Payment Card Industry (PCI)

Point-to-Point Encryption (P2PE)®

Program Guide

Version 3.1

For Use With the PCI P2PE Standard v3.x

September 2024

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
December 2020	3.0 r1.0	Errata revision – resolved requirements in Appendix G part 3a Resolved definition of P2PE Expired Listings Other general revisions made for increased consistency and clarity
September 2024	3.1	General updates throughout document Added links to internal section references Former P2PE QSA terms have been updated in accordance with new terms in the currently published P2PE Qualification Requirements (QRs) regarding assessor companies and employees New terminology added as well as terminology revised New Publication references added as well as minor revisions to certain descriptions Partial section/structure reordering Added section regarding P2PE Technical FAQs Added content from published P2PE Technical FAQs where appropriate Revised content regarding PTS POI device and HSM expiry Added content regarding PTS POI device testing Added new Listed P2PE Product Outsourcing Matrix New figures regarding listing lifecycle and expiry Revisions to Appendices B, C, & D Removal of Appendices E, F, & G. External Change Impact Template to take their place. Internal references revised Typical response times updated to 40 calendar days Fixed the attributions in the Requirement Applicability Matrix for: 3A-4, 10-1, 12-8, 20-6 and 5I-1

Contents

i. Terminology

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

Term	Meaning
Accepted, Acceptance	A P2PE Product is deemed to have been "Accepted" (and "Acceptance" is deemed to have occurred, so long as such Acceptance has not been revoked, suspended, withdrawn, or terminated) when PCI SSC has: (i) received the corresponding Validated P2PE Product submission in the Portal, including the completed P-ROV(s), P-AOV, and all other documentation and information as required by the P2PE Standard and P2PE Program Requirements, from the P2PE Assessor Company qualified to perform the P2PE Assessment of the P2PE Product; (ii) received the corresponding P2PE Program fee for the P2PE Product submission; and (iii) confirmed that: - the P2PE Product submission to the Portal is complete (all applicable documents completed appropriately/sufficiently), and - the P2PE Assessor Company properly determined that the P2PE Product satisfies the P2PE Standard and P2PE Program Requirements for a Validated P2PE Product.
Administrative Change	A change affecting defined administrative information on the Listing for a Listed P2PE Product that is not a Delta Change. See also: *Delta Change*
Administrative Expiry	The early expiry of a Listed P2PE Product due to Program Requirements for that Listed P2PE Product not being satisfied, whereby the P2PE Product becomes an Expired P2PE Product, is moved to the applicable Expired P2PE Product List, and is no longer considered a Validated P2PE Product.
Annual Revalidation	The annual process required of P2PE Product Vendors to confirm their Listed P2PE Product continues to adhere to the P2PE Standard and Program Requirements.
Delta Change	A security-impacting change to a Listed P2PE Product that affects defined elements on the associated Listing for that P2PE Product that is not an Administrative Change. See also: *Administrative Change*
Expired P2PE Product	A P2PE Product on the P2PE Expired Listings that is no longer considered a Validated P2PE Product.

Term	Meaning
Full Assessment	A complete assessment and validation of a P2PE Product by a qualified P2PE Assessor Company in accordance with the P2PE Standard, Program Requirements, and all associated documentation that results in a Validated P2PE Product. A Full Assessment is NOT an: - Administrative Change, or a - Delta Change A New Assessment and a Reassessment both require a Full Assessment. See also: *New Assessment, Reassessment*
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 Products	Refers to the List of Validated P2PE Solutions, List of Validated P2PE Components, and List of Validated P2PE Applications. The List of Validated P2PE Products is the authoritative source of on-going Acceptance by PCI SSC of Validated P2PE Products.
List of Validated P2PE Solutions	The Council's authoritative List of Validated P2PE Solutions appearing on the Website.
Listed	A Validated P2PE Product has been published on the Website after corresponding Acceptance has occurred, so long as such Acceptance has not been revoked, suspended, withdrawn, or terminated. See also: *List of Validated P2PE Products, Acceptance*
Listing	The information regarding a Validated P2PE Product appearing on the applicable List of Validated P2PE Products after Acceptance has occurred. Listings contain information about Validated P2PE Products, as described in *Appendix B*, *Appendix C*, and *Appendix D* herein.
New Assessment	A Full Assessment of a P2PE Product where that P2PE Product: - Is not already Listed, or - Is an Expired P2PE Product See also: *Reassessment*
P2PE Application Assessment	A Full Assessment of a P2PE Application to validate compliance with the P2PE Standard as part of the Program Requirements.
P2PE Application Assessor Company	Refer to the *P2PE Qualification Requirements.*
P2PE Application Assessor Employee	Refer to the *P2PE Qualification Requirements.*
P2PE Application Vendor	An entity that develops and then sells, distributes, or licenses a P2PE Application for use in a P2PE Solution or an applicable P2PE Component.
P2PE Assessment	Refer to the *P2PE Qualification Requirements.*

Term	Meaning
P2PE Assessor Company	Refer to the *P2PE Qualification Requirements.*
P2PE Assessor Employee	Refer to the *P2PE Qualification Requirements.*
P2PE Attestation of Validation (P-AOV)	A form for P2PE Assessors and P2PE Vendors to declare the validation status of a P2PE Product to the P2PE Standard and Program Requirements. See also: *P-AOV* in Related Publications
P2PE Component	A P2PE service that is eligible for validation as a "P2PE Component" (as defined in the P2PE Glossary and herein) intended for use in a P2PE Solution as part of the P2PE Program.
P2PE Component Assessment	A Full Assessment of a P2PE Component to validate compliance with the P2PE Standard as part of the P2PE Program.
P2PE Component Provider	An entity providing a service on behalf of other P2PE Solution Providers or P2PE Component Providers, intended for use in P2PE Solutions.
P2PE Expired Listings (Expired List / Expired Listings)	The Council's authoritative list of Expired P2PE Products appearing on the Website. Expired P2PE Products are no longer considered Validated P2PE Products.
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. See also: *P2PE Glossary* in the Related Publications section
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. See also: *PIM* in the Related Publications section
P2PE Product	A P2PE Application, P2PE Component, or P2PE Solution.
P2PE Program (Program)	The PCI SSC program for Point-to-Point Encryption (P2PE)® whereby an entity can choose to have their P2PE Product validated by a qualified P2PE Assessor, and subsequently submitted to PCI SSC for consideration of being Accepted and Listed for purposes of demonstrating compliance with the PCI P2PE Standard and Program Requirements.
P2PE Program Documents (Program Documents)	The P2PE Standard and P2PE Program Guide, all written agreements executed between PCI SSC and P2PE Vendors, and PCI SSC and P2PE Assessors (Companies & Employees) in connection with the P2PE Program, all other materials, requirements, obligations, policies, and procedures published from time to time by PCI SSC on the Website or elsewhere relating to the P2PE Program, and all successor versions of the foregoing, in each case, as amended from time to time.

Term	Meaning
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 Program Requirements (Program Requirements)	All requirements, obligations, policies and procedures for P2PE Products, P2PE Product Vendors and P2PE Assessors, as applicable, and as set forth in the corresponding P2PE Program Documents, the VRA or otherwise established by PCI SSC from time to time in connection with the P2PE Program, including without limitation, those relating to disclosure, PCI SSC's quality assurance initiatives, and / or export control and administration, and such P2PE Vendor's warranties pursuant to the VRA.
P2PE Report on Validation (P-ROV)	A set of templates provided by PCI SSC that require completion by a P2PE Assessor Company as part of the validation effort of a P2PE Product as per the Program Requirements. See also: *P-ROV* in the Related Publications section
P2PE Solution Assessment	A Full Assessment of a P2PE Solution 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. See also: *P2PE Standard* in the Related Publications section
P2PE Vendor	A P2PE Solution Provider, P2PE Component Provider, or P2PE Application Vendor.
Participating Payment Brand	A payment card brand that, as of the time in question, is then formally admitted as (or an affiliate of) a member of PCI SSC pursuant to its governing documents. ***Note:*** *At the time of this publication, Participating Payment Brands include PCI SSC's Founding Members and Strategic Members.*
PCI DSS Assessment	The onsite review of an entity by a QSA Company to determine the entity's compliance with the PCI DSS for QSA Program purposes.
PCI SSC or the Council	Refers to the PCI Security Standards Council, LLC.
Reassessment	A Full Assessment of a Listed P2PE Product to the P2PE Standard and Program Requirements where that P2PE Product is not an Expired P2PE Product. See also: *New Assessment*

Term	Meaning
Reference Number	A unique identifier assigned to a Validated P2PE Product upon Acceptance and denoted on its Listing per the Program Requirements.
Solution-specific P2PE Application	A Validated P2PE Application included as part of a P2PE Solution assessment for use in that P2PE Solution only that is not separately Listed on the List of Validated P2PE Applications.
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. 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 undergone a Full Assessment by a P2PE Application Assessor Company that satisfies the P2PE Standard and Program Requirements, as documented in the corresponding P-ROV(s), AOV, and all other associated supporting material and information. See also: *List of Validated P2PE Applications*
Validated P2PE Component	A P2PE Component that has undergone a Full Assessment by a P2PE Assessor Company that satisfies the P2PE Standard and P2PE Program, as documented in the corresponding P-ROV(s), AOV, and all other associated supporting material and information. See also: *List of Validated P2PE Components*
Validated P2PE Product	A Validated P2PE Application, Validated P2PE Component, or Validated P2PE Solution. See also: *List of Validated P2PE Products*
Validated P2PE Solution	A P2PE Solution that has undergone a Full Assessment by a P2PE Assessor Company that satisfies the P2PE Standard and P2PE Program, as documented in the corresponding P-ROV(s), AOV, and all other associated supporting material and information. See also: *List of Validated P2PE Solutions*
Vendor Release Agreement (VRA)	The then-current and applicable form of vendor release agreement that PCI SSC: (a) Requires to be executed by P2PE Vendors in accordance with the Program Requirements, and (b) Is available on the Website. See also: *VRA* in the Related Publications section
Website	The then-current PCI SSC Website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org.

Term	Meaning
Wildcard	A character that may be substituted for a defined subset of possible characters in a P2PE Application versioning scheme.

ii. Related Publications

This Program Guide shall be used in conjunction with the latest versions of (or successor documents to) the following PCI SSC publications, each as available through the Website. Related Publications are italicized within this document.

Document name	Description
Payment Card Industry (PCI) Point-to-Point Encryption Glossary of Terms, Abbreviations, and Acronyms (“P2PE Glossary”)	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.
PCI Point-to-Point Encryption Security Requirements and Testing Procedures (“P2PE Standard”)	Contains the requisite security requirements and associated test procedures for the assessment and validation of P2PE Products.
PCI Point-to-Point Encryption Technical FAQs for use with PCI P2PE version 3.x (“P2PE Technical FAQs”)	Technical FAQs are normative and are an integral and mandatory part of the PCI P2PE Standard and Program. Technical FAQs must be fully considered during a P2PE Assessment.
PCI P2PE Report on Validation Reporting Template (“P-ROV”)	Mandatory templates used by P2PE Assessors for validating a P2PE Product.
PCI P2PE Attestation of Validation (“P-AOV”)	A form for P2PE Assessor Companies and/or P2PE Vendors to attest to the validation status of a P2PE Product and the specific submission type to PCI SSC.
PCI Qualification Requirements for Point-to-Point Encryption (P2PE)® - P2PE Assessors and P2PE Application Assessors (“P2PE Qualification Requirements”)	The minimum requirements and related documentation that a P2PE Assessor Company and P2PE Application Assessor Company, including P2PE Assessor Employees and P2PE Application Assessor Employees, must satisfy and provide to the PCI Security Standards Council, LLC ("PCI SSC”) in order to qualify to perform P2PE Assessments as a participant in the P2PE Assessor Program.
PCI Data Security Standard Qualification Requirements For Qualified Security Assessors (QSA) *("QSA Qualification Requirements")*	A baseline set of requirements that describe the necessary qualifications for security companies and their employees to be qualified by PCI SSC to perform PCI DSS Assessments.
PCI Qualification Requirements for Qualified PIN Assessors (QPA) (“QPA Qualification Requirements”)	A baseline set of requirements that describe the necessary qualifications for security companies and their employees to be qualified by PCI SSC to perform PCI PIN Assessments.
Vendor Release Agreement (“VRA”)	Establishes the terms and conditions under which Validated P2PE Products are Accepted and Listed by PCI SSC.
PCI P2PE Change Impact Template (“Change Impact Template”)	Mandatory template to account for and submit Administrative Changes and Delta Changes to Listed P2PE Products.

Document name	Description
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.
PCI SSC Remote Assessments Guidelines and Procedures	Describes how remote assessment methods may be incorporated into practices for validating environments, solutions, and products to PCI SSC standards.
PCI PIN Transaction Security (PTS) Device Testing and Approval Program Guide ("PTS Program Guide")	Program information for the PTS Program, which includes program information for PTS POI devices and PTS HSMs.

1. Introduction

***Note**: Capitalized terms used but not otherwise defined herein have the meanings set forth in Section i Terminology, in the P2PE Glossary or the P2PE Qualification Requirements (found on the Website), as applicable.*

This document, the PCI Point-to-Point Encryption (P2PE)® Program Guide, provides information on the P2PE Program operated and managed by the PCI Security Standards Council, LLC (PCI SSC).

The P2PE Program Guide is intended for P2PE Assessor Companies and P2PE Vendors of P2PE Products (P2PE Solutions, P2PE Components, and P2PE Applications).

***Note:** Information regarding the qualification of P2PE Assessor Companies and their employees can be found in the PCI P2PE Qualification Requirements on the Website.*

1.1. P2PE Program Overview

A P2PE Vendor may choose to have its P2PE Products validated to the P2PE Standard as part of the Program in order to have those P2PE Products considered for Acceptance by PCI SSC and included in the applicable List of Validated P2PE Products on the Website.

***Note:** Refer to Figure 1: P2PE Products Overview below.*

- A P2PE Solution can be made up of Validated P2PE Applications and Validated P2PE Components or can be validated as a standalone solution.
- P2PE Applications and P2PE Components can be validated and Listed on the Website on a standalone basis and made available for P2PE Components and P2PE Solutions. Refer to Section 2.1.3 P2PE Component Providers for details on P2PE Components.
- The P2PE requirements and test procedures (sourced from the P2PE Standard) for validating P2PE Products can be found in the corresponding P2PE Report on Validation (P-ROV) templates found on the Website.
- For each P2PE Product to be considered for Acceptance by PCI SSC and subsequently Listed on the Website as a Validated P2PE Product, 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 and described herein.
- Listed P2PE Products must be revalidated on an annual basis. Refer to Section 6.1 Annual Revalidation of Listed P2PE Products for further details.
- A Reassessment is required on all Listed P2PE Products every three years based on the Acceptance date of each Listing. Refer to Section 6.2 Reassessment of Listed P2PE Products for further details.
- 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 Program Requirements. Refer to Section 5 Changes to Listed P2PE Products for further details.
- For a mapping of the requirements of the P2PE Standard to all P2PE Products, refer to Appendix H.

***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.*

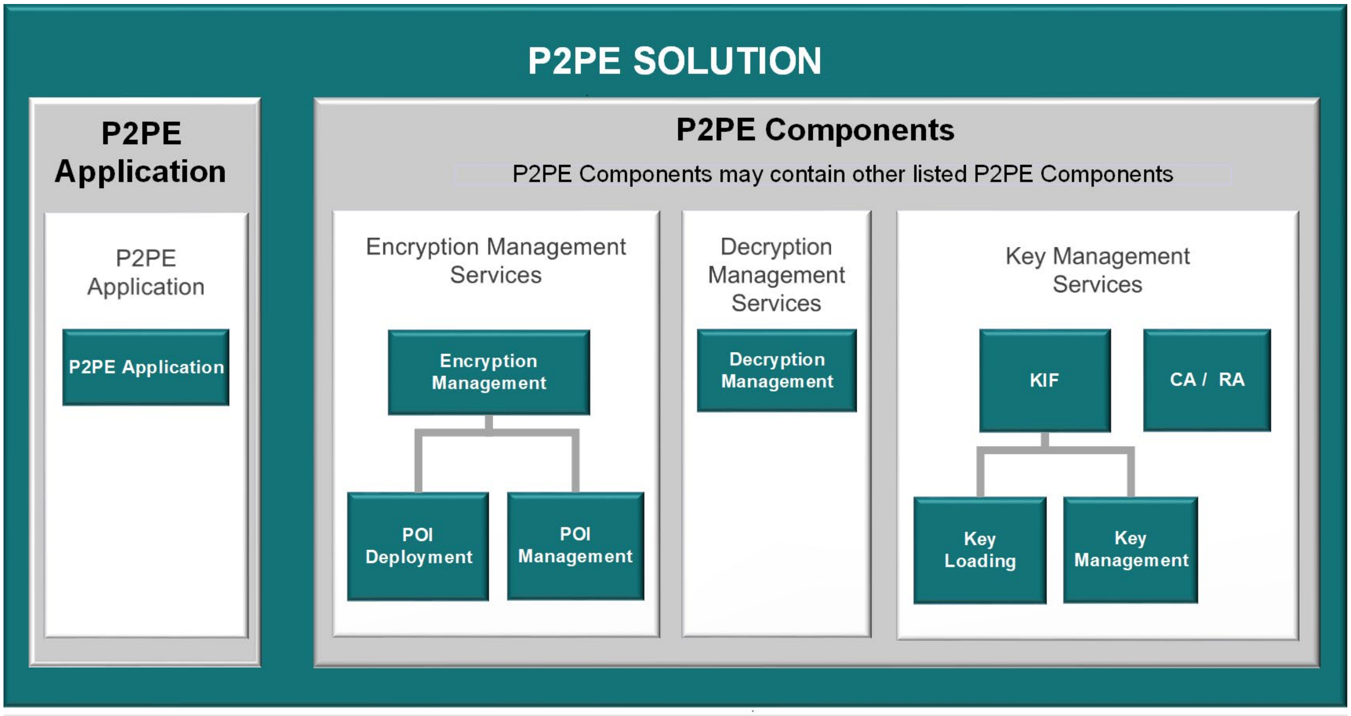


Figure 1: P2PE Products Overview

1.2. Updates to Documents and Security Requirements

This Program Guide is reviewed regularly and may be modified to reflect continual improvement and quality management of the P2PE Program.

PCI SSC reserves the right to add, change, amend, or withdraw security requirements, test requirements, guidance, training, or other requirements at any time.

PCI SSC may provide interim updates to the PCI community through a variety of means, including required training, e-mail bulletins and newsletters, frequently asked questions (which may include technical/normative FAQs), the Website, and other communication methods.

If change to the P2PE Program is required, PCI SSC endeavors to work closely with stakeholders to help minimize the impact.

1.3. Technical FAQs

The PCI P2PE Technical FAQs provide answers to questions regarding the PCI P2PE Standard and Program. The P2PE Technical FAQs are a separate document from the P2PE Standard and are effective immediately upon publication.

Technical FAQs are normative and are an integral and mandatory part of the PCI P2PE Standard and Program. Technical FAQs must be fully considered during a PCI P2PE Assessment.

The PCI P2PE Technical FAQs document can be found in the PCI Council's Document Library for P2PE on the Website at: https://www.pcisecuritystandards.org/document_library.

2. Roles and Responsibilities

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

Note: *Refer to Table 2: P-ROV Templates as needed for a list and description of all the P-ROV templates used in P2PE v3.x Assessments.*

2.1. P2PE Vendors

Note: *The decision to undergo an assessment of a P2PE Product in pursuit of Acceptance by PCI SSC and subsequent Listing of the Validated P2PE Product on the Website is a business decision of the P2PE Vendor.*

P2PE Vendors (P2PE Solution Providers, P2PE Component Providers, and P2PE Application Vendors) seeking Acceptance and subsequent Listing of their Validated P2PE Product as part of the Program are entities that:

- 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, an AOV, and all other required information and documentation for the submission to PCI SSC.

2.1.1. P2PE Solution Providers

P2PE Solution Providers are entities 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 P2PE Solution Provider has numerous options in creating a P2PE Solution. They can satisfy all the P2PE requirements solely as the Solution Provider, or they can choose to outsource applicable requirements to Third Party Service Providers, Listed P2PE Component Providers, and Listed P2PE Application Vendors. Refer to the subsequent sections below for more information.

2.1.2. P2PE Application Vendors

A P2PE Application Vendor develops applications with access to clear-text account data for use on a PCI-approved PTS POI device intended to be used in a P2PE Solution. P2PE Application Vendors must:

- Have their applications assessed against the P2PE Standard for secure operation within the applicable PCI-approved PTS POI device(s), and
- Provide corresponding Implementation Guides that describe the secure installation and administration of such applications on the corresponding PCI-approved PTS POI devices.

A P2PE Application may be assessed as part of an overall P2PE Solution (referred to as a Solution-specific P2PE Application) or may optionally be validated and Accepted as a standalone, Validated P2PE Application, and Listed on the List of Validated P2PE Applications.

Note*: P2PE Applications must be validated by a P2PE Application Assessor Company, whether included as part of a P2PE Solution assessment (Solution-specific P2PE Application), or as an individual P2PE Application intended to be Listed as a Validated P2PE Application.*

For P2PE Applications intended for use in multiple P2PE Solutions or applicable P2PE Components, 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 or P2PE Component in which it is used.

A P2PE Application P-ROV 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:

- Require a P2PE Assessment for Program purposes, and
- Are performed on behalf of a P2PE Solution Provider or a P2PE Component Provider for use in P2PE Solutions. These services (and their respective P2PE Component Providers) are described further below.

Only P2PE Components validated by a P2PE Assessor Company 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 must be submitted to PCI SSC for each P2PE Component assessed as part of the Program for it to be Accepted and Listed. If a P2PE Component service described above is assessed as part of a P2PE Solution (or a P2PE Component, as applicable) 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 (or P2PE Component Provider) customers' P2PE Assessments.

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

P2PE Assessor Companies are qualified to perform P2PE Assessments of P2PE Components for consideration of Acceptance by PCI SSC and subsequent inclusion on the List of Validated P2PE Components.

Encryption Management Services (EMS)

Encryption Management Services relates to the distribution, management, and use of PCI-approved PTS POI devices in a P2PE Solution.

- **Encryption Management Component Provider (EMCP)** is an entity that deploys and manages PCI-approved PTS POI devices and any resident P2PE Applications or P2PE Non-payment Software that can support a P2PE Solution.
- **POI Deployment Component Provider (PDCP)** is an entity that prepares and deploys PCI-approved PTS POI devices and any resident P2PE Applications or P2PE Non-payment Software that can support a P2PE Solution.
- **POI Management Component Provider (PMCP)** is an entity that maintains the PCI-approved PTS POI devices and any resident P2PE Applications or P2PE Non-payment Software, once deployed, that can support a P2PE Solution.

The EMS P-ROV must be used to validate P2PE Components included within Encryption Management Services.

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 used to validate P2PE Components included within Decryption Management Services.

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 (KIF)** is an entity that performs cryptographic key services for PCI-approved PTS POI devices and HSMs (including, but not limited to, key generation, conveyance, and/or key loading).
- **Key Loading Component Provider (KLCP)** is an entity that manages the cryptographic key loading for PCI-approved PTS POI devices and HSMs that can support a P2PE solution.
- **Key Management Component Provider (KMCP)** is an entity that manages cryptographic key generation and key conveyance for PCI-approved PTS 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 must be used to validate P2PE Components included within Key Management Services.

2.1.4. Third-Party Service Providers

A P2PE Solution Provider (or a merchant acting as its own P2PE Solution Provider in the case of a Merchant-Managed Solution) or P2PE Component Provider may choose to manage their P2PE Solution or P2PE Component, respectively, without outsourcing to Third-Party Service Providers.

Alternatively, a P2PE Solution Provider (or a merchant acting as its own P2PE Solution Provider in the case of a Merchant-Managed Solution) or P2PE Component Provider may choose to outsource certain services that are part of the applicable P2PE Solution or P2PE Component to Third-Party Service Providers who perform these services on behalf of the P2PE Solution Provider or the P2PE Component Provider.

All P2PE services 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. Third-Party Service Providers also have the option of having their P2PE Component services validated under the Program.

There are two validation options for Third-Party Service Providers performing P2PE functions on behalf of P2PE Solution Providers or P2PE Component Providers:

1) Undergo a P2PE Assessment of the applicable P2PE Component services against relevant P2PE Requirements and have their P2PE Assessor Company 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 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 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 services to Third-Party Service Providers and have the services assessed as part of the overall P2PE Assessment of that P2PE Solution or P2PE Component; and/or

2) A P2PE Solution Provider or P2PE Component Provider (or a merchant as a P2PE Solution Provider in the case of an MMS) can outsource certain P2PE Component services to Listed P2PE Component Providers and report use of those Listed P2PE Component(s) in its P2PE Solution P-ROV or applicable P2PE Component P-ROV.

P2PE Solution Providers (or merchants as P2PE Solution Providers in the case of an MMS) and P2PE Component Providers must manage the overall P2PE Solution or P2PE Component, respectively, and any third-party services (and corresponding Third-Party Service Providers) used to perform P2PE Component services 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. P2PE Assessor Companies

There are two types of P2PE Assessor Companies:

P2PE Assessor Company:

P2PE Assessor Companies are QSA or QPA companies that have been additionally qualified by PCI SSC to perform P2PE Assessments of P2PE Solutions and P2PE Components.

Note: *P2PE Assessor Companies are not qualified by PCI SSC to perform P2PE Application Assessments unless they are also qualified as a P2PE Application Assessor Company.*

P2PE Application Assessor Company:

P2PE Application Assessor Companies are P2PE Assessor Companies that have been qualified by PCI SSC to perform P2PE Assessments of P2PE Solutions, P2PE Components, in addition to P2PE Applications.

P2PE Assessor Companies are responsible for:

- Performing P2PE Assessments of P2PE Solutions and P2PE Components (and P2PE Applications for P2PE Application Assessor Companies) in accordance with the P2PE Standard, the P2PE Program, 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 Applications for P2PE Application Assessor Companies) against the P2PE Standard.
- Documenting each P2PE Assessment using the applicable P-ROV Reporting Templates.

- Submitting the applicable P-ROV(s) 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.

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.

2.3. PCI Security Standards Council (PCI SSC)

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 Products on the Website;
- Hosts the P2PE Expired Listings on the Website;
- Provides required training for and qualifies P2PE Assessor Companies (and their P2PE Assessor Employees), P2PE Application Assessor Companies (and their P2PE Application Assessor Employees), to assess and validate P2PE Products against the P2PE Standard and Program;
- Maintains and updates the P2PE Standard, Program, and related documentation;
- Reviews all P-ROVs (and other related documents) 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, Change Impact Submissions, and Annual Revalidations) are correct as to form;
    - The P2PE Assessor Company determines whether P2PE Products are eligible for validation under the P2PE Program (PCI SSC reserves the right to reject or remove the applicable Listing of any Validated P2PE Product determined to be ineligible for the P2PE Program);
    - The P2PE Assessor Company adequately report the P2PE compliance of P2PE 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, a P2PE Assessor Company's operations appear to conform to PCI SSC's quality assurance and qualification requirements. (Refer to Section 4.6 P2PE Assessor Information.)

***Note**: PCI SSC does not assess or validate P2PE Products for P2PE compliance; assessment and validation is the role of the P2PE Assessor Company qualified to evaluate the P2PE Product. Listing of a P2PE Product on the List of Validated P2PE Products signifies only that the applicable P2PE Assessor Company has determined that the P2PE Product complies with the P2PE Standard and Program Requirements, that the P2PE Assessor Company has submitted the corresponding P-ROV(s) and all associated documentation and information to PCI SSC, and that everything submitted to PCI SSC has satisfied all Program Requirements as of the time of PCI SSC's review.*

2.4. Customers Using Listed P2PE Solutions

***Note:** The PCI Security Standards Council (PCI SSC) does not manage compliance programs and does not impose any consequences for non-compliance. Whether an entity is required to comply with or validate compliance to a PCI SSC standard is at the discretion of organizations that manage compliance programs, such as a payment brand, acquirer, or other entity.*

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

- Determining which P2PE Solutions, including the associated PCI-approved PTS POI devices and P2PE Applications to implement.
- Adhering to the *P2PE Instruction Manual* (PIM), provided to the merchant by the P2PE Solution Provider.

2.5. PCI-recognized Laboratories

Security laboratories qualified by PCI SSC under the PCI SSC laboratory program (“PCI-recognized Laboratories”) are responsible for the evaluation of PTS POI devices, KLDs, 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 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 if a given P2PE Product (which may include multiple POI/HSM/KLD devices) is in compliance with the P2PE Standard.*

2.6. Payment Device (Hardware) Vendors

A POI device vendor submits a POI device for evaluation to a PCI-recognized Laboratory. Only eligible PCI-approved PTS POI devices (per the P2PE Standard and Program Requirements) on the list of “Approved PTS Devices” on the Website may be used as part of a P2PE Solution.

2.7. Participating Payment Brands

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

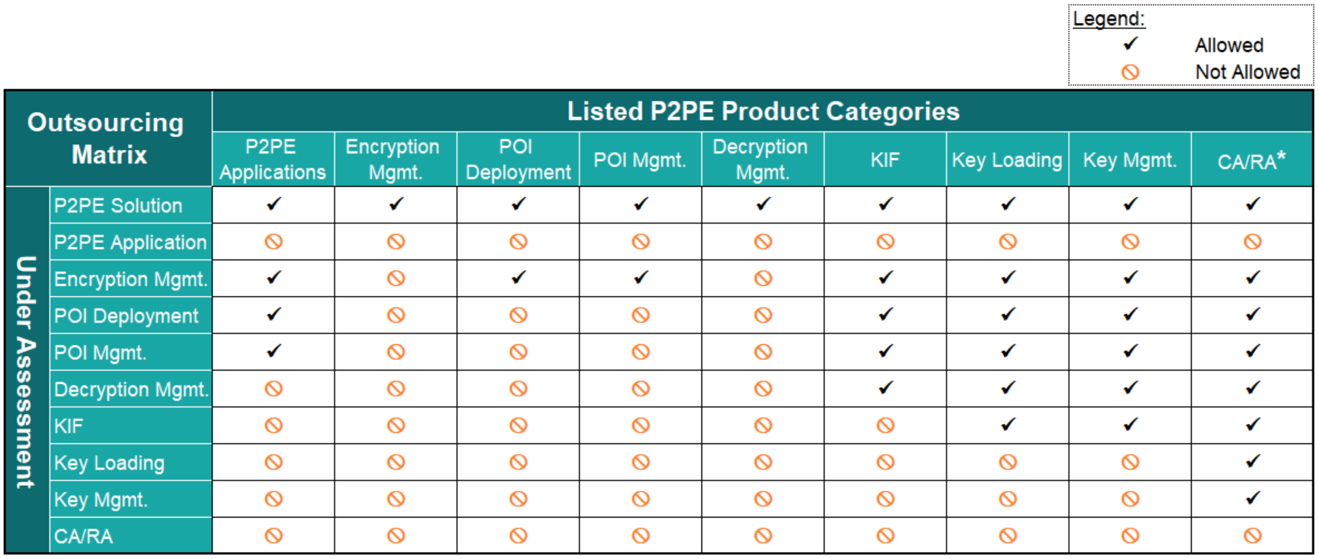
3. P2PE Product Assessment Considerations

The following sections provide useful information and applicable criteria related to defined P2PE Product elements and/or dependencies that must be considered for P2PE Product assessments.

3.1. Listed P2PE Product Outsourcing Matrix

***Note**: Refer to* Figure 1: P2PE Products Overview *for a diagram of all the P2PE Product categories.*

The P2PE Standard and Program provide significant flexibility in allowing the use of Listed P2PE Products to assist in satisfying P2PE Program Requirements for a P2PE Product assessment. The following matrix indicates the allowable Listed P2PE Products that can be included in a P2PE Product undergoing validation. While the use of Listed P2PE Products in a P2PE Product assessment is optional, all requisite requirements must be satisfied by the P2PE Product under assessment. Refer to Appendix H: P2PE Applicability of Requirements.



Legend:
✓ Allowed
⊘ Not Allowed

Outsourcing Matrix		Listed P2PE Product Categories								
		P2PE Applications	Encryption Mgmt.	POI Deployment	POI Mgmt.	Decryption Mgmt.	KIF	Key Loading	Key Mgmt.	CA/RA*
Under Assessment	P2PE Solution	✓	✓	✓	✓	✓	✓	✓	✓	✓
	P2PE Application	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘
	Encryption Mgmt.	✓	⊘	✓	✓	⊘	✓	✓	✓	✓
	POI Deployment	✓	⊘	⊘	⊘	⊘	✓	✓	✓	✓
	POI Mgmt.	✓	⊘	⊘	⊘	⊘	✓	✓	✓	✓
	Decryption Mgmt.	⊘	⊘	⊘	⊘	⊘	✓	✓	✓	✓
	KIF	⊘	⊘	⊘	⊘	⊘	⊘	✓	✓	✓
	Key Loading	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	✓
	Key Mgmt.	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	✓
	CA/RA	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘

* *Listed CA/RAs can be used to complement a P2PE Product assessment, e.g., to accommodate Remote Key Distribution, however they cannot be used to otherwise descope a P2PE Component assessment.*

Figure 2: Listed P2PE Product Outsourcing Matrix

3.2. PCI-Approved PTS POI Devices

The use of eligible PCI-approved PTS POI devices (with SRED) is mandatory in the P2PE Standard and Program Requirements, and they are a primary element of a Validated P2PE Solution. The following information is paramount regarding their use:

3.2.1. PTS POI Device Expiry

A Listed (not Expired) P2PE Product with expired PCI-approved PTS POI devices may undergo a Reassessment 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 Listed P2PE Product.

A PCI-approved PTS POI device may not be used in a Listed P2PE Product longer than five years past the corresponding PTS POI device expiry date. A Listed P2PE Product will be subject to Administrative

Expiry per Section 6.1 if all of the P2PE Product's associated PTS POI device types exceed the five-year window.

A table is included in the associated *P2PE Technical FAQs* on the Website that provides the current PTS POI device expiry dates and the corresponding Reassessment window for Listed P2PE Products using these devices. The P2PE Technical FAQs also contain information regarding POI v6+ device firmware expiry.

The following information applies to PTS POI v6+ device firmware expiry. Refer to the *PTS Program Guide* on the Website for additional details.

PTS POI v6+ Firmware Expiry

New Assessments: As per the P2PE Standard, the PTS POI device approval must not be expired. In addition, for PTS POI v6 and later devices, the firmware must not be expired and past its 4-month grace period (i.e., it must not be red status). If at any time prior to Acceptance of the P2PE Product submission, including during the PCI SSC AQM review process, the PTS POI device firmware status turns red, the P2PE Product submission will be rejected.

Annual Revalidations and Reassessments: Entities are encouraged to use non-expired PTS POI device firmware. Regarding the overall PTS POI approval expiry, refer to the information above as well as the *P2PE Technical FAQs*.

3.2.2. Previously Deployed PTS POI Devices

The P2PE Standard contains various requirements regarding the establishment and enablement of PTS POI devices in merchant locations for use in a validated P2PE solution. If these requirements are not specifically adhered to, it may be difficult or impossible for a P2PE Assessor to verify the applicable requirements in the Standard have been satisfied, especially when the PTS POI devices were deployed either without knowledge of the requirements and/or prior to a P2PE Assessment.

P2PE Solution Providers (or P2PE Component Providers, as applicable) should engage a P2PE Assessor as soon as possible to assess the status of the previously deployed PTS POI devices. The P2PE Assessor can assess the solution provider's documented processes for their PTS POI deployment and note any potential deficiencies requiring remediation.

The following table depicts various scenarios and associated guidance for both a P2PE Solution Provider and a P2PE Assessor.

Table 1: Uses Cases for Previously Deployed PTS POI Devices

SCENARIO	PROCESS
New Assessments A P2PE Assessor is engaged to perform an initial assessment of a solution provider's new P2PE solution. There are PTS POI device type(s) that need to be assessed that have already been deployed to merchant locations.	The P2PE Solution Provider engages a P2PE Assessor to assess their solution as required by the PCI P2PE Standard and Program. - If the P2PE Assessor determines the applicable P2PE Standard requirements regarding the previously deployed PTS POI devices have been satisfied, the P2PE Assessor will document the P-ROV accordingly, which per the Program Requirements, can be submitted to the PCI Council upon completion of a successful P2PE Assessment. - If the solution provider lacks sufficient evidence to verify the applicable P2PE requirements have been satisfied (as determined by a P2PE Assessor during a P2PE Assessment), then all firmware, cryptographic keys[1], configurations, and software must be reloaded into the POI devices in accordance with applicable P2PE requirements. At this point, the P2PE Assessor can reassess the applicable requirements.
Adding a New Merchant with the same PTS POI Device Types to a Listed P2PE Solution A solution provider with a Listed P2PE Solution wants to add a merchant that has already deployed PTS POI devices of the same POI device type as those approved for use in their P2PE Solution (as shown as device dependencies on the Solution Listing).	The P2PE Solution Provider follows their documented processes that were assessed previously as part of their P2PE Assessment. - If the applicable P2PE requirements regarding the previously deployed PTS POI devices have been satisfied, the results must be documented by the solution provider and retained for future review. - If the solution provider lacks sufficient evidence to verify the applicable P2PE requirements have been satisfied, then all firmware, cryptographic keys[1], configurations, and software must be reloaded into the PTS POI devices in accordance with applicable P2PE requirements.
Adding a New Merchant with different PTS POI Device Types to a Listed P2PE Solution A solution provider with a Listed P2PE Solution wants to add a merchant that has already deployed PTS POI devices of a different POI device type as those approved for use in their P2PE Solution.	The P2PE Solution Provider must engage a P2PE Assessor. The P2PE Assessor must follow the Program Requirements and the Delta Change process to add the new PTS POI device type(s) to the Listed P2PE Solution. The P2PE Solution Provider follows their documented processes that were assessed previously as part of their P2PE Assessment. - If the applicable P2PE requirements regarding the previously deployed PTS POI devices have been satisfied, the results must be documented by the solution provider and retained for future review. - If the solution provider lacks sufficient evidence to verify the applicable P2PE requirements have been satisfied, then all firmware, cryptographic keys[1], configurations, and software must be reloaded into the PTS POI devices in accordance with applicable P2PE requirements.

1 - Note: *It is acceptable for the PTS POI devices to retain the necessary keying material to facilitate remote loading (including firmware loading and remote key injection.) If, however, there is any indication there has been a compromise of these keys or the firmware itself, the PTS POI devices must be sent back for reinitialization.*

3.2.3. *PTS POI Device Sampling Criteria*

The Program allows for the following regarding testing PCI-approved PTS POI devices as part of the validation effort to the P2PE Standard:

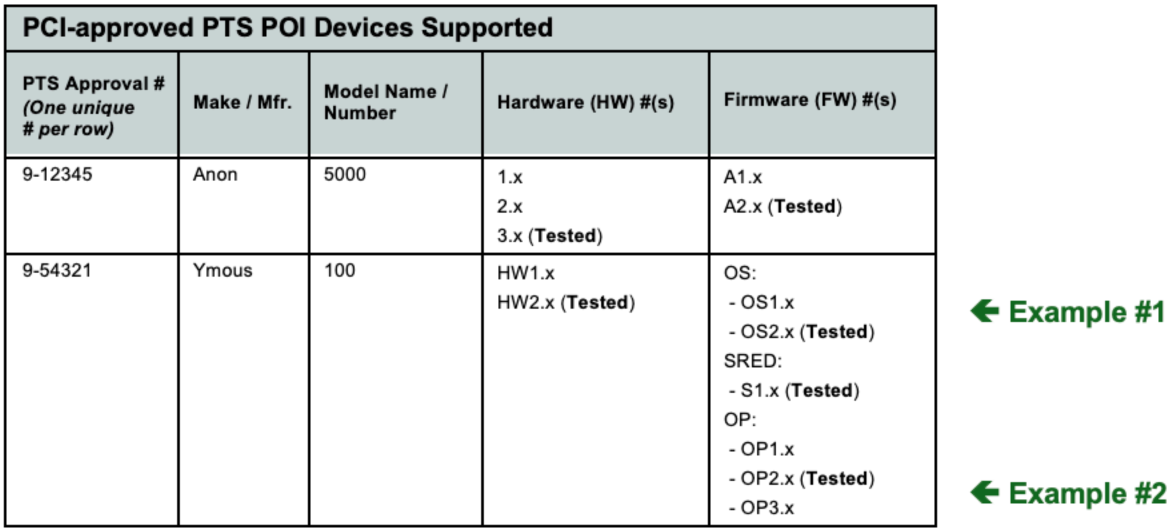
With respect to the PTS POI device hardware/firmware (HW/FW) combinations, at least one unique combination of PTS POI device HW and FW (Figure 3, Example #1 below) supported by the P2PE Product must be validated and functionally tested (as determined by the P2PE Standard requirements and associated testing procedures) from each PTS approval that is being associated with the P2PE Product assessment.

Where the FW is not monolithic (Figure 3, Example #2 below), i.e., it is split into separate FW functionality (e.g., OS, SRED, OP), every FW required for the device to function as intended must be validated and functionally tested (as determined by the P2PE Standard requirements and associated testing procedures).

The P2PE Assessor must document in the appropriate P-ROV, for each associated PTS approval, the supported PTS POI device HW/FW(s) combinations that were validated and functionally tested, in addition to all eligible HW and FW from the same PTS approval being supported by and intended to be listed for the P2PE Product. Note that all supported POI devices must be in accordance with the governing P2PE Standard requirements (e.g., 1A-1). When populating the POI device version information in the P-ROV, where the version tested is included in a wildcard version as shown in the PTS approval, document the wildcard version instead of the explicit version tested. E.g., if FW version 1.1 is tested, and the PTS approval denotes 1.x, then populate 1.x.

The P2PE Assessor is encouraged to determine if more combinations within a PTS Approval should be examined and tested based on their knowledge of the P2PE Product and the PTS POI devices.

Example P-ROV documentation extract (for illustrative purposes only):



PCI-approved PTS POI Devices Supported				
PTS Approval # ***(One unique # per row)***	**Make / Mfr.**	**Model Name / Number**	**Hardware (HW) #(s)**	**Firmware (FW) #(s)**
9-12345	Anon	5000	1.x 2.x 3.x (**Tested**)	A1.x A2.x (**Tested**)
9-54321	Ymous	100	HW1.x HW2.x (**Tested**)	OS: - OS1.x - OS2.x (**Tested**) SRED: - S1.x (**Tested**) OP: - OP1.x - OP2.x (**Tested**) - OP3.x

Example #1
Example #2

Figure 3: P-ROV Documentation Example for PCI-approved PTS POI Devices

3.3. Secure Cryptographic Devices

P2PE Products require the use of Secure Cryptographic Devices (SCDs). To assist in evaluating these device types, note the following:

Refer to information regarding SCDs in the P2PE Standard.

Obtaining and maintaining PCI PTS HSM or FIPS 140 device approval is the responsibility of the secure cryptographic device vendor. The P2PE Assessor Company will request evidence of device approvals being in place and current as part of performing a P2PE Assessment, where applicable.

A Listed (not Expired) P2PE Product may undergo a Reassessment **up to but not exceeding three years** past the expiry date of any PCI-listed HSMs **already included** in the corresponding Listed P2PE Product. 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) has the potential to be valid for three years, this will allow P2PE Product Vendors to continue to use the expired HSMs for up to a total of six years after any associated PCI PTS HSM listings have expired, depending on their reassessment date.

A table is included in the associated *P2PE Technical FAQs* on the Website that provides the current PCI PTS HSM expiry dates and the corresponding Reassessment window for Listed P2PE Products using these devices, along with additional relevant information regarding the use of HSMs.

For additional details, refer to Appendix I: Figure 9: PCI-Approved PTS HSM Expiry Flowchart.

3.3.1. NIST CMVP Historical Validation List

The following applies to the use of HSMs on NIST's 'CMVP Historical Validation List':

New Assessments: HSMs on the CMVP Historical Validation List can be used, however, the P2PE Assessor must determine the Historical Reason for the transition to the 'CMVP Historical Validation List' does not compromise the P2PE Product from satisfying applicable P2PE Standard requirements. This analysis must be documented in the appropriate P-ROV for requirements 4A-1.1 and 1-3, as applicable.

Annual Revalidations & Reassessments: P2PE Products can continue to use HSMs that are on the 'CMVP Historical Validation List' that were assessed as part of the P2PE Product's New Assessment, if all other requirements are met during the Annual Revalidation and Reassessment processes per the Program Requirements.

The P2PE Product vendor is encouraged to make a risk determination on whether to continue using the HSMs on the 'CMVP Historical Validation List' based on their own assessment of where and how the HSM is used within the P2PE Product.

3.4. P2PE Applications

P2PE Solutions generally include P2PE Applications installed on the PCI-approved PTS POI devices. To assist in evaluating P2PE Applications, note the following:

- Refer to the definition of P2PE Application in the *P2PE Glossary*.
- Refer to the information regarding P2PE Applications in the *P2PE Standard*.
- Must undergo validation per all applicable P2PE Application Requirements by a P2PE Application Assessor Company, with the option to be:
  - Independently Listed on the List of Validated P2PE Applications

    OR,

- A Solution-specific P2PE Application, which is not Listed on the List of Validated P2PE Applications and therefore only considered an element of the specific Validated P2PE Solution for which it has been submitted. While a P2PE Solution and a P2PE Component can be assessed by either a P2PE Assessor Company or a P2PE Application Assessor Company, only a P2PE Application Assessor Company can assess and validate a P2PE Application.

- For P2PE Solution Assessments, if a P2PE Application is not already on the List of Validated P2PE Applications, both the P2PE Solution P-ROV (including P2PE Component P-ROVs, if applicable) and the P2PE Application P-ROV(s) (one for each P2PE Application), must be submitted to PCI SSC. The P2PE Application P-ROV(s) must undergo PCI SSC review (and Acceptance, where the P2PE Application is being submitted to be Listed on the List of Validated P2PE Applications) **prior** to PCI SSC review and Acceptance of the P2PE Solution. This applies for **each** P2PE Solution in which the P2PE Application(s) is used.
- For applicable P2PE Component Assessments, if a P2PE Application is not already on the List of Validated P2PE Applications, both the applicable P2PE Component P-ROV and the P2PE Application P-ROV(s), (**one for each P2PE Application**), must be submitted to PCI SSC. The P2PE Application P-ROV(s) must undergo PCI SSC review (and Acceptance, where the P2PE Application is being submitted to be Listed on the List of Validated P2PE Applications) **prior** to PCI SSC review and Acceptance of the P2PE Component. This applies for **each** P2PE Component in which the P2PE Application(s) is used.

3.5. P2PE Non-payment Software

P2PE Solutions can include P2PE Non-payment Software on the PCI-approved PTS POI devices. To assist in evaluating P2PE Non-payment Software, note the following:

- Refer to the definition of P2PE Non-payment Software in the P2PE Glossary.
- P2PE Non-payment Software is not a P2PE Application.
- Refer to information regarding P2PE Non-payment Software in the P2PE Standard.
- Can be assessed by a P2PE Assessor Company *that is not additionally qualified* as a P2PE Application Assessor Company.
- Not eligible to be Listed by PCI SSC.

3.6. P2PE Components

Acceptance and subsequent inclusion of Third-Party Service Provider component services on the List of Validated P2PE Components 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/or P2PE Components without the need for a Full Assessment of those services each time they are used with a different P2PE Solution and/or P2PE Component.

For P2PE Solution Assessments or P2PE Component Assessments (that use another P2PE Component):

- If a P2PE Component is currently listed on the List of Validated P2PE Components, the applicable P2PE Component P-ROV has already been Accepted by PCI SSC. As a result, any Listed P2PE Components included in a P2PE Solution or P2PE Component Assessment only need to be identified in the P2PE Solution P-ROV or the applicable P2PE Component P-ROV, respectively, and an assessment of that already-Listed P2PE Component is not required as part of the P2PE Solution or P2PE Component Assessment submission.
- If a P2PE Component that is included in a P2PE Solution or applicable P2PE Component Assessment is not already on the List of Validated P2PE Components but is being submitted to PCI SSC for

Acceptance and Listing on the List of Validated P2PE Components, the applicable P2PE Component P-ROV must be submitted to PCI SSC for review and Accepted **before** the P-ROVs of the P2PE Solution or applicable P2PE Component Assessment in which it is included 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.

3.7. Remote Assessments

P2PE Assessors are expected to perform onsite assessments for P2PE Products, where applicable. While onsite assessments continue to be the expected method for PCI SSC assessments, the use of remote assessment methods may provide a suitable alternative in legitimate scenarios where an onsite assessment is not feasible. Refer to the *PCI SSC Remote Assessments Guidelines and Procedures* for details of remote assessment procedures and methods that may be used when an onsite assessment cannot be performed.

If remote assessment methods are used in place of an onsite assessment, the P2PE Assessor must complete the Addendum for ROC/ROV: Remote Assessments, as provided in Appendix A of the *PCI SSC Remote Assessment Guidelines and Procedures* document, for submission to PCI SSC along with the applicable P-ROV(s).

3.8. New Assessments and Reassessments using Expired P2PE Products

New Assessments and Reassessments of P2PE Products will not be Accepted if they use Expired P2PE Products. If at any time prior to Acceptance of the submission, including during the PCI SSC AQM review process, a P2PE Product dependency is expired or expires, the P2PE Product submission will be rejected. If a Component or Application is not on the List of Validated P2PE Components or the List of Validated P2PE Applications, respectively, then it must undergo a Full Assessment as part of the assessment and submission process.

3.9. Listed P2PE Products with Expired P2PE Product Dependencies

During the 3-year lifecycle of a Listed P2PE Product, underlying Listed P2PE Product dependencies (P2PE Components and/or P2PE Applications) denoted within the details of that P2PE Product might Expire (e.g., a Listed P2PE Solution using a Listed KIF, where the KIF Expires and moves to the Expired List).

An Expired P2PE Product dependency is not automatically removed from the details of the Listed P2PE Product. The parent Listed P2PE Product will include an indication that it is using a dependency that is not in accordance with applicable P2PE Program Requirements. The Expired P2PE Product dependency will be denoted as being Expired in the details of the parent Listed P2PE Product.

However, as P2PE Products on the P2PE Expired Listings are no longer considered validated, the P2PE Product Vendor is encouraged to promptly remediate any Expired dependencies.

Options for remediating the existence of an Expired dependency will vary depending on the specific P2PE Products involved. These options may include, but are not limited to, one or more of the following:

- Discontinuing the use of the Expired dependency and removing it from the Validated P2PE Product's Listing.
- Replacing the expired dependency with a commensurate Validated P2PE Product.
- Undergo a P2PE Assessment to validate the applicable P2PE Program Requirements previously satisfied using the now-expired P2PE Product dependency.

P2PE Product Vendors are encouraged to consult with a P2PE Assessor Company to determine the appropriate course of action for your unique situation.

4. Overview of the Validation Processes

The following sections provide a general overview of the validation processes for P2PE Products.

4.1. 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.

Notes:

Refer to Section 4.2 for information regarding validation of Merchant-managed Solutions (MMS).

Refer to Section 2.1.4 to understand options for validating Third-Party Service Providers.

P2PE Application Assessments may only be performed by P2PE Application Assessor Companies.

1) The P2PE Vendor selects a P2PE Assessor Company from PCI SSC's list of PCI Point-to-Point Encryption (P2PE)® Assessors on the Website and negotiates the cost and other terms of the assessor engagement directly 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 Product to be assessed, PTS 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 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 Product, including its security functions and features, using the appropriate *P-ROV(s),* to determine whether it complies with the P2PE Standard and Program Requirements.

4) If the P2PE Assessor Company determines that the P2PE Product is in compliance with the P2PE Standard and Program Requirements, the P2PE Assessor Company submits the corresponding *P-ROV(s)* to PCI SSC, attesting to compliance and setting forth the results and observations of the P2PE Assessor Company on all test procedures, along with the P2PE Vendor's signed *VRA* and the corresponding *P-AOV*. Refer to Appendix A for more details on Acceptance.

5) PCI SSC issues an invoice to the P2PE Vendor for the applicable P2PE submission fee (Refer to the 'Programs Fee Schedule' on the Website). After the P2PE Vendor has paid the invoice, PCI SSC reviews the submission to confirm that it satisfies the P2PE Program Requirements and if confirmed, PCI SSC notifies the P2PE Assessor Company and P2PE Vendor that the P2PE Product submission is Accepted as a Validated P2PE Product.

6) Once the above process is complete for the submitted P2PE Product, PCI SSC signs the corresponding P-AOV and adds the P2PE Product to the corresponding List of Validated P2PE Products on the Website.

The diagrams on the following pages explain in further detail the processes for the P2PE Program:

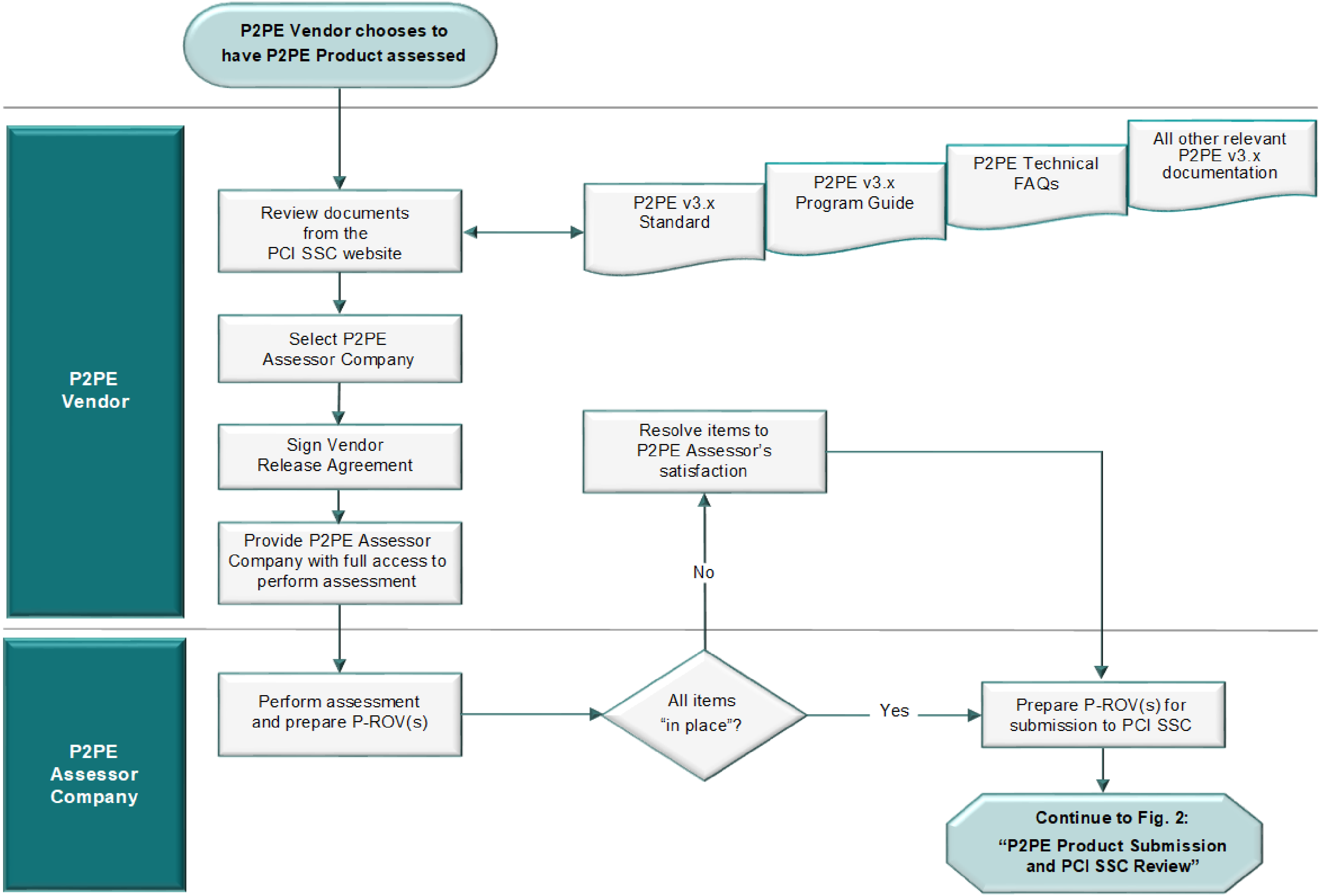

P2PE Vendor chooses to have P2PE Product assessed
P2PE Vendor
Review documents from the PCI SSC website
P2PE v3.x Standard
P2PE v3.x Program Guide
P2PE Technical FAQs
All other relevant P2PE v3.x documentation
Select P2PE Assessor Company
Sign Vendor Release Agreement
Resolve items to P2PE Assessor's satisfaction
Provide P2PE Assessor Company with full access to perform assessment
No
P2PE Assessor Company
Perform assessment and prepare P-ROV(s)
All items "in place"?
Yes
Prepare P-ROV(s) for submission to PCI SSC
Continue to Fig. 2: "P2PE Product Submission and PCI SSC Review"

Figure 4: P2PE Product Validation Overview

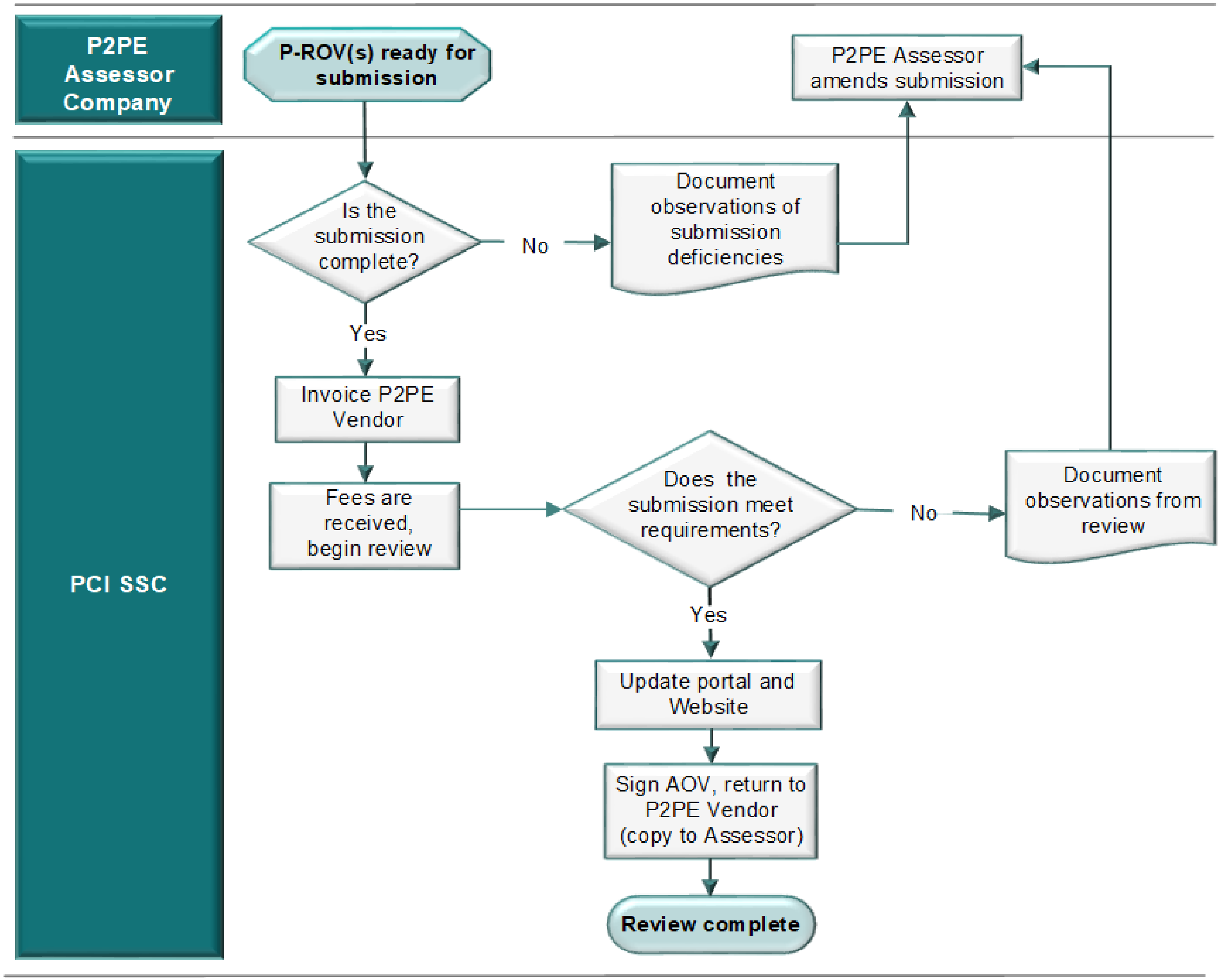

P2PE Assessor Company
P-ROV(s) ready for submission
P2PE Assessor amends submission
PCI SSC
Is the submission complete?
No
Document observations of submission deficiencies
Yes
Invoice P2PE Vendor
Fees are received, begin review
Does the submission meet requirements?
No
Document observations from review
Yes
Update portal and Website
Sign AOV, return to P2PE Vendor (copy to Assessor)
Review complete

Figure 5: P2PE Product Submission and PCI SSC Review

4.2. Overview of Validation Processes for Merchant-Managed P2PE Solutions

Notes:

Merchant-Managed Solution (MMS) assessments are not submitted to PCI SSC and are not eligible to be Listed on the Website. A Merchant-Managed P2PE Solution may utilize Third-Party Service Providers, Listed P2PE Applications, and/or Listed P2PE Components. There are MMS-specific P-ROVs and P-AOVs on the Website.

Refer to Section 2.1.4 to understand options for validating Third-Party Service Providers.

P2PE Application Assessments may only be performed by P2PE Application Assessor Companies.

The P2PE Assessment process for P2PE Solutions 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 PCI SSC's list of PCI Point-to-Point Encryption (P2PE)® Assessors on the Website and negotiates the cost and other terms of the assessor engagement directly with the P2PE Assessor Company.
2) The merchant provides the P2PE Assessor Company access to the MMS to be assessed, PCI-approved PTS POI Device Types, corresponding *Implementation Guides* for P2PE Applications*,* *P2PE Instruction Manual* for the 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 is in accordance with the P2PE Standard and Program Requirements.
4) If the P2PE Assessor Company determines that the MMS is in accordance with the P2PE Standard and Program Requirements, the P2PE Assessor Company prepares and submits to the merchant a corresponding P2PE Merchant-Managed Solution P-ROV (and all additional P-ROVs as required for the P2PE Assessment) attesting to compliance and setting forth the results and observations of the P2PE Assessor Company on all test procedures.
5) The merchant and the P2PE Assessor Company complete and sign the applicable MMS P-AOV.

4.3. Prior to P2PE Product Validation

Note: *The security requirements applicable to P2PE Products and the test procedures for validating P2PE Products are 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 the P2PE Standard and all related documentation located at the Website, including the *P2PE Technical FAQs*.
- Determine/assess the applicable P2PE Product's readiness to satisfy the P2PE Standard and Program Requirements: Select the appropriate P-ROV(s) based on the type of P2PE Product assessment. Refer to Table 2: P-ROV Templates.

- For P2PE Application assessments, determine whether the P2PE Application Vendor's *Implementation Guide* meets P2PE Standard requirements and correct any gaps.
- For P2PE Solution Assessments, determine whether the P2PE Solution Provider's *P2PE Instruction Manual (PIM)* meets P2PE Standard requirements and correct any gaps.

4.4. P2PE Product Validation Required Documentation

The P2PE Vendor and P2PE Assessor work together to account for all P2PE Assessment-related materials (such as, but not limited to, *P-ROVs*, *P-AOV*, the *P2PE Instruction Manual (PIM)*, *P2PE Application Implementation Guide (IG)*, the *Vendor Release Agreement (VRA),* and all other materials related to the P2PE Product assessment and participation in the P2PE Program). The P2PE Vendor does not submit any documentation directly to PCI SSC as part of a P2PE Assessment.

4.5. P2PE Product Validation Review Timeframes

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

- The degree that the P2PE Product satisfies the P2PE Standard and Program Requirements at the start of the P2PE Assessment:

  Corrections to the P2PE Product to remediate gaps will delay validation.

- Prompt payment of the P2PE Program fees due to PCI SSC for the P2PE Product submission.

  PCI SSC will not commence review of the P-ROV(s) for the P2PE Products until the applicable fee has been paid.

- 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 or the P2PE Component can be reviewed and Accepted.

- The scope of the P2PE Product assessment and validation effort. The use of Listed P2PE Components and/or Listed P2PE Applications can reduce the scope.

  The greater the scope of the P2PE Product assessment, which usually requires additional P-ROVs to be used, will increase the review time of the P2PE Product submission.

- Whether the P2PE Application's *Implementation Guide* and/or the P2PE Solution's *P2PE Instruction Manual* meets all P2PE Standard requirements at the start of the assessment:

  Extensive rewrites will delay validation.

- 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 satisfy all P2PE Standard and Program Requirements quickly. If issues 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 the review timeline and cause delays and/or cause the review to end prematurely (for example, if the P2PE Vendor decides it does not want to remediate identified issues).

4.6. P2PE Assessor Information

Notes:

By definition, a P2PE Application Assessor Company is also a P2PE Assessor Company.

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.

PCI SSC qualifies and provides required training for P2PE Assessor Companies and P2PE Application Assessor Companies to assess and validate P2PE Products to the P2PE Standard and Program Requirements.

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 or QPA Qualification Requirements* and *P2PE Qualification Requirements*, as applicable) or in remediation as both a QSA or QPA Company and P2PE Assessor Company.

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 or QPA Qualification Requirements* and *P2PE Qualification Requirements*, as applicable) or in remediation as both a P2PE Assessor Company and a P2PE Application Assessor 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 Product assessments.

- For each P2PE Product assessment, the corresponding *P-ROVs* for that assessment must be utilized and completed. Refer to Table 2: P-ROV Templates.
- The P2PE Assessor Company must prepare each *P-ROV* based on evidence obtained by following the P2PE Standard and Program Requirements.
- 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 P2PE Product (including all applicable *P-ROVs*) submitted to PCI SSC for Acceptance and Listing must be accompanied by a corresponding *P2PE Attestation on Validation* (*P-AOV*) available on the Website.

4.6.1. 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 PCI Point-to-Point Encryption (P2PE)® Assessors on the Website, talk to several P2PE Assessor Companies, and follow its own vendor-selection processes.

4.7. 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 Product 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.

4.8. Vendor Release Agreement (VRA)

For PCI SSC to review any submission, PCI SSC must have on file the P2PE Vendor's signed copy of the then-current version of the *Vendor Release Agreement (VRA)* available on the Website.

- If PCI SSC **does not** have a copy of the P2PE Vendor's signed, then-current *VRA* on file, the P2PE Assessor Company must provide such *VRA* to PCI SSC.
- If PCI SSC **does** have a copy of the P2PE Vendor's signed, then-current VRA on file, the P2PE Assessor Company is not required to re-submit the same *VRA* to PCI SSC at that time.

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.

The VRA, in part:

- Covers confidentiality issues;
- Covers the P2PE Vendor's agreement to P2PE Program Requirements, policies, and procedures;
- Gives permission to the P2PE Vendor's chosen 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.

4.9. The Portal

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

The Portal is also used by PCI SSC to track all communications relating to a submission.

5. Changes to Listed P2PE Products

P2PE Vendors may need to update their Listed P2PE Products for various reasons. The *Change Impact Template* must be used to account for and submit Administrative Changes and Delta Changes to PCI SSC.

Notes:

Changes are permissible only for Listed (not Expired) P2PE Products.

Any change to a Listed P2PE Product that is not an Administrative Change and not a Delta Change is accounted for by the P2PE Vendor as part of the Annual Revalidation process for the Listed P2PE Product. Refer to section 6.1 Annual Revalidation of Listed P2PE Products for further details.

Administrative Changes and Delta Changes do not have any impact on Annual Revalidation dates or Reassessment dates of Listed P2PE Products.

5.1. Administrative Changes to Listed P2PE Products

***Note:** The Change Impact Template on the Website must be used for Administrative Changes.*

An Administrative Change is used to update the following information on a Listed P2PE Product:

- P2PE Vendor Company Name (requires an updated *VRA*)
- P2PE Product Name (including Solution-specific P2PE Applications)

5.1.1. Administrative Change Submission Process Overview

1) The P2PE Vendor and the P2PE Assessor Company prepare and complete the *Change Impact Template* and corresponding *P-AOV*;
2) If the Administrative Change requires an updated VRA, the P2PE Vendor completes the then-current VRA and submits this to the P2PE Assessor Company;
3) The P2PE Assessor Company submits the Administrative Change (and then-current VRA, if applicable) to PCI SSC through the Portal;
4) PCI SSC will then issue an invoice to the P2PE Vendor for the applicable change fee; and
5) Upon payment of the invoice, PCI SSC will review the Administrative Change submission.

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

1) Amend the Listed P2PE Product details on the corresponding List of Validated P2PE Products on the Website accordingly based on the Administrative Change submission; and
2) Sign and return a copy of the corresponding *P-AOV* to both the P2PE Vendor and the P2PE Assessor Company. An Administrative Change does not change the Listed P2PE Product's Annual Revalidation date or its Reassessment date.

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 submission if it determines that a change described therein and purported to be an Administrative Change by the P2PE Assessor Company and/or P2PE Vendor is ineligible for an Administrative Change.

5.2. Delta Changes to Listed P2PE Products

Notes:

The assessment of Delta Changes to a Listed P2PE Product must be performed using the ***same major version*** *of the P2PE Standard as the Full Assessment.*

Delta Change submissions to add Expired P2PE Products will not be Accepted. If at any time prior to Acceptance of the Delta Change submission, including during the PCI SSC AQM review process, a P2PE Product being added as part of the Delta Change is expired or expires, the Delta Change submission will be rejected. Delta Changes to add P2PE Components/Applications to an existing Listed P2PE Solution or Listed P2PE Component without further assessment requires the P2PE Component/Application being added to be on the List of Validated P2PE Components or the List of Validated P2PE Applications, respectively.

The Change Impact Template on the Website must be used for Delta Changes.

Delta Changes are security-impacting changes (not Administrative Changes) made to a Listed P2PE Product as defined and accounted for in the *Change Impact Template* that affect a Listing element as defined in Appendix B, Appendix C, and Appendix D. Generally, Delta Changes include, but are not limited to, the following:

- Add/remove a PCI-approved PTS POI Device Type;
- Add/remove a PCI-approved and/or FIPS-validated HSM;
- Add/remove a P2PE Application;
- Add/remove a P2PE Component;
- Address P2PE Application changes

Note: *Delta Changes cannot be used to perform partial assessments of new applications.*

5.2.1. Delta Change Submission Process Overview

The P2PE Vendor and P2PE Assessor Company prepare and complete the *Change Impact Template.* It is recommended that the P2PE Vendor submit the Delta Change request to the same P2PE Assessor Company used for the last Full Assessment of the Listed P2PE Product.

If the P2PE Assessor Company agrees that the change as documented and conveyed by the P2PE Vendor is eligible as a Delta Change under the Program:

1) The P2PE Assessor Company notifies the P2PE Vendor that it agrees;
2) As required, the P2PE Vendor completes a new *VRA* and submits this to the P2PE Assessor Company;
3) The P2PE Assessor Company satisfies and completes the *Change Impact Template* for the Listed P2PE Product, including all required [re]testing and validation;
4) The P2PE Assessor Company provides redlined *P-ROV(s)* as instructed in and required by the *Change Impact Template*;
5) The P2PE Vendor prepares and signs the corresponding *P-AOV* and sends it to the P2PE Assessor Company;
6) The P2PE Assessor Company signs its concurrence on the *P-AOV* and submits it along with the completed *Change Impact Template* and all required documentation 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 eligibility, quality assurance purposes, and consistency.

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

1) Amend the Listed P2PE Product details on the corresponding List of Validated P2PE Products on the Website accordingly based on the Delta Change submission; and

2) Sign and return a copy of the corresponding *P-AOV* to both the P2PE Vendor and the P2PE Assessor Company. A Delta Change does not change the Listed P2PE Product's Annual Revalidation date or its Reassessment date.

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 Change Impact submission if it determines that a change described therein and purported to be a Delta Change by the P2PE Assessor Company and/or P2PE Vendor is ineligible for a Delta Change.

5.2.2. P2PE Application Changes and Version Numbers

All P2PE Application changes must result in a new application version number; however, whether this affects the version number specified within the P2PE Product Listing on the Website depends on the nature of the change and the Vendor's validated versioning methodology. The use of wildcards may be permitted for managing the versioning methodology for non-security-impacting 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 Standard requirement, is prohibited.*

Only those P2PE Applications that have had the P2PE Vendor's wildcard versioning methodology validated to P2PE v3.x by a P2PE Application Assessor Company are eligible for wildcard usage and inclusion on the Website with wildcards.

Changes falling within the scope of wildcard usage are not required to be reported to PCI SSC; therefore, any such changes will not result in an update to the P2PE Application Listing on the Website. Refer to Appendix E for additional information regarding the use of wildcards.

6. Lifecycle for Listed P2PE Products

A Listed P2PE Product, upon Acceptance and being Listed as the result of a Full Assessment, remains Validated for 3 years based on the date of the most recent Acceptance, provided it satisfies the Program Requirements as described herein.

Once Listed, a P2PE Product is required to satisfy the Annual Revalidation process at year 1 and year 2 based on the date of the most recent Acceptance.

At the end of the 3-year lifecycle, P2PE Vendors have the option of undergoing a Reassessment as described herein to renew the Listing for their P2PE Product.

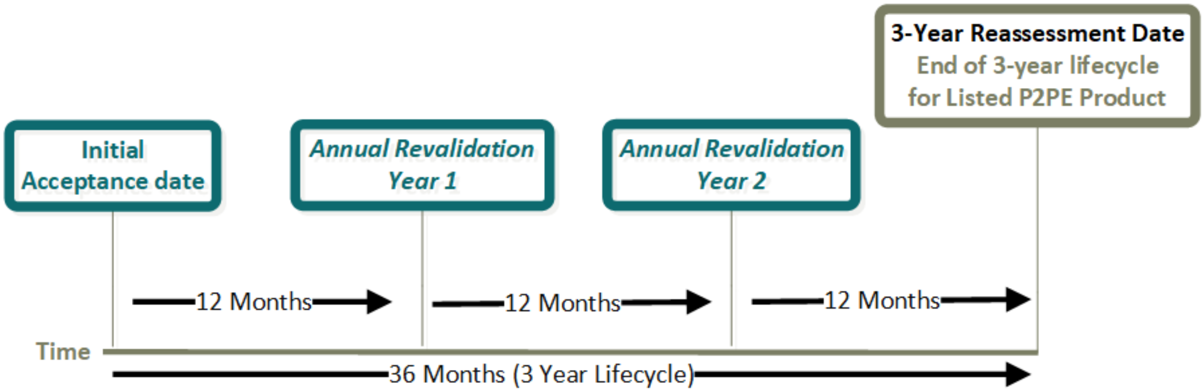


Figure 6: Listed P2PE Product 3-Year Lifecycle

6.1. Annual Revalidation of Listed P2PE Products

The Annual Revalidation process requires the P2PE Vendor to attest to and account for their Listed P2PE Product continuing to adhere to the P2PE Standard and Program Requirements via their submittal of the appropriate *P-AOV*.

The first Annual Revalidation is required one calendar year after the most recent date of Acceptance based on the last Full Assessment, and the second Annual Revalidation is required one calendar year after the first Annual Revalidation date, provided the P2PE Vendor satisfies all applicable Program Requirements for the first Annual Revalidation.

PCI SSC will send a courtesy reminder e-mail notification to the P2PE Vendor’s contact (as identified in the applicable *P-AOV*) within 90 calendar days prior to the relevant Annual Revalidation date, however 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 submit the applicable *P-AOV* to the PCI SSC P2PE Program Manager and confirm, in part, that:

a) Changes have been applied to the Listed P2PE Product in a way that is consistent with the P2PE Standard and Program Requirements;

b) The Listed P2PE Product continues to meet the requirements of the P2PE Standard and Program Requirements;

***Note**: The P2PE Vendor is required to consider the impact of external threats and whether updates to the Listed P2PE Product are necessary to address changes to the external threat environment.*

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

If an updated *P-AOV* is not submitted and Accepted by PCI SSC on or before the Listed P2PE Product's current Annual Revalidation Date, the P2PE Product will be subject to Administrative Expiry, as follows:

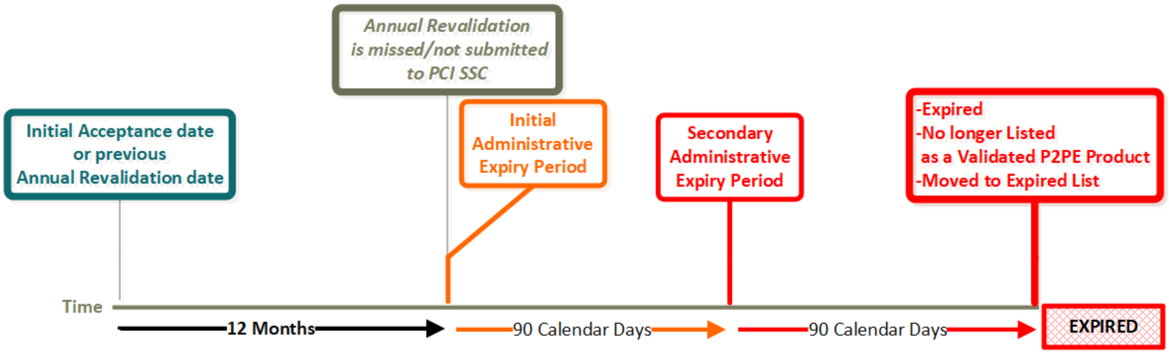

Annual Revalidation is missed/not submitted to PCI SSC
Initial Acceptance date or previous Annual Revalidation date
Initial Administrative Expiry Period
Secondary Administrative Expiry Period
-Expired
-No longer Listed as a Validated P2PE Product
-Moved to Expired List
Time
12 Months
90 Calendar Days
90 Calendar Days
EXPIRED

Figure 7: Administrative Expiry

6.1.1. Initial Administrative Expiry Period

- The corresponding P2PE Product Listing will be updated to show the P2PE Product's Annual Revalidation date in **Orange** for a period up to 90 consecutive calendar days unless the Annual Revalidation requirements of the Program are satisfied.
- If the updated and complete *P-AOV* is received by PCI SSC within this initial 90-day period, PCI SSC will, upon Acceptance, remove the **Orange** status from the P2PE Product Listing.

6.1.2. Secondary Administrative Expiry Period

- If the updated and complete *P-AOV* is not received and Accepted by PCI SSC within the 90-day initial Administrative Expiry period, the corresponding P2PE Product Listing will be updated to show the P2PE Product's Annual Revalidation date in **Red** for a period up to 90 consecutive calendar days.
- Once a Listed P2PE Product is in this secondary Administrative Expiry period (**Red)**, a Full Assessment (including applicable Program fees) is required to relist the P2PE Product and avoid Expiry.
- If a Full Assessment is conducted, submitted to and Accepted by PCI SSC, before the P2PE Product Expires, the submission will qualify as a Reassessment as described herein. Otherwise, once Expired, any Full Assessment submission of the P2PE Product to PCI SSC will be considered a New Assessment.

6.1.3. Administrative Expiry

- If a P2PE Product's Listing has been in a **Red** status for more than 90 consecutive calendar days (over 180 days overdue in satisfying the Annual Revalidation requirements of the Program), it becomes an Expired P2PE Product, is no longer considered a Validated P2PE Product, and will be moved to the P2PE Expired Listings.

6.2. Reassessment of Listed P2PE Products

A Listed P2PE Product is eligible for Reassessment provided all applicable Program Requirements have been satisfied. A Reassessment is a Full Assessment of a Listed P2PE Product that is submitted to and Accepted by PCI SSC before the Listed P2PE Product Expires.

As a Listed P2PE Product approaches its 3-year Reassessment date, PCI SSC will provide a courtesy notification to the P2PE Vendor via email notification of the pending expiration. However, it is the sole responsibility of the P2PE Vendor to initiate a Reassessment of their P2PE Product regardless of any such courtesy reminder(s). The P2PE Vendor can choose to perform a Reassessment, otherwise, the P2PE Product will become an Expired P2PE Product and move to the P2PE Expired Listings as described below.

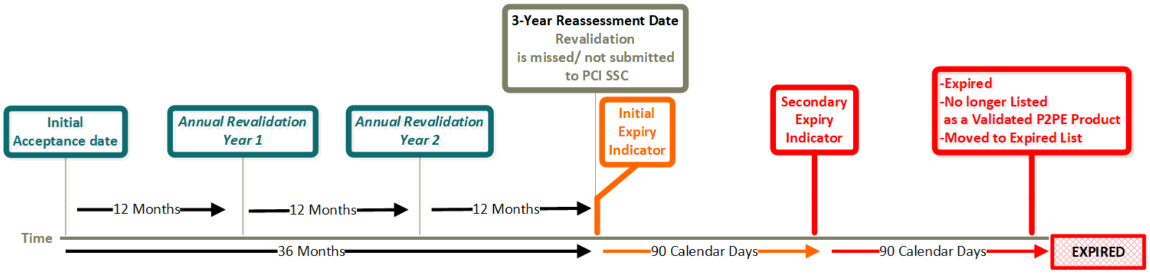


Figure 8: Reassessment Timeline & Listing Expiry

6.2.1. Listing Expiry

A Listed P2PE Product for which a new Acceptance based on a Full Assessment has not occurred on or before the Listed P2PE Product's applicable Reassessment date will immediately appear in **Orange** for up to 90 consecutive calendar days, and in **Red** thereafter for up to 90 additional consecutive calendar days.

If a new Acceptance has not occurred within 180 consecutive calendar days following the Listed P2PE Product's applicable Reassessment date, the P2PE Product will become an Expired P2PE Product and be moved to the P2PE Expired Listings. Expired P2PE Products are no longer considered Validated P2PE Products. Any assessment of an Expired P2PE Product is considered a New Assessment.

7. Program Fees

Program Fees are denoted in the Programs Fee Schedule on the Website. Program fees are non-refundable and are subject to change upon posting of revised fees on the Website.

PCI SSC will invoice the P2PE Vendor for all associated Program Fees for a submission and the P2PE Vendor is required to pay these fees directly to PCI SSC.

Program fees must be received by PCI SSC for a submission to be reviewed and Accepted (provided the submission satisfies the P2PE Standard and Program Requirements). 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 a Program 'late' fee associated with the processing of P-AOVs received as part of the Annual Revalidation process for a Listed P2PE Product if the P-AOV is not received by PCI SSC on or before the respective Annual Revalidation date for the Listed P2PE Product.

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

8. Security Issue Notifications

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.

8.1. 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.

8.2. 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 SSC P2PE Program Manager at P2PE@pcisecuritystandards.org.

8.3. Notification Details

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

- The name, PCI SSC approval (Reference) 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.

8.4. 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

8.5. 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 Products) 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.

Appendix A. P2PE Products and Acceptance

Acceptance of a given P2PE Product by PCI SSC only applies to the specific P2PE Product validated by a P2PE Assessor Company qualified to assess the specific P2PE Product, and subsequently Accepted by PCI SSC (the "Accepted Product"). Only a P2PE Assessor Company additionally qualified as a P2PE Application Assessor Company may perform P2PE Application Assessments – regardless of if the P2PE Application being assessed is intended to be Listed on the List of Validated P2PE Applications or is not intended to be Listed and is only being validated and submitted as part of an overall P2PE Solution Assessment. If any aspect of a P2PE Product is different from that which was validated by the P2PE Assessor Company qualified to assess the specific P2PE Product, and Accepted by PCI SSC — even if the different P2PE Product (the "Alternate Product") conforms to the basic product description of the Accepted P2PE 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 Vendor or the functionality, quality, or performance of the Validated 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

P2PE Vendor Company Name (link to company website)

The P2PE Solution Provider for the P2PE Solution.

P2PE Solution Information

The following fields in the Listing provide relevant information for each Validated P2PE Solution, consisting of the following:

- **P2PE Solution Name**

  The P2PE Solution Name is provided by the P2PE Solution Provider and is the name by which the P2PE Solution is known.

- **POI Device Key Loading Supported**

  Denotes Local Key Injection and/or Remote Key Distribution being supported by the P2PE Product as determined and validated as part of the P2PE Product Assessment. The "Remote Key" distribution requirements are additional requirements that apply to any entity implementing remote key distribution using asymmetric techniques for the distribution of keys to PCI-approved PTS POI devices for use in connection with account-data encryption.

- **Key Types Supported**

  Denotes Symmetric and/or Asymmetric key types being supported as a result of the assessment and validation of the P2PE Product. The requisite set of requirements in the P2PE Standard must be satisfied to denote a key type. At least one key type must be supported.

- **Reference Number**

  PCI SSC assigns the Reference Number once the Validated P2PE Solution is Accepted, which uniquely identifies the Listed P2PE Solution.

  Note: *A Listed P2PE Solution that undergoes a Reassessment that is subsequently Accepted and Listed results in a new Reference Number.*

  An example reference number format is 2024-xxxxx.yyy consisting of the following, in order:

Field	Format
Year of Listing	4 digits + hyphen
P2PE Solution Provider Identifier	5 digits + period This value uniquely identifies the P2PE Solution Provider.
P2PE Solution Identifier	3 digits This value uniquely identifies the P2PE Solution of the P2PE Solution Provider.

- **P2PE Solution Details**

  Details specific to the P2PE Solution consisting of underlying dependencies that include the following:

  - **P2PE Components Supported**

This section identifies the P2PE Components validated for use with the P2PE Solution including the Reassessment Date of the P2PE Component.

While a P2PE Solution may include third-party services (including services potentially eligible for being Listed as a P2PE Component) those third-party services are not identified within the P2PE Solution's Listing or on the List of Validated P2PE Components. Any use of such a service in another P2PE Product would require either an independent Listing as a P2PE Component, if eligible, or an assessment as part of each P2PE Product where the third-party services are used.

– **P2PE Applications Supported**

This section identifies the P2PE Applications validated for use with the P2PE Solution, including the P2PE Application's Reassessment date.

Note: *A P2PE Solution may include P2PE Applications that were validated as part of the Solution assessment that are not separately Listed on the List of Validated P2PE Applications (referred to as a 'Solution-specific P2PE Application').*

P2PE Applications in this case are denoted on the P2PE Solution Listing, however they do not have an associated Reference Number or an independent Reassessment Date. The P2PE Application name and its validated version(s) will be displayed under the associated P2PE Solution. These types of P2PE Applications are only validated for use in the P2PE Solution for which it is listed under and are denoted as such. Any use of such an application in another P2PE Product would require either independent listing as a Listed P2PE Application, if eligible, or an assessment as part of each P2PE Product the application is used in.

– **PCI-Approved PTS POI Devices Supported**

This section identifies PCI-approved PTS POI devices, including the PTS POI device hardware and firmware versions, validated for use with the P2PE Solution and will include the relevant PCI PTS reference numbers and expiry dates of the PCI PTS approval. A website link to the associated PTS Approval on the PCI List of Approved PIN Transaction Security (PTS) Devices is included for each device supported.

– **PCI-approved PTS HSMs Supported**

This section identifies PCI-approved PTS HSM devices validated for use with the P2PE Solution and will include the relevant PCI PTS reference numbers and expiry dates of the PCI PTS approval. A website link to the associated PTS Approval on the PCI List of Approved PIN Transaction Security (PTS) Devices is included for each device supported.

– **FIPS 140 Validated HSMs Supported**

This section identifies FIPS 140 validated HSMs for use with this P2PE Solution, including the *NIST Cryptographic Module Validation Program (CMVP)* certificate number and sunset date. A website link will be provided to the appropriate entry in the *NIST CMVP database of validated cryptographic modules*.

P2PE Standard Version

The version of the P2PE Standard used to validate the P2PE Solution.

P2PE Assessor Company

The qualified P2PE Assessor Company that performed the validation and determined that the P2PE Solution is in accordance with the P2PE Standard and Program Requirements.

Annual Revalidation Date

The date by which the P2PE Solution Provider must satisfy the Annual Revalidation process, which occurs at the 12- and 24-month mark from the last date of Acceptance based on a Full Assessment.

Reassessment Date

The 3-year date from the last date of Acceptance based on a Full Assessment by which time the P2PE Solution Provider can choose to undergo and submit another Full Assessment of the P2PE Solution to the P2PE Standard and Program Requirements to, provided Acceptance occurs, maintain their Listing.

Appendix C. Elements for the List of Validated P2PE Components

P2PE Vendor Company Name (link to company website)

The P2PE Component Provider for the P2PE Component.

P2PE Component Information

The following fields in the Listing provide relevant information for each Validated P2PE Component, consisting of the following:

- **P2PE Component Name**

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

- **POI Device Key Loading Supported**

  Denotes Local Key Injection and/or Remote Key Distribution being supported by the P2PE Product as determined and validated as part of the P2PE Product Assessment. The "Remote Key" distribution requirements are additional requirements that apply to any entity implementing remote key distribution using asymmetric techniques for the distribution of keys to PCI-approved PTS POI devices for use in connection with account-data encryption.

- **Key Types Supported**

  Denotes Symmetric and/or Asymmetric key types being supported as a result of the assessment and validation of the P2PE Product. The requisite set of requirements in the P2PE Standard must be satisfied to denote a key type. At least one key type must be supported.

- **Reference Number**

  PCI SSC assigns the Reference Number once the Validated P2PE Component is Accepted, which uniquely identifies the Listed P2PE Component.

  Note: *A Listed P2PE Component that undergoes a Reassessment to the same major version of the P2PE Standard that is subsequently Accepted and Listed will retain the existing Reference Number.*

  A Listed P2PE Component that undergoes a Reassessment to a new major version of the P2PE Standard that is subsequently Accepted and Listed will result in an updated (new) Reference Number.

  An example reference number format is 2024-xxxxx.yyy consisting of the following, in order:

Field	Format
Year of Listing	4 digits + hyphen
P2PE Component Provider Identifier	5 digits + period This value uniquely identifies the P2PE Component Provider
P2PE Component Identifier	3 digits This value uniquely identifies the P2PE Component of the P2PE Component Provider

- **P2PE Component Details**

  Details specific to the P2PE Component consisting of underlying dependencies that include the following:

  ***Note:** Not all component detail categories will apply to every P2PE Component type. For example, Decryption Environments do not have associated P2PE Applications.*

  - **P2PE Components Supported**

    ***Note:** Certain Component Types can outsource to other predefined Listed Component types. Refer to the Outsourcing Matrix in Section 3.1.*

    This section identifies the P2PE Components validated for use with this P2PE Component including the Reassessment Date of the P2PE Component.

    While a P2PE Component may include third-party services (including those offering services potentially eligible for being Listed as a Validated P2PE Component), those third-party services are not identified within the P2PE Component's Listing or on the List of Validated P2PE Components. Any use of such a service in another P2PE Product would require either an independent Listing as a P2PE Component, if eligible, or assessment as part of each P2PE Product of which the P2PE Component is a part of.

  - **P2PE Applications Supported**

    This section identifies the P2PE Applications validated for use with the P2PE Component including the P2PE Application's Reassessment date.

  - **PCI-Approved PTS POI Devices Supported**

    This section identifies PCI-approved PTS POI devices, including the PTS POI device hardware and firmware versions, validated for use with this P2PE Component and will include relevant PCI PTS reference numbers and expiry dates of the PTS approval. A Website link to the associated PTS Approval on the PCI List of Approved PIN Transaction Security (PTS) Devices is included for each device supported.

  - **PCI-Approved PTS HSMs Supported**

    This section identifies PCI-approved PTS HSM devices validated for use with this P2PE Component and will include the relevant PCI PTS reference numbers and expiry dates of the PCI PTS approval. A Website link to the associated PTS Approval on the PCI List of Approved PIN Transaction Security (PTS) Devices is included for each device supported.

  - **FIPS 140 Validated HSMs Supported**

    This section identifies FIPS 140 validated HSMs for use with this P2PE Component, including the *NIST Cryptographic Module Validation Program (CMVP)* certificate number and sunset date. A website link will be provided to the appropriate entry in the *NIST CMVP database of validated cryptographic modules*.

P2PE Standard Version

The version of the P2PE Standard used to validate the P2PE Component.

P2PE Assessor Company

The qualified P2PE Assessor Company that performed the validation and determined that the P2PE Component is in accordance with the P2PE Standard and Program Requirements.

Annual Revalidation Date

The date by which the P2PE Component Provider must satisfy the Annual Revalidation process, which occurs at the 12- and 24-month mark from the last date of Acceptance based on a Full Assessment.

Reassessment Date

The 3-year date from the last date of Acceptance based on a Full Assessment by which time the P2PE Component Provider can choose to undergo and submit another Full Assessment of the P2PE Component to the P2PE Standard and Program Requirements to, provided Acceptance occurs, maintain their Listing.

Appendix D. Elements for the List of Validated P2PE Applications

P2PE Vendor Company Name (link to Company website)

The P2PE Application Vendor for the P2PE Application.

P2PE Application Information

The following fields in the Listing provide relevant information for each Validated P2PE Application, consisting of the following:

- **P2PE Application Name**

  Note: *The P2PE Application Name cannot contain any variables or special characters.*

  The P2PE Application Name is provided by the Application Vendor and is the name by which the application is known.

- **P2PE Application Version Number**

  Note: *Refer to Appendix E for details about content to include in the P2PE Application P-ROV and P2PE Application Implementation Guide for the Application Vendor's versioning methods.*

  Represents the validated application version. The format of the version number:

  Is set by the P2PE Application Vendor, in accordance with Program Requirements;

  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*.

- **Reference Number**

  PCI SSC assigns the Reference Number once the Validated P2PE Application is Accepted, which uniquely identifies the Listed P2PE Application.

  Note: *A Listed P2PE Application that undergoes a Reassessment that is subsequently Accepted and Listed on the Website results in a new Reference Number.*

  An example reference number format is 2024-xxxxx.yyy, consisting of the following:

Field	Format
Year of Listing	4 digits + hyphen
P2PE Application Vendor Identifier	5 digits + period This value uniquely identifies the P2PE Application Vendor.
P2PE Application Identifier	3 digits This value uniquely identifies the P2PE Application of the P2PE Application Vendor.

- **P2PE Application Details**

  Details specific to the P2PE Application consisting of underlying dependencies that include the following:

  – **PCI-Approved PTS POI Devices Supported**

This section identifies PCI-approved PTS POI devices, including the PTS POI device hardware and firmware versions, validated for use with the P2PE Application and will include the relevant PCI PTS reference numbers and expiry dates of the PCI PTS approval. A Website link to the associated PTS Approval on the PCI List of Approved PIN Transaction Security (PTS) Devices is included for each device supported.

P2PE Standard Version

The version of the P2PE Standard used to validate the P2PE Application.

P2PE Application Assessor Company

The qualified P2PE Application Assessor Company that performed the validation and determined that the P2PE Application is in accordance with the P2PE Standard and Program Requirements.

Annual Revalidation Date

The date by which the P2PE Application Vendor must satisfy the Annual Revalidation process, which occurs at the 12- and 24-month mark from the last date of Acceptance based on a Full Assessment.

Reassessment Date

The 3-year date from the last date of Acceptance based on a Full Assessment by which time the P2PE Application Vendor can choose to undergo and submit another Full Assessment of the P2PE Application to the P2PE Standard and Program Requirements to, provided Acceptance occurs, maintain their Listing.

Appendix E. 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 Application Assessor Companies are required to verify the P2PE Application Vendor is adhering to the documented versioning methodology and the requirements of the *P2PE Program Guide* as part of the P2PE Assessment. Note that if a separate version-numbering scheme is maintained internally by the P2PE Application Vendor, a method to accurately map the internal version numbers to the publicly listed version number(s) must be documented and maintained by the P2PE Application Vendor.

E.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.

E.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 (refer to Section E.3, "Wildcards" below). All changes that impact security functionality and/or any P2PE Standard 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 Standard 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 Standard requirements
- Changes that impact any security functionality or P2PE Standard requirements

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.

E.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 Accepted and Listed. The use of wildcard elements is permitted subject to the following:

a) Wildcard elements may only be used for non-security-impacting changes, which have no impact on security and/or any P2PE Standard 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 Application Assessor Company as part of the P2PE Assessment of the P2PE Application.

Appendix F. P2PE Report on Validation (P-ROV) Templates

The P2PE Program includes P-ROV templates required for use by P2PE Assessor Companies to facilitate the Validation of P2PE Products. The table below can be used as a reference regarding which P-ROV(s) is required to Validate each P2PE Product type. Note that more than one P-ROV type may be required depending on the unique P2PE Product implementation and whether it leverages Listed P2PE Components and/or Listed P2PE Applications.

Table 2: P-ROV Templates

P-ROV Name (Abbreviated)	Used for the Following Assessments	Purpose
Template for Report on Validation for use with P2PE v3.1 for P2PE Solution Assessments	P2PE Solution	Validation of a P2PE Solution requires, at a minimum, a P2PE Solution P-ROV. Additional P-ROVs (below) may be required for Validating a P2PE Solution depending on whether Listed P2PE Components and/or P2PE Applications are included. ***Note:*** *A separate Merchant-Managed Solution P-ROV is used as part of validating MMS.*
Template for Report on Validation for use with P2PE v3.1 for P2PE Encryption Management Services Assessments	P2PE Solution (as needed) Encryption Management POI Deployment POI Management	"Encryption Management Services" relates to the distribution, management, and use of PCI-approved PTS POI devices in a P2PE Solution. Validation of P2PE Solutions that do not outsource the entirety of their Encryption Management Services to Listed P2PE Component Providers, either to an EMCP or to BOTH a PDCP AND a PMCP, must include this P-ROV in addition to a Solution P-ROV. Validation of P2PE Component services provided by an EMCP, PDCP, or a PMCP must use this P-ROV.
Template for Report on Validation for use with P2PE v3.1 for P2PE Application Assessments	P2PE Application	Validation of a P2PE Application (software on the PCI-approved POI device intended for use in a P2PE Solution that has the potential to access clear-text cardholder data) must use this P-ROV. This applies for both P2PE Applications intended to be Listed, as well as P2PE Applications that are not intended to be Listed and are assessed only as part of, and allowed for use in, a specific P2PE Solution (Solution-specific P2PE Applications). ***Note:*** *Validation of a P2PE Application must be performed by a qualified P2PE Application Assessor Company.*

P-ROV Name (Abbreviated)	Used for the Following Assessments	Purpose
Template for Report on Validation for use with P2PE v3.1 for Decryption Management Services Assessments	P2PE Solution (as needed) 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. Validation of P2PE Solutions that do not outsource the entirety of their Decryption Management Services to a Listed DMCP must include this P-ROV in addition to a Solution P-ROV. Validation of P2PE Component services provided by a DMCP must use this P-ROV.
Template for Report on Validation for use with P2PE v3.1 for Key Management Services Assessments	P2PE Solution (as needed) 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 (POI devices, HSMs, etc.). Validation of a P2PE Solution that has not satisfied the key management services requirements (Domain 5) either using Listed P2PE Component Providers and/or through the assessment of their Encryption Management Services and/or Decryption Management Services must complete the KMS P-ROV. E.g., if the P2PE Solution offers remote key-distribution using asymmetric techniques for the distribution of keys to PCI-approved PTS 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 Validation of the P2PE Solution must include the use of this [KMS] P-ROV. Validation of P2PE Component services provided by a KIF, KMCP, KLCP, and a CA/RA must complete this P-ROV.

Appendix G. P2PE Report on Validation (P-ROV) Submission Overview

This section focuses specifically on the P-ROVs submitted to PCI SSC as part of a P2PE Product validation submission.

P-ROV Preparation and Submission:

The P2PE Assessor Company must complete the applicable P-ROV(s) in accordance with the Program Requirements. If the P2PE Assessor determines there are items that need to be addressed, the P2PE Vendor must address those items, and the P2PE Assessor Company 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 on behalf of the P2PE Vendor. 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.

PCI SSC P-ROV Submission Review

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.

PCI SSC's Assessor Quality Management Team ("AQM") reviews each P-ROV submission after the invoice for the applicable fees have been paid by the P2PE Vendor. The administrative review will be performed in "pre-screening" to ensure that the submission is complete prior to the AQM review, during which a member of AQM reviews the submission in its entirety.

AQM will review the P2PE submission first to determine whether the P2PE Product is eligible for validation as described in the herein for the Program. If there are questions as to eligibility, AQM will contact the P2PE Assessor Company for additional information. If the P2PE submission is determined to be ineligible for Validation, the P-ROV submission will be rejected, and 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 Program, AQM will conduct a complete review of the P2PE Product submission. Any comments or feedback from AQM will be made via the Portal, and the P2PE Assessor Company must address all inquiries and feedback in a timely manner. AQM's role is to ensure sufficient evidence is included to provide reasonable assurance that the Validation of the P2PE Product was performed in accordance with applicable Program Requirements and meets quality standards.

Subsequent iterations will also be responded to, typically within 40 calendar days of receipt. If the P-ROV(s) meet all applicable quality assurance requirements (as documented or referred to in the *P2PE Qualification Requirements* and related P2PE Program materials), PCI SSC sends the countersigned *P-AOV* to both the P2PE Vendor and the P2PE Assessor Company and adds the product to the List of Validated P2PE Products, as applicable.

PCI SSC communicates any quality issues associated with the submitted P-ROVs directly 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 PCI SSC within 30 calendar days of the preceding submission (clearly denoting and communicating the cumulative changes within the document(s), including redline as applicable). If resubmitting to PCI SSC within 30 calendar days is not possible, the P2PE Assessor Company must inform 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.

Appendix H. 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.

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

When undergoing a P2PE Assessment, ‘Not Applicable’ cannot be used by entities that provide only partial aspects of a defined P2PE Component Provider service to validate to that P2PE Component Provider type.

Notes for the P2PE Standard Requirement Applicability Matrix:

1 - Where a Solution Provider (or a Merchant as a Solution Provider in a Merchant-Managed Solution - MMS) is using a Listed P2PE Component Provider, the Solution Provider is not required to have the requirements applicable to that Listed P2PE Component assessed as part of their P2PE Solution assessment. E.g., if a Solution Provider outsources to a 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 Listed P2PE Component Providers, the Solution Provider is responsible for including all applicable key management services requirements in the scope of their assessment.

E.g., if the P2PE Solution offers remote key-distribution using asymmetric techniques for the distribution of keys to PCI-approved 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 Listed P2PE Component Provider, then the P2PE Solution assessment must include all applicable key management services requirements (Domain 5).

2 - Where an Encryption Management Component Provider is using a Listed P2PE POI Deployment or Listed 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 Provider, as applicable, assessed as part of their Encryption Management Component Provider assessment.

3 - Where a Key Injection Facility (KIF) Component Provider is using a Listed P2PE Key Loading or Listed Key Management Component Provider, the KIF Component Provider is not required to have the requirements applicable to the Key Loading or Key Management Component Provider, 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 PCI-approved PTS 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 Listed P2PE Decryption Management Component Provider that employs hybrid decryption.

P2PE Standard 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							

P2PE Standard 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)*											
2B-4				X							
2C-1				X							
2C-2				X							
2C-3				X							
Domain 3											
3A-1											X
3A-2											X
3A-3											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						

P2PE Standard 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											
1-1	***Note:*** *Not used in P2PE*										
1-2							X	X			
1-3	X	X	X		X	X	X	X	X		X
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

P2PE Standard 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)											
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		X
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	
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

P2PE Standard 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)											
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			
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			

P2PE Standard 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)											
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
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	
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	

P2PE Standard 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)											
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
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

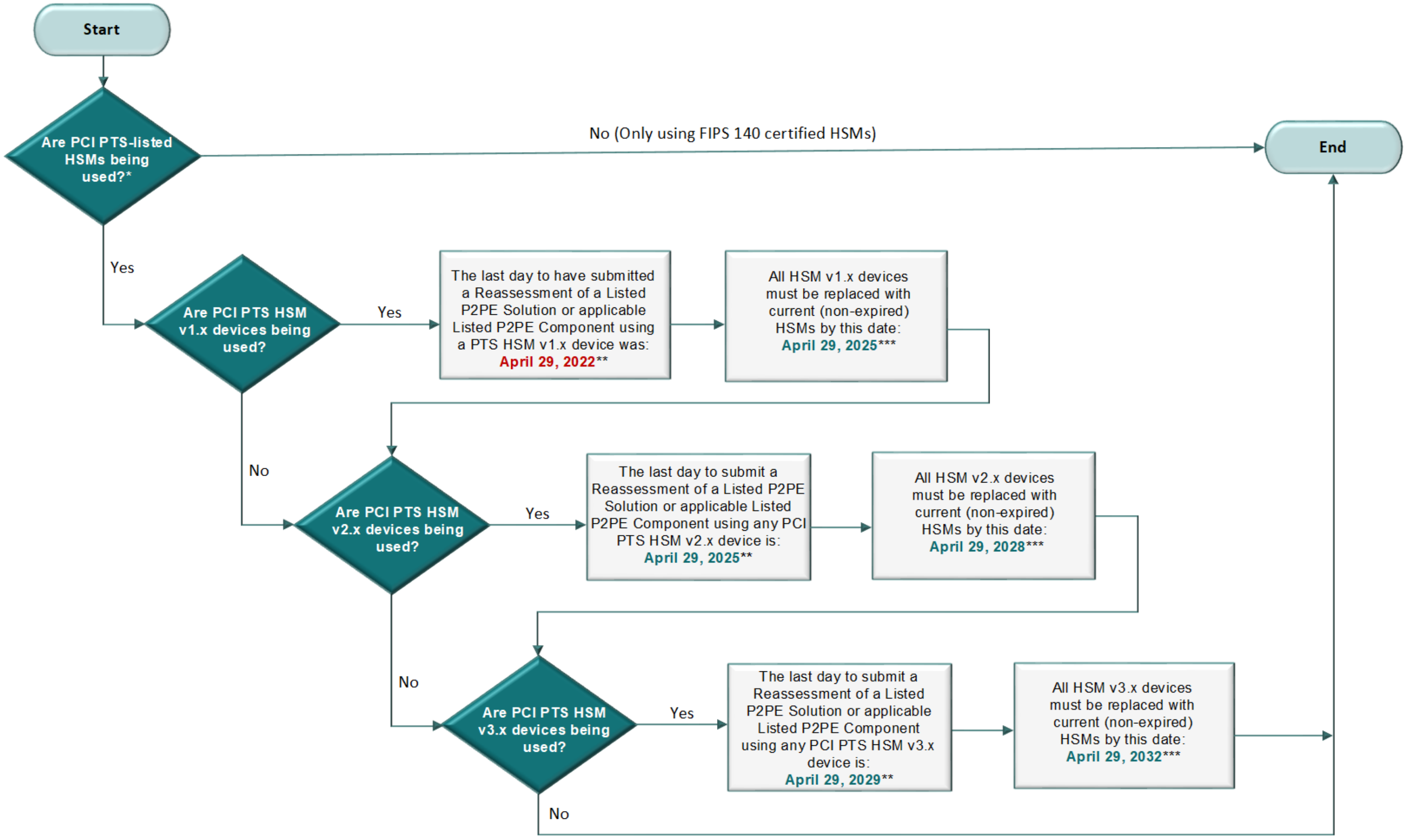
P2PE Standard Security Requirements

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)											
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
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			

P2PE Standard 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)											
32-9							X	X			
33-1	X	X	X		X		X	X	X		X
5A-1	X	X	X		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 applicable to Component Providers performing key management services for POI devices and/or HSMs*											
5I-1	X	X	X		X	X	X	X	X		X
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 I. PCI-Approved HSM Expiry Flowchart


Start
Are PCI PTS-listed HSMs being used?*
No (Only using FIPS 140 certified HSMs)
End
Yes
Are PCI PTS HSM v1.x devices being used?
Yes
The last day to have submitted a Reassessment of a Listed P2PE Solution or applicable Listed P2PE Component using a PTS HSM v1.x device was: April 29, 2022**
All HSM v1.x devices must be replaced with current (non-expired) HSMs by this date: April 29, 2025***
No
Are PCI PTS HSM v2.x devices being used?
Yes
The last day to submit a Reassessment of a Listed P2PE Solution or applicable Listed P2PE Component using any PCI PTS HSM v2.x device is: April 29, 2025**
All HSM v2.x devices must be replaced with current (non-expired) HSMs by this date: April 29, 2028***
No
Are PCI PTS HSM v3.x devices being used?
Yes
The last day to submit a Reassessment of a Listed P2PE Solution or applicable Listed P2PE Component using any PCI PTS HSM v3.x device is: April 29, 2029**
All HSM v3.x devices must be replaced with current (non-expired) HSMs by this date: April 29, 2032***
No

* Answer YES if you are using any HSMs in your P2PE Solution or P2PE 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).

** Listed P2PE Solutions and applicable Listed 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.

*** Listed P2PE Solutions and applicable Listed 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.

Figure 9: PCI-Approved PTS HSM Expiry Flowchart