 140-certified HSMs for use with this P2PE Solution and will include reference numbers and expiry dates. A website link will be provided to the appropriate entry on the List of Approved PIN Transaction Security Devices and the NIST CMVP (Cryptographic Module Validation Program) list of FIPS validated HSMs.

- **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 on 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 of which the P2PE Component is a part.

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 a Validated P2PE Component is the date by which the P2PE Component Provider must have the P2PE Component re-evaluated against the P2PE Standard in order to maintain the Acceptance.

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

Company (link to Company website)

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
- P2PE 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 P2PE vendor,
  - May consist of a combination of alphanumeric characters; and
  - Must be consistent with the P2PE 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 P2PE 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 P2PE Application Vendor and will remain the same for the life of the listing.

  An example reference number is 2019-XXXXX.XXX.AAA, consisting of the following:

Field	Format
Year of listing	4 digits + hyphen
P2PE Application Vendor #	5 digits + period (assigned alphabetically initially, then as received)
P2PE Application Vendor App #	3 digits (assigned as received)
Minor version	3 alpha characters (assigned as received)

- **P2PE Application Details**

  Clicking on this link brings up a list of details specific to this P2PE Application consisting of the following fields (fields are explained in detail below): PCI-approved POI devices Supported

P2PE Application Details: Detail

- **PCI-Approved POI 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. 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 P2PE Standard in order to maintain Acceptance.

Note: *P2PE Applications validated to P2PE Standard v2 and v3 are valid for a period of three years from their Acceptance Date.*

Appendix E: Change Impact Template for P2PE Solutions

This *P2PE Change Impact Template* is required for Administrative Change and Delta 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 *(Select one)*	☐ 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 Delta Change (if indicated at Part 1)

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

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

Add additional rows or pages as necessary if multiple POI devices are being added/removed in a single change submittal.

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 POI Device type(s) using the table below as a minimum set of testing procedures.

P2PE Requirements (including all testing procedures)
☐ All of 1A-1.1
☐ All of 1A-1.2
☐ 1A-1.3
☐ 1A-1.4
☐ 1B-1.1
☐ 1B-2.2
☐ 1B-2.3
☐ 1C-2.1.1
☐ 1C-2.1.2

Note: The above testing does not have to performed by the Solution if the POI Device was tested as part of a listed Component.

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

HSM		
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)*
HSM name/identifier		
HSM manufacturer, model, and number		
PTS or FIPS 140 approval number for HSM		
HSM Hardware version #		
HSM Firmware version #		

Copy the above table for each additional HSM model being added or removed.

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

P2PE Requirements (including all testing procedures) for Decryption Management	P2PE Requirements (including all testing procedures) for Encryption Management and/or Key Management Services
☐ All 4A-1	☐ 1-3
☐ 4B-1.3	☐ 1-4
☐ 4B-1.7	☐ 5-1
☐ 5-1	☐ 5A-1.1
☐ 5A-1.1	

Part 3c. 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)*	
P2PE Application Name	P2PE Application version #	P2PE Application vendor name	P2PE Application reference #	Brief description of P2PE Application function/purpose	POI Device type name/identifier P2PE Application is installed on

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

P2PE Requirements (including all testing procedures)
☐ 1D-2.1

Part 3d. 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	Key Loading	Key Mgmt	CA/RA	Encryption Mgmt	POI Deployment	POI Management	Decryption Mgmt	
	☐	☐	☐	☐	☐	☐	☐	☐	
	☐	☐	☐	☐	☐	☐	☐	☐	
	☐	☐	☐	☐	☐	☐	☐	☐	

Appendix F: Change Impact Template for P2PE Components

This *P2PE Change Impact Template* is required for Administrative Change and Delta 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	Key Loading	Key Mgmt	CA/RA	Encryption Mgmt	POI Deployment	POI Management	Decryption Mgmt	
	☐	☐	☐	☐	☐	☐	☐	☐	
Type of Change *(Select one)*	☐ 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 Delta Change (if indicated at Part 1)

Delta Change Revision		
Identify the type of Delta changes applicable to this submission and complete the appropriate sections of this *P2PE Change Impact Template* (check all that apply). *Refer to the* P2PE Program Guide *for details about each type of Delta change.*		
Add/Remove POI Device Type *(Complete Part 3a)*	☐ Add	☐ Remove
Add/Remove HSM *(Complete Part 3b)*	☐ Add	☐ Remove
Add/Remove P2PE Application *(Complete Part 3c)*	☐ Add	☐ Remove
	Version Number of the Application:	
Add/Remove P2PE Component *(Complete Part 3d)*	☐ 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)

Add additional rows or pages as necessary if multiple POI devices are being added/removed in a single change submittal.

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 POI Device type(s) using the table below as a minimum set of testing procedures.

P2PE Requirements (including all testing procedures)
☐ All of 1A-1.1
☐ All of 1A-1.2
☐ 1A-1.3
☐ 1A-1.4
☐ 1B-1.1
☐ 1B-2.2
☐ 1B-2.3
☐ 1C-2.1.1
☐ 1C-2.1.2

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

Add additional rows or pages as necessary if multiple HSM devices are being added/removed in a single change submittal.

HSM		
Adding for inclusion in listing or removal from listing?	☐ Addition/Inclusion in listing *(**Red-lined** P-ROV review required, see details below)*	☐ Removal from *(No Red-lined P-ROV review required)*
HSM name/identifier		
HSM manufacturer, model, and number		
PTS or FIPS 140 approval number for HSM		
HSM Hardware version #		
HSM Firmware version #		

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

P2PE Requirements (including all testing procedures) for Decryption Management	P2PE Requirements (including all testing procedures) for Encryption Management and/or Key Management Services
☐ All 4A-1	☐ 1-3
☐ 4B-1.3	☐ 1-4
☐ 4B-1.7	☐ 5-1
☐ 5-1	☐ 5A-1.1
☐ 5A-1.1	

Part 3c. 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)*	
P2PE Application Name	P2PE Application version #	P2PE Application P2PE Vendor name	P2PE Application reference #	Brief description of P2PE Application function/purpose	POI Device type name/identifier P2PE Application is installed on

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

P2PE Requirements (including all testing procedures)
☐ 1D-2.1

Part 3d. 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
	PDCP	PMCP	KLCP	KMCP	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	

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 Section 5.2, "Delta Changes for P2PE Products"). 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 *(Select one)*	☐ 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 P2PE 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** Delta Change eligible for 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 Requirements/sub-Requirements are impacted

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

Add additional rows or pages as necessary if multiple POI device types are being added/removed in a single change submittal

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 POI Device types using the table below as a minimum set of testing procedures.

P2PE Requirements (including all testing procedures)
☐ **All of 1A-1.1**
☐ **All of 1A-1.2**
☐ **1A-1.3**
☐ **1A-1.4**
☐ **1B-1.1**
☐ **1B-2.2**
☐ **1B-2.3**
☐ **1C-2.1.1**
☐ **1C-2.1.2**

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 accurately map the internal version numbers to the publicly 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—For example, 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.

Appendix I: P2PE Applicability of Requirements

–––––The following matrix indicates with an "x" all P2PE Security Requirements that apply to P2PE Solutions (including Merchant-Managed Solutions), P2PE Applications, and P2PE Components.

Note: *Each requirement denoted includes all sub-requirements unless indicated otherwise.*

Notes for the P2PE Requirement Applicability Matrix:

1 - Where a Solution Provider (or a Merchant as a Solution Provider in a Merchant-Managed Solution - MMS) is using a PCI-Listed P2PE Component Provider, the Solution Provider is not required to have the requirements applicable to that P2PE Component assessed as part of their Solution assessment. For example, if a Solution Provider outsources to a PCI-Listed P2PE Encryption Management Component Provider, the Solution Provider is not required to assess to any of the requirements denoted below for Encryption Management. Note that neither a Solution Provider or a Merchant-Managed Solution Provider are permitted to outsource any requirements in Domain 3 (and additionally Appendix A for MMS). However, for any key management services requirements (Domain 5) not otherwise included as part of the assessment for included PCI-listed P2PE Component Providers, the Solution Provider is responsible for including all applicable key management services requirements in the scope of their assessment.

For example, if the P2PE Solution offers remote key-distribution using asymmetric techniques for the distribution of keys to POI devices for use in connection with account-data encryption, or the operation of an applicable CA/RA, or any other relevant key management service that has not already been assessed as part of the inclusion of a PCI-listed P2PE Component Provider, then the Solution assessment must include all applicable key management services requirements (Domain 5).

2 - Where an Encryption Management Component Provider is using a PCI-Listed P2PE POI Deployment or POI Management Component Provider, the Encryption Management Component Provider is not required to have the requirements applicable to that POI Deployment or POI Management Component, as applicable, assessed as part of their Encryption Management Component Provider assessment.

3 - Where a Key Injection Facility (KIF) Component Provider is using a PCI-Listed P2PE Key Loading or Key Management Component Provider, the KIF Component Provider is not required to have the requirements applicable to the Key Loading or Key Management Component, as applicable, assessed as part of their KIF Component Provider assessment.

4 - The "Remote Key" requirements are additional requirements that apply to any entity implementing remote key distribution using asymmetric techniques for the distribution of keys to POI devices for use in connection with account-data encryption. Note that these requirements are additional requirements that must be met – i.e., they cannot be assessed in isolation – they must be assessed in addition to all applicable Domain 5 requirements relevant to the assessment. Refer to Domain 5 in the P2PE Standard for more information.

5 - These requirements apply only to entities operating Certification and/or Registration Authorities. Refer to Domain 5 in the P2PE Standard for more information.

6 - Merchant-Managed Solutions are not permitted to utilize a hybrid decryption environment unless they are using a PCI-Listed P2PE Decryption Management Component Provider that employs hybrid decryption.

P2PE Security Requirements												
P2PE Requirement	Encryption Management Services			P2PE Application	Decryption Management Services	Key Management Services					Solution *(or MMS)* [1,4,6]
	POI Deployment[4]	POI Management[4]	Encryption Management[2,4]		Decryption Management[4]	Key Management[4]	Key Loading[4]	KIF[3,4]	CA/RA[5]	Remote Key[4]	
Domain 1												
1A-1	X		X								X
1A-2	X		X								X
1B-1.1	X		X								X
1B1.2		X	X								X
1B-2		X	X								X
1B-3		X	X								X
1B-4		X	X								X
1B-5		X	X								X
1C-1		X	X								X
1C-2	X	X	X								X
1D-1		X	X								X
1D-2	X	X	X								X
Note: *1E-1 is only applicable to Encryption Management Services Component Providers (EMCP, PDCP, PMCP)*												
1E-1	X	X	X								
Domain 2												
2A-1				X							
2A-2				X							
2A-3				X							
2B-1				X							
2B-2				X							
2B-3				X							
2B-4				X							
2C-1				X							

P2PE Security Requirements												
P2PE Requirement	Encryption Management Services			P2PE Application	Decryption Management Services	Key Management Services					Solution *(or MMS)* [1,4,6]
	POI Deployment[4]	POI Management[4]	Encryption Management[2,4]		Decryption Management[4]	Key Management[4]	Key Loading[4]	KIF[3,4]	CA/RA[5]	Remote Key[4]	
Domain 2 *(continued)*												
2C-2				X							
2C-3				X							
Domain 3												
3A-1											X
3A-2											X
3A-3											X
3A-4											X
3B-1											X
3C-1											X
Domain 4												
4A-1					X						X
4B-1					X						X
4C-1					X						X
Note: *If a hybrid decryption environment is being used, the following requirements (4D) will apply*												
4D-1					X						X
4D-2					X						X
4D-3					X						X
4D-4					X						X
Note: *4E-1 is only applicable to Decryption Management Services Component Providers (DMCP)*												
4E-1					X						
Domain 5												
1-1	***Note:*** *Not used in P2PE*											
1-2							X	X			
1-3	X	X	X		X	X	X	X	X		X

P2PE Security Requirements											
P2PE Requirement	Encryption Management Services			P2PE Application	Decryption Management Services	Key Management Services					Solution *(or MMS)* [1,4,6]
	POI Deployment[4]	POI Management[4]	Encryption Management[2,4]		Decryption Management[4]	Key Management[4]	Key Loading[4]	KIF[3,4]	CA/RA[5]	Remote Key[4]	
Domain 5 (continued)											
1-4	X	X	X		X	X	X	X	X		X
1-5						X	X	X			
Note: *PIN Requirements 2, 3, and 4 are all PIN-specific and are therefore omitted from P2PE*											
5-1	X	X	X		X	X		X	X		X
6-1	X	X	X		X	X		X	X		X
6-2	X	X	X		X	X		X	X		X
6-3	X	X	X		X	X		X	X		X
6-4	X	X	X		X	X		X	X		X
6-5	X	X	X		X	X		X	X		X
6-6	X	X	X		X	X		X	X		X
7-1	X	X	X		X	X		X	X		X
7-2	X	X	X		X	X		X	X		X
8-1	X	X	X		X	X	X	X	X		X
8-2	X	X	X		X	X	X	X	X		X
8-3	X	X	X		X	X	X	X	X		X
8-4	X	X	X		X	X	X	X	X		X
9-1	X	X	X		X	X		X	X		X
9-2	X	X	X		X	X		X	X		X
9-3	X	X	X		X	X		X	X		X
9-4	X	X	X		X	X		X	X		X
9-5	X	X	X		X	X		X	X		X
9-6	X	X	X		X	X		X	X		X
10-1	X	X	X		X	X	X	X			X

P2PE Security Requirements											
P2PE Requirement	Encryption Management Services			P2PE Application	Decryption Management Services	Key Management Services					Solution *(or MMS)* [1,4,6]
	POI Deployment[4]	POI Management[4]	Encryption Management[2,4]		Decryption Management[4]	Key Management[4]	Key Loading[4]	KIF[3,4]	CA/RA[5]	Remote Key[4]	
Domain 5 (continued)											
10-2	***Note:*** *Not used in P2PE*										
10-3											
10-4											
10-5											
11-1	X	X	X		X	X	X	X	X		X
11-2	X	X	X		X	X	X	X			X
12-1	X	X	X		X		X	X	X		X
12-2	X	X	X		X		X	X	X		X
12-3	X	X	X		X		X	X	X		X
12-4	X	X	X		X		X	X	X		X
12-5	X	X	X		X		X	X	X		X
12-6	X	X	X		X		X	X	X		X
12-7	X	X	X		X		X	X			X
12-8	X	X	X		X		X	X			X
12-9							X	X			
13-1	X	X	X		X		X	X	X		X
13-2	X	X	X		X		X	X	X		X
13-3	X	X	X		X		X	X	X		X
13-4	X	X	X		X		X	X	X		X
13-5	X	X	X		X		X	X	X		X
13-6	X	X	X		X		X	X	X		X
13-7	X	X	X		X		X	X	X		X
13-8	X	X	X		X		X	X	X		X
13-9							X	X			

P2PE Security Requirements											
P2PE Requirement	Encryption Management Services			P2PE Application	Decryption Management Services	Key Management Services					Solution *(or MMS)* [1,4,6]
	POI Deployment[4]	POI Management[4]	Encryption Management[2,4]		Decryption Management[4]	Key Management[4]	Key Loading[4]	KIF[3,4]	CA/RA[5]	Remote Key[4]	
Domain 5 (continued)											
14-1	X	X	X		X		X	X	X		X
14-2	X	X	X		X		X	X	X		X
14-3	X	X	X		X		X	X	X		X
14-4	X	X	X		X		X	X	X		X
14-5	X	X	X		X		X	X	X		X
15-1	X	X	X		X		X	X	X		X
15-2	X	X	X		X		X	X	X		X
15-3										X	
15-4										X	
15-5									X	X	
16-1	X	X	X		X		X	X	X		X
16-2	X	X	X		X		X	X	X		X
17-1	X	X	X		X						X
18-1	X	X	X		X						X
18-2	X	X	X		X	X	X	X	X		X
18-3	X	X	X		X		X	X			X
18-4										X	
18-5										X	
18-6							X	X			
18-7							X	X			
19-1	X	X	X		X		X	X	X		X
19-2	X	X	X		X		X	X	X		X
19-3	X	X	X		X		X	X	X		X
19-4	X	X	X		X		X	X	X		X

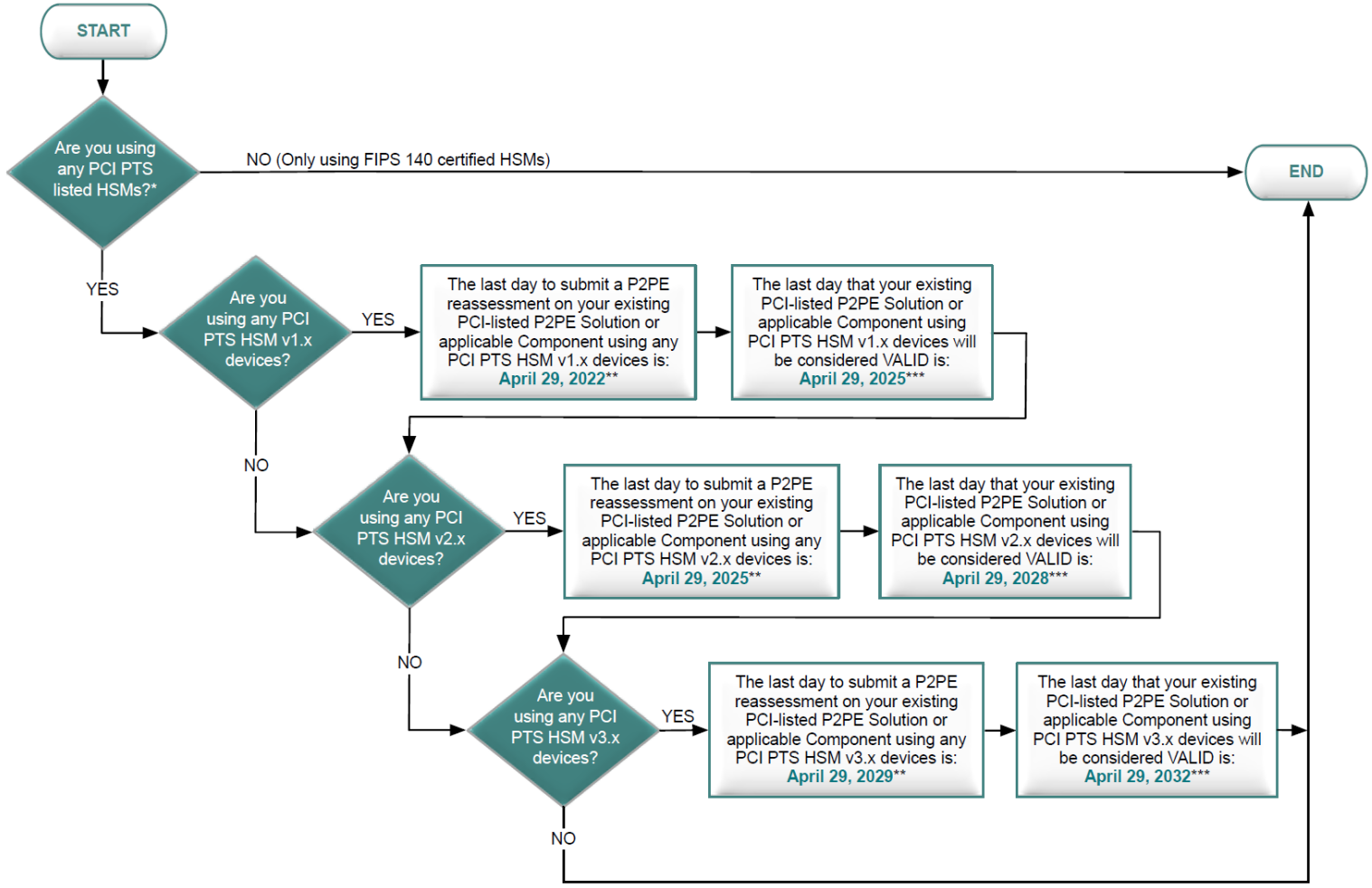
P2PE Security Requirements											
P2PE Requirement	Encryption Management Services			P2PE Application	Decryption Management Services	Key Management Services					Solution *(or MMS)* [1,4,6]
	POI Deployment[4]	POI Management[4]	Encryption Management[2,4]		Decryption Management[4]	Key Management[4]	Key Loading[4]	KIF[3,4]	CA/RA[5]	Remote Key[4]	
Domain 5 (continued)											
19-5	X	X	X		X		X	X	X		X
19-6									X	X	
19-7										X	
19-8										X	
19-9									X		
19-10									X		
19-11									X		
19-12									X		
20-1	X	X	X		X	X	X	X			X
20-2	X	X	X		X	X	X	X			X
20-3	X	X	X		X	X	X	X			X
20-4	X	X	X		X	X	X	X			X
20-5							X	X			
20-6							X	X			
21-1	X	X	X		X	X	X	X	X		X
21-2	X	X	X		X	X	X	X	X		X
21-3	X	X	X		X	X	X	X	X		X
21-4									X	X	
22-1	X	X	X		X	X	X	X	X		X
22-2	X	X	X		X	X	X	X	X		X
22-3									X		
22-4									X		
22-5									X		
23-1	X	X	X		X	X	X	X	X		X

P2PE Security Requirements											
P2PE Requirement	Encryption Management Services			P2PE Application	Decryption Management Services	Key Management Services					Solution *(or MMS)* [1,4,6]
	POI Deployment[4]	POI Management[4]	Encryption Management[2,4]		Decryption Management[4]	Key Management[4]	Key Loading[4]	KIF[3,4]	CA/RA[5]	Remote Key[4]	
Domain 5 (continued)											
23-2	X	X	X		X	X	X	X	X		X
23-3	X	X	X		X	X	X	X	X		X
24-1	X	X	X		X	X	X	X	X		X
24-2	X	X	X		X	X	X	X	X		X
25-1	X	X	X		X	X	X	X	X		X
25-2									X		
25-3									X		
25-4									X		
25-5									X		
25-6									X		
25-7									X		
25-8									X		
25-9									X		
26-1	X	X	X		X	X	X	X	X		X
27-1	X	X	X		X	X	X	X	X		X
27-2	X	X	X		X	X	X	X	X		X
28-1	X	X	X		X	X	X	X	X		X
28-2									X		
28-3									X		
28-4									X		
28-5									X		
29-1	X	X	X		X		X	X	X		X
29-2							X	X	X		
29-3	X	X	X		X		X	X	X		X

P2PE Security Requirements											
P2PE Requirement	Encryption Management Services			P2PE Application	Decryption Management Services	Key Management Services					Solution *(or MMS)* [1,4,6]
	POI Deployment[4]	POI Management[4]	Encryption Management[2,4]		Decryption Management[4]	Key Management[4]	Key Loading[4]	KIF[3,4]	CA/RA[5]	Remote Key[4]	
Domain 5 (continued)											
29-4	X	X	X		X	X	X	X	X		X
29-5	X	X	X		X	X	X	X	X		X
30-1	***Note:*** *Not used in P2PE*										
30-2											
30-3							X	X			
31-1	X	X	X		X	X	X	X	X		X
32-1	X	X	X			X	X	X	X		X
32-2									X		
32-3									X		
32-4									X		
32-5									X		
32-6									X		
32-7									X		
32-8 (8.1, 8.2)						X	X	X			
32-8 (8.3 – 8.7)							X	X			
32-9							X	X			
33-1	X	X	X		X		X	X	X		X
5A-1	X	X	X		X						X
Note: *If a hybrid decryption environment is being used, the following additional requirements (5H) will apply*											
5H-1					X						X
Note: *5I-1 is only applicable to Key Management Services Component Providers*											
5I-1											X

P2PE Security Requirements											
P2PE Requirement	Encryption Management Services			P2PE Application	Decryption Management Services	Key Management Services					Solution *(or MMS)* [1,4,6]
	POI Deployment[4]	POI Management[4]	Encryption Management[2,4]		Decryption Management[4]	Key Management[4]	Key Loading[4]	KIF[3,4]	CA/RA[5]	Remote Key[4]	
APPENDIX A											
***Note:** Appendix A is only applicable to Merchant-Managed Solutions (MMS)*											
MM-A-1											**X**
MM-A-2											**X**
MM-B-1											**X**
MM-C-1											**X**

Appendix J: PCI SSC-Listed PTS HSM Expiry Flowchart



* Answer YES if you are using any HSMs in your P2PE Solution or Component that were evaluated to the PCI PTS HSM Standard and subsequently listed on the PCI website (even if their approval has expired) and do not also have a corresponding FIPS 140 certificate (approval).

** Existing PCI-listed P2PE Solutions and applicable P2PE Components are prohibited from performing a P2PE reassessment with any expired HSMs that exceed the reassessment date shown relative to the specified PCI PTS HSM Standard version. Note that a successful reassessment is valid for three years.

*** P2PE Solutions and applicable P2PE Components must have replaced any expired HSMs with current (non-expired) HSMs by the date shown here relative to the specified PCI PTS HSM Standard version.