Payment Card Industry (PCI)

# Qualification Requirements

## For Point-to-Point Encryption (P2PE)™ Qualified Security Assessors – QSA (P2PE) and PA-QSA (P2PE)

**Version 2.1**
December 2015

## Document Changes

| Date | Version | Description |
|---|---|---|
| June 2012 | 1.0 | Initial Release of the *PCI P2PE Qualification Requirements* |
| February 2013 | 1.1 | Updated to reflect changes to Domain 2 assessments and changes to the evolving P2PE Program |
| September 2015 | 2.0 | Updated to align to v2.0 of the *P2PE Standard* and *QSA Qualification Requirements v2.0* |
| December 2015 | 2.1 | Updated *Appendix A: Addendum to QSA Agreement for P2PE Assessor Companies* to allow QSA (P2PE)s to assess the Token Service Provider (TSP) Requirements. |

# Table of Contents

# 1 Introduction

Building upon the solid data and environmental security foundation established and promulgated by the PCI Security Standards Council, LLC ("PCI SSC" or the "Council") for the payments industry via the PCI DSS, PA-DSS, and PTS, the P2PE Standard is a comprehensive set of requirements focused on providing the requisite security requirements, testing procedures, assessor training, and resources necessary to support the deployment of secure P2PE Solutions.

Please note that the existence of the P2PE Standard does not constitute a recommendation from the Council, nor does it obligate merchants, service providers, or financial institutions to purchase or deploy P2PE Solutions. As with all other PCI SSC standards, any mandates, regulations, or rules regarding compliance with any of the foregoing are provided by the participating payment brands.

These *P2PE Qualification Requirements* supplement the QSA Qualification Requirements for each Qualified Security Assessor Company ("QSA Company") that intends to qualify as a P2PE Assessor Company, and describe the minimum qualification requirements and related documentation that a P2PE Assessor Company must satisfy and provide to PCI SSC in order to qualify to perform P2PE Assessments as a participant in the P2PE Assessor program described herein (the "P2PE Assessor Program"). These *P2PE Qualification Requirements* amend, restate, and supersede in its entirety the *Payment Card Industry (PCI) QSA Qualification Requirements Supplement for Point-to-Point Encryption (P2PE) Qualified Security Assessors – QSA (P2PE) and PA-QSA (P2PE), v1.1 (February 2013).*

## 1.1 Terminology

Throughout this document, the following terms shall have the following meanings.

| Term | Meaning |
|---|---|
| **P-ROV** | A "P2PE Report on Validation" completed by a P2PE Assessor Company and (except with respect to Merchant Managed P2PE Solutions) submitted directly to PCI SSC for review and Acceptance (defined in the P2PE Program Guide).<br>For a P2PE Solution, P2PE Component, or P2PE Application to be included on the corresponding list of validated solutions, components, or applications on the Website, a corresponding P-ROV must be submitted directly to PCI SSC for review and Acceptance. |
| **P2PE Application** | Refer to definition in *P2PE Glossary*. |
| **P2PE Application Assessment** | Assessment of a P2PE Application against the *P2PE Domain 2 Testing Procedures* in isolation of any point-to-point solution in order to validate compliance with such Testing Procedures in connection with the P2PE Assessor Program. |
| **P2PE Application Vendor** | Refer to definition in *P2PE Glossary*. |
| **P2PE Assessment** | A P2PE Solution Assessment, P2PE Component Assessment, or P2PE Application Assessment. |
| **P2PE Assessor Addendum** | The *Addendum to Qualified Security Assessor (QSA) Agreement for P2PE Assessor Companies* in the form attached as Appendix A to the *P2PE Qualification Requirements*. |

| Term | Meaning |
|---|---|
| **P2PE Assessor Company** | A company then qualified by PCI SSC as either a QSA (P2PE) Company or a PA-QSA (P2PE) Company. |
| **P2PE Assessor Employee** | A QSA (P2PE) Employee or PA-QSA (P2PE) Employee. |
| **P2PE Assessor List** | The list of P2PE Assessor Companies maintained on the Website. |
| **P2PE Assessor Requirements** | The QSA (P2PE) Requirements and/or PA-QSA (P2PE) Requirements, as applicable. |
| **P2PE Component Assessment** | Assessment of a P2PE Component in order to validate compliance with the P2PE Standard as part of the P2PE Assessor Program. |
| **P2PE Component Provider** | Refer to definition in *P2PE Glossary.* |
| **P2PE Component** | A P2PE service (such as encryption management, decryption management, or key injection) that is eligible for validation and Acceptance on a standalone basis as part of the P2PE Program and may be incorporated into and/or referenced as part of a P2PE Solution. |
| **P2PE Domain 2 Testing Procedures** | All testing procedures for P2PE Domain 2 specified in the column labeled "Testing Procedures" in the P2PE Standard. |
| **P2PE Domain 2 Requirements** | All items specified in the column labeled "Domain 2 Requirements" in the P2PE Standard. |
| **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. |
| ***P2PE Qualification Requirements*** | The then-current version of (or successor document to) the *Payment Card Industry (PCI) Qualification Requirements For Point-to-Point Encryption (P2PE) Qualified Security Assessors – QSA (P2PE) and PA-QSA (P2PE)*, as from time to time amended and made available on the Website. |
| **P2PE Program Guide** | The then-current version of (or successor document to) the *Payment Card Industry (PCI) Point-to-Point Encryption Program Guide*, as from time to time amended and made available on the Website. |
| **P2PE Solution** | A combination of secure devices, applications, and processes that encrypt cardholder data from a PCI SSC-approved point-of-interaction (POI) device through to decryption and is eligible for validation and Acceptance as part of the P2PE Program. |
| **P2PE Solution Assessment** | Assessment of a P2PE Solution in order to validate compliance with the P2PE Standard as part of the P2PE Assessor Program. |
| **P2PE Solution Provider** | Refer to definition in *P2PE Glossary.* |

| Term | Meaning |
|---|---|
| **P2PE Standard** | The then-current version of (or successor document(s) to) the *Payment Card Industry (PCI) Point-to-Point Encryption Solution Requirements and Testing Procedures*, any and all appendices, exhibits, schedules, and attachments to the foregoing and all materials incorporated therein, in each case, as from time to time amended and made available on the Website. |
| **P2PE Vendor Release Agreement** | The then-current and applicable form of release agreement that PCI SSC:<br>(a) Requires to be executed by P2PE Solution Providers, P2PE Component Providers, and/or P2PE Application Vendors (as applicable) in connection with the P2PE Assessor Program, and<br>(b) Makes available on the Website. |
| **PA-QSA Addendum** | The *Addendum to Qualified Security Assessor (QSA) Agreement for Payment Application QSAs* in the form attached as Appendix A to the *PA-QSA Qualification Requirements*. |
| **PA-QSA Company** | Refer to definition in *PA-QSA Qualification Requirements*. |
| **PA-QSA Qualification Requirements** | The *Payment Card Industry (PCI) Qualification Requirements for Payment Application Qualified Security Assessors (PA-QSA)* (or successor document), as from time to time amended and made available on the Website. |
| **PA-QSA (P2PE) Company** | A Payment Application-Qualified Security Assessor (PA-QSA) Company that:<br>(a) Is qualified by PCI SSC to provide services to P2PE Solution Providers, P2PE Component Providers, and/or P2PE Application Vendors in order to validate that such providers' or vendors' P2PE Solutions, P2PE Components, and/or P2PE Applications adhere to all aspects of the P2PE Standard, including but not limited to validation that payment applications, when incorporated into or used as part of a P2PE Solution, adhere to all P2PE Domain 2 requirements; and<br>(b) Remains in Good Standing (defined in Section 1.3 of the *P2PE Qualification Requirements*) or in remediation as a PA-QSA (P2PE) Company. |
| **PA-QSA (P2PE) Employee** | An individual employed by a PA-QSA (P2PE) Company who has satisfied, and continues to satisfy, all PA-QSA (P2PE) Requirements applicable to employees of PA-QSA (P2PE) Companies who will conduct P2PE Application Assessments, as described in further detail herein. |

| Term | Meaning |
|---|---|
| **PA-QSA (P2PE) Requirements** | The requirements and obligations generally applicable to all PA-QSA (P2PE) Companies as provided for in the *P2PE Qualification Requirements*, *the P2PE Assessor Addendum*, the *P2PE Program Guide*, and any and all other policies, procedures, requirements, or obligations imposed, mandated, provided for, or otherwise established by PCI SSC from time to time for PA-QSA (P2PE) Companies generally in connection with the P2PE Assessor Program. These include but are not limited to all QSA (P2PE) Requirements and the requirements of all applicable training programs, quality assurance and remediation programs, program guides, and other P2PE Assessor Program materials. |
| **QSA Agreement** | The *Qualified Security Assessor (QSA) Agreement,* in the form attached as Appendix A to the *QSA Qualification Requirements*. |
| **QSA Qualification Requirements** | The then-current version of the *Payment Card Industry (PCI) Data Security Standard Qualification Requirements for Qualified Security Assessors (QSA)* (or successor document), as from time to time amended and made available on the Website. |
| **QSA Requirements** | Refer to definition in *QSA Qualification Requirements*. |
| **QSA (P2PE) Company** | A Qualified Security Assessor (QSA) Company that:<br>(a) Is qualified by PCI SSC to provide services to P2PE Solution Providers and/or P2PE Component Providers in order to validate that such providers' P2PE Solutions and/or P2PE Components adhere to all applicable aspects of the P2PE Standard, and<br>(b) Remains in Good Standing (defined in Section 1.3 of the *P2PE Qualification Requirements*) or in remediation as a QSA (P2PE) Company.<br>QSA (P2PE) Company qualification, alone, does not qualify a company to conduct P2PE Application Assessments. P2PE Application Assessments may only be performed by PA-QSA (P2PE) Companies. |
| **QSA (P2PE) Employee** | An individual employed by a QSA (P2PE) Company who has satisfied, and continues to satisfy, all QSA (P2PE) Requirements (defined in the *P2PE Qualification Requirements*) applicable to employees of QSA (P2PE) Companies who will conduct P2PE Application Assessments, as described in further detail herein. |
| **QSA (P2PE) Requirements** | The requirements and obligations generally applicable to all QSA (P2PE) Companies as provided for in the *P2PE Qualification Requirements,* the *P2PE Assessor Addendum*, the *P2PE Program Guide,* and any and all other policies, procedures, requirements, or obligations imposed, mandated, provided for, or otherwise established by PCI SSC from time to time for QSA (P2PE) Companies generally in connection with the P2PE Assessor Program. These include but are not limited to the requirements of all applicable training programs, quality assurance and remediation programs, program guides, and other P2PE Assessor Program materials. |

| Term | Meaning |
|---|---|
| **Website** | The then-current PCI SSC website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org. |

All capitalized terms used in these *P2PE Qualification Requirements* without definition shall have the meanings ascribed to them in the *QSA Qualification Requirements* or the *QSA Agreement*, as applicable, and if not defined therein, then in other relevant PCI SSC program materials.

## 1.2 Goal

Each company (and employee thereof) wishing to participate in the P2PE Assessor Program must satisfy all applicable P2PE Assessor Requirements prior to applying to the Program.

Together, the QSA Requirements and QSA (P2PE) Requirements — and for PA-QSA (P2PE) Companies, the PA-QSA (P2PE) Requirements and PA-QSA Requirements (as defined in the *PA-QSA Qualification Requirements*) — are intended to serve as a qualification baseline and provide a transparent process for P2PE Assessor Company and P2PE Assessor Employee qualification and re-qualification for P2PE Assessor Program purposes.

All P2PE Assessor Companies appear on the P2PE Assessor List. If a company is not so identified, its work product as a P2PE Assessor Company is not recognized by PCI SSC.

## 1.3 Qualification Process Overview

The P2PE Assessor qualification process first involves the qualification of the QSA Company itself as a P2PE Assessor Company, followed by qualification of the P2PE Assessor Company's employee(s) who will be performing and/or managing the P2PE Assessments.

- **QSA (P2PE) Company:** In order to be and remain qualified as a QSA (P2PE) Company, and accordingly, in order to validate compliance of P2PE Solutions and P2PE Components with the P2PE Standard and otherwise participate as a QSA (P2PE) Company in the P2PE Assessor Program, the assessor company must:

  (a) Be in Good Standing as a QSA Company (as defined in the *QSA Agreement*),

  (b) Have submitted an approved P2PE Assessor Company application package to PCI SSC,

  (c) Have an effective *P2PE Assessor Addendum* in place with PCI SSC,

  (d) Comply with all applicable P2PE Assessor Requirements (including but not limited to payment of all applicable fees and satisfaction of all applicable staffing, training, and examination requirements), and

  (e) Not have had any qualification provided by PCI SSC revoked, suspended, or terminated or be in breach of any applicable Program Requirements (defined in the *P2PE Assessor Addendum*) or any term, condition, or requirement of P2PE Assessor Company quality assurance or remediation.

  An assessor company satisfying all of the above requirements is considered to be in "Good Standing" as a QSA (P2PE) Company and, while it is in such Good Standing, may market itself as a QSA (P2PE) Company.

  ***Note:*** *A QSA (P2PE) Company that is in remediation as a QSA Company or QSA (P2PE) Company but otherwise satisfies all of the requirements specified in (a) through (e) above is permitted to perform P2PE Solution Assessments and P2PE Component Assessments and market itself as a QSA (P2PE) Company, subject to the terms of the applicable remediation program.*

- **PA-QSA (P2PE) Company:** In order to be and remain qualified as a PA-QSA (P2PE) Company, and accordingly, in order to validate compliance of P2PE Applications with the P2PE Standard and otherwise participate as a PA-QSA (P2PE) Company in the P2PE Assessor Program, the assessor company must:

  (a) Be in QSA Company, PA-QSA Company and QSA (P2PE) Company Good Standing,

  (b) Comply with all requirements applicable to PA-QSA Companies in connection with the PA-QSA Program (including but not limited to payment of all applicable fees and satisfaction of all applicable staffing, training, and examination requirements), and

  (c) Not have had its PA-QSA (P2PE) Company qualification revoked, suspended or terminated.

  A PA-QSA (P2PE) Company satisfying all of the requirements specified in (a) through (c) above is considered to be in "Good Standing" as a PA-QSA (P2PE) Company and, while it is in such Good Standing, may market itself as a PA-QSA (P2PE) Company.

  ***Note:*** *A PA-QSA (P2PE) Company that is in remediation as a QSA Company, PA-QSA Company, QSA (P2PE) Company or PA-QSA (P2PE) Company but otherwise satisfies all of the requirements specified in (a) through (c) above is permitted to perform P2PE Solution Assessments, P2PE Component Assessments, and P2PE Application Assessments and market itself as a PA-QSA (P2PE) Company, subject to the terms of the applicable remediation program.*

  To initiate the qualification process, the applicant P2PE Assessor Company must sign the P2PE Assessor Addendum and submit it to PCI SSC, along with the company's executed P2PE Assessor Company application (see Appendix B).

## 1.4 Document Structure

This document is structured as follows.

**Section 1: Introduction** offers a high-level overview of the P2PE Assessor application process.

**Section 2: P2PE Assessor Company Business Requirements** covers minimum additional business requirements that must be demonstrated to PCI SSC by the P2PE Assessor Company. This section outlines information and items that must be provided to prove business stability, independence, and insurance coverage. P2PE Assessor Company fees and agreements are also covered.

**Section 3: P2PE Assessor Company and Employee Capability Requirements** reviews the information and documentation necessary to demonstrate the QSA (P2PE) Company and/or PA-QSA (P2PE) Company's service expertise, as well as that of its employees.

**Section 4: P2PE Assessor Company Administrative Requirements** focuses on the logistics of doing business as a P2PE Assessor Company, including adherence to PCI SSC procedures, quality assurance, and protection of confidential and sensitive information.

**Section 5: P2PE Assessor List, Re-qualification, Remediation, and Revocation** describes the process for being listed as a P2PE Assessor Company, how to re-qualify for the P2PE Assessor List, and related Remediation and Revocation processes.

***Note:*** *In addition to the requirements set forth in the* P2PE Qualification Requirements*, ALL P2PE Assessor Companies must satisfy all requirements of the QSA Qualification Requirements, and for PA-QSA (P2PE) Companies, all requirements of the* PA-QSA Qualification Requirements*.*

**Section 6: Assessor Quality Management Program** describes quality management requirements.

**Appendices:** The appendices to these *P2PE Qualification Requirements* include the *P2PE Assessor Addendum* (Appendix A), *P2PE Assessor Company Application* (Appendix B) and *P2PE Assessor Employee Application* (Appendix C) forms.

## 1.5 Related Publications

The *P2PE Qualification Requirements* are intended for use with the current version of the *QSA Qualification Requirements,* which are used in conjunction with the current versions of the following other PCI SSC publications, each as available through the Website:

- P2PE Standard
- *Payment Card Industry Data Security Standard Security (PCI DSS) Requirements and Security Assessment Procedures*
- *PA-QSA Qualification Requirements*
- *PA-QSA Addendum*

## 1.6 P2PE Assessor Company Application Process

In addition to outlining the requirements that a P2PE Assessor Company and its P2PE Assessor Employees must meet to be recognized by PCI SSC to perform P2PE Assessments, this document describes the information that must be provided to PCI SSC as part of the P2PE Assessor Company and P2PE Assessor Employee application and qualification process. Each outlined requirement is followed by the information that must be submitted to document that the P2PE Assessor Company meets or exceeds the stated requirements.

***Important Note:*** *PCI SSC reserves the right to reject any application for any applicant (company or individual) that PCI SSC determines has committed, within three (3) years prior to the application date, any conduct that would have been considered a "Violation" for purposes of the* QSA Qualification Requirements *or QSA Agreement, if committed by a QSA Company or QSA Employee. The period of ineligibility will be a minimum of one (1) year, as determined by PCI SSC in a reasonable and non-discriminatory manner, in light of the circumstances.*

### *1.6.1 Preparation*

To facilitate preparation of the application package, refer to Appendix B: P2PE Assessor Company – Application and Appendix C: P2PE Assessor Employee – Application. All application materials and the signed *P2PE Assessor Addendum* must be submitted in English. The *P2PE Assessor Addendum* is binding in English even if it was translated and reviewed in another language. All other documentation provided to PCI SSC by the applicant P2PE Assessor Company at any time in a language other than English must be accompanied by a certified English translation (examples include application materials, P-ROVs, and any other materials provided to PCI SSC).

### *1.6.2 Submission*

All P2PE Assessor Company application packages must include a signed *P2PE Assessor Addendum* (see Appendix A) and all other required documentation. All application materials must be submitted electronically via PCI SSC's secure portal (the "Portal"). Applicants should submit their request for access to the Portal by sending an e-mail to p2pe@pcisecuritystandards.org, "Attention: Program Manager."

### *1.6.3 Fees*

Applicants must pay all applicable fees (see Section 2.4 below) before PCI SSC will review corresponding application materials.

## 1.7 Additional Information Requests

In an effort to maintain the integrity of the P2PE Assessor Program, PCI SSC may from time to time request that P2PE Assessor Companies and P2PE Assessor Employees submit additional information or materials in order to demonstrate adherence to applicable requirements, as part of the applicable qualification or re-qualification process, or as part of the P2PE Assessor Program approval or quality assurance process, including but not limited to in connection with remediation, revocation, or appeals. All such additional information and materials must be submitted in accordance with the corresponding PCI SSC request, and in English or with a certified English translation. P2PE Assessor Companies are required to respond to each such request with the required information or documentation no later than three (3) weeks from receipt of the corresponding PCI SSC request or as otherwise requested by PCI SSC.

# 2 P2PE Assessor Company Business Requirements

This section describes the minimum business requirements and related information that must be provided to PCI SSC. The provisions requested include information about the company's business legitimacy, independence, and required insurance coverage.

## 2.1 Business Legitimacy

All P2PE Assessor Companies must meet all business legitimacy requirements provided for in the *QSA Qualification Requirements.*

## 2.2 Independence

All P2PE Assessor Companies must meet all independence requirements provided for in the *QSA Qualification Requirements.*

A P2PE Assessor Company must neither conduct a P2PE Assessment of, nor submit a P-ROV attesting to the validation of, any of its own P2PE Solutions, P2PE Components, or P2PE Applications.

## 2.3 Insurance Coverage

All P2PE Assessor Companies must meet all insurance coverage requirements as set forth in the *QSA Qualification Requirements.*

## 2.4 P2PE Assessor Program Fees

Each P2PE Assessor Company applicant must provide to PCI SSC the applicable initial application fees (see the Website – *PCI SSC Programs Fee Schedule*). Initial application fees must be paid in advance of PCI SSC reviewing the application materials and are credited toward regional qualification fees (see below) if a company is qualified as a P2PE Assessor Company. All fees are invoiced by PCI SSC and must be paid to PCI SSC according to the instructions accompanying the invoice.

Once a company meets the requirements for qualification as a P2PE Assessor Company, the following fees as then specified on the Website shall also apply:

- Regional qualification fees (vary by country or region)
- Annual regional re-qualification fees for subsequent years (also vary by country or region)
- Annual P2PE Assessor Employee training fee for each P2PE Assessor Employee (or candidate).

***Note:*** *All P2PE Assessor Program fees are subject to change and are non-refundable.*

## 2.5 P2PE Assessor Company Agreements

As described in further detail in the *QSA Qualification Requirements*, each QSA Company must have executed and submitted the QSA Agreement to qualify as a QSA Company.

Once qualified as a QSA Company, there are various other agreements that a QSA Company must execute and submit to PCI SSC, depending on the PCI SSC Programs in which the QSA Company wishes to participate.

In order to participate in the P2PE Assessor Program, PCI SSC requires that all related agreements between PCI SSC and the applicant P2PE Assessor Company (including the *P2PE Assessor Addendum)* be signed by a duly authorized officer of the applicant P2PE Assessor Company, and submitted in unmodified form to PCI SSC via the Portal (see Section 1.6.2) with the completed P2PE Assessor Company application package.

The *P2PE Assessor Addendum* requires, among other things, that the P2PE Assessor Company and its P2PE Assessor Employees comply with all applicable P2PE Assessor Requirements.

# 3 P2PE Assessor Company Capability Requirements

The types and roles of P2PE Assessor Companies are outlined in *Appendix D: Types of P2PE Assessor Companies and Applicability to the P2PE Standard.*

## 3.1 P2PE Assessor Company – Services and Experience

### *3.1.1 P2PE Assessor Company Requirements*

- Each P2PE Assessor Company performing or managing any P2PE Assessment must be qualified by PCI SSC as, and in Good Standing (or in compliance with remediation) as, both a QSA Company and a QSA (P2PE) Company.
- Each P2PE Assessor Company (or applicant) must fulfill all QSA Qualification Requirements, all QSA (P2PE) Company Requirements, and comply with all terms and provisions of the *QSA Agreement*, the *P2PE Assessor Addendum*, any other agreements executed with PCI SSC, and all other applicable policies and requirements of the P2PE Assessor Program, as mandated or imposed by PCI SSC from time to time, including but not limited to all requirements in connection with PCI SSC's quality assurance initiatives, remediation, and revocation.
- Each P2PE Assessor Company (or applicant) must have completed at least two PCI DSS Assessments as a QSA Company. Only PCI DSS Assessments performed by the applicant P2PE Assessor Company are eligible to meet this requirement.
- Each P2PE Assessor Company must have at least one year of experience with direct responsibility for implementing, operating, and/or assessing cryptographic systems and/or key management functions. For example, implementing and managing key management functions, or performing lab evaluations of cryptographic systems against NIST, ANSI, or ISO standards.
- Each P2PE Assessor Company (or applicant) must have demonstrated competence in cryptographic techniques, to include cryptographic algorithms, key management, and key lifecycle as determined in the sole discretion of PCI SSC. Competencies must include knowledge in all of the following areas:
  - Cryptographic techniques including cryptographic algorithms, key management, and key lifecycle
  - Industry standards for cryptographic techniques and key management, including but not limited to ISO 11568 and 13491, ANSI X9.24 and X9.97, and NIST 140-2 Level 3
  - Public key infrastructure (PKI) and the role and operations of a Certification Authority (CA) and Registration Authority (RA)
  - Hardware Security Modules (HSMs) operations, policies, and procedures
  - POI key-injection systems and techniques including key-loading devices (KLDs) and key-management methods, such as Master/Session or DUKPT
  - Physical security techniques for high-security areas
  - Relevant PTS Security Requirements (e.g., SRED, SCR, OP)
  - POI integration software development, deployment, and updates
  - PCI PTS authentication requirements for accessing account data or sensitive services
  - Modern, secure, embedded systems hardware and software architectures

- PCI PTS quality and security management requirements related to POI software development
- POI software authenticity and integrity verification techniques and self-tests
- Attack methodologies through exploitation of logical vulnerabilities
- Application penetration testing methodologies, to include use of forensic tools/methods, ability to exploit vulnerabilities, and ability to execute arbitrary code to test processes

All of the above skill sets must be present and fully utilized on every P2PE Assessment.

***Note:*** *Appendix B contains a list of all deliverables to be provided to PCI SSC to meet this requirement.*

### *3.1.2 Additional Requirements for PA-QSA (P2PE) Companies*

In addition to satisfying the requirements specified in Section 3.1.1 above:

- Each P2PE Assessor Company performing or managing any P2PE Application Assessment must be qualified by PCI SSC as, and in Good Standing (or in compliance with remediation) as, a QSA Company, a PA-QSA Company (as defined in the *PA-QSA Qualification Requirements*), a QSA (P2PE) Company, and a PA-QSA (P2PE) Company. Only PA-QSA (P2PE) Companies may conduct P2PE Application Assessments.
- Each PA-QSA (P2PE) Company (or applicant) must:
  - Fulfill all PA-QSA Requirements (including the laboratory requirements attested to and set forth in Appendix B of the *PA-QSA Qualification Requirements*)
  - Comply with all terms and provisions of the *PA-QSA Addendum* and all other applicable policies and requirements of the PA-DSS Program, as mandated or imposed by PCI SSC from time to time, including but not limited to all requirements in connection with PCI SSC's quality assurance initiatives, remediation, and revocation
  - Possess demonstrated competence and knowledge in surrogate PAN-generation techniques, such as format-preserving encryption and tokenization
  - Have completed at least two PA-DSS Assessments as a PA-QSA Company. Only PA-DSS Assessments performed by the applicant P2PE Assessor Company are eligible to meet this requirement

All of the above skill sets must be present and fully utilized on every P2PE Application Assessment.

***Note:*** *Appendix B contains a list of all deliverables to be provided to PCI SSC to meet this requirement.*

## 3.2 P2PE Assessor Employee – Skills and Experience

Each P2PE Assessor Employee performing or managing any P2PE Assessment must be qualified by PCI SSC as *both* a QSA Employee and a P2PE Assessor Employee. Only P2PE Assessor Employees so qualified by PCI SSC are permitted to conduct P2PE Assessments.

In addition, each P2PE Assessor Employee performing or managing a P2PE Application Assessment must be qualified by PCI SSC as a PA-QSA Employee and a PA-QSA (P2PE) Employee. Only PA-QSA (P2PE) Employees qualified by PCI SSC are permitted to conduct P2PE Application Assessments.

P2PE Assessor Employees are responsible for the following:

- Performing the applicable P2PE Assessments

- Verifying that the P2PE Assessor Company's work product addresses all applicable P2PE requirements and testing procedures, and supports the compliance status of the applicable P2PE Solution, P2PE Component, or P2PE Application
- Strictly following the P2PE Standard
- Producing all final P-ROVs

### *3.2.1 P2PE Assessor Employee Requirements*

Each P2PE Assessor Employee performing or managing P2PE Assessments must:

- Be a QSA Employee and comply with all applicable QSA Requirements, including fulfillment of all requirements for QSA Employees specified in the *QSA Qualification Requirements*
- Have completed at least two PCI DSS Assessments as a QSA Employee
- Possess experience with and substantial knowledge in *each* of the following:
  - Cryptographic techniques including cryptographic algorithms, key management, and key lifecycle
  - Knowledge of industry standards for cryptographic techniques and key management, including but not limited to ISO 11568 and 13491, ANSI X9.24 and X9.97, and NIST 140-2 Level 3
  - Public key infrastructure (PKI) and the role and operations of a Certification Authority (CA) and Registration Authority (RA)
  - Hardware security modules (HSMs) operations, policies, and procedures
  - POI key-injection systems and techniques including key-loading devices (KLDs) and key-management methods, such as Master/Session or DUKPT
  - Physical security techniques for high-security areas
  - Relevant PTS Security Requirements (e.g., SRED, SCR, OP)
  - POI integration software development, deployment and updates
  - PCI PTS authentication requirements for accessing account data or sensitive services

  Possess experience with and substantial knowledge of at least three of the following:

  - Modern, secure, embedded systems hardware and software architectures
  - PCI PTS quality and security management requirements related to POI software development
  - POI software authenticity and integrity verification techniques and self-tests
  - Attack methodologies through exploitation of logical vulnerabilities
  - Application penetration testing methodologies, to include use of forensic tools/methods, ability to exploit vulnerabilities, and ability to execute arbitrary code to test processes
- Attend annual P2PE Assessor Employee training provided by PCI SSC, and legitimately pass—of his or her own accord without any unauthorized assistance—all examinations conducted as part of training. If a P2PE Assessor Employee fails to pass any exam in connection with such training, the P2PE Assessor Employee must no longer perform or participate in P2PE Assessments until successfully passing all required exams on a future attempt.

- For new QSA (P2PE) Employee candidates, there are two training courses and corresponding exams: P2PE Fundamentals and QSA (P2PE). Candidates must achieve a passing grade in the P2PE Fundamentals exam before attempting the QSA (P2PE) exam.
- For new PA-QSA (P2PE) Employee candidates, there is an additional required training course and corresponding exam.

- Be employees of the P2PE Assessor Company (meaning this work cannot be subcontracted to non-employees) unless PCI SSC has given prior written consent for each subcontracted worker

In addition:

- Approved subcontractors are not permitted to include a company logo other than that of the responsible P2PE Assessor Company or any reference to another company in the P-ROV or attestation documents while performing work on behalf of the P2PE Assessor Company.
- If a P2PE Assessor Company is actively in process with a P2PE Assessment and loses its QSA (P2PE) Company or PA-QSA (P2PE) Company qualification or foundational QSA Company or PA-QSA Company qualification, it may be required to obtain the services of another QSA (P2PE) Company or PA-QSA (P2PE) Company (as applicable) to complete the P2PE Assessments and applicable PCI SSC review processes.

***Note:*** *Appendix C contains a list of all deliverables to be provided to PCI SSC to meet this requirement.*

### *3.2.2 Additional Requirements for PA-QSA (P2PE) Employees*

In addition to the requirements specified in Section 3.2.1 above, each PA-QSA (P2PE) Employee must:

- Be a PA-QSA Employee and comply with all applicable PA-QSA Requirements, including fulfillment of all requirements for PA-QSA Employees specified in the *PA-QSA Qualification Requirements*
- Have performed at least two PA-DSS Assessments as a PA-QSA Employee
- Possess experience with and substantial knowledge in each of the following:
  - Modern, secure, embedded systems hardware and software architectures
  - PCI PTS quality and security management requirements related to POI software development
  - POI software authenticity and integrity verification techniques and self-tests
  - Surrogate PAN-generation techniques, such as format-preserving encryption and tokenization
  - Attack methodology through exploitation of logical vulnerabilities
  - Application penetration testing methodologies, to include use of forensic tools/methods, ability to exploit vulnerabilities, and ability to execute arbitrary code to test processes

***Note:*** *Appendix C contains a list of all deliverables to be provided to PCI SSC to meet this requirement.*

# 4 P2PE Assessor Company Administrative Requirements

## 4.1 Contact Person

The P2PE Assessor Company must provide PCI SSC with contact information for each of the following:

- Primary contact person responsible for P2PE Assessments, and
- Secondary contact person responsible for oversight of quality assurance of P2PE Assessments

***Note:*** *Appendix B contains a list of all deliverables to be provided to PCI SSC to meet this requirement.*

## 4.2 Background Checks

Each P2PE Assessor Employee must meet all background check requirements as specified in the QSA Qualification Requirements.

## 4.3 P2PE Assessor Company Internal Quality Assurance

- The P2PE Assessor Company must have implemented a quality assurance program that covers and includes P2PE Assessment reviews, and must have documented such program in the company's quality assurance program manual (further described in the *QSA Qualification Requirements*), in each case, in a manner equivalent to the corresponding quality assurance requirements specified in the *QSA Qualification Requirements*.
- Each P2PE Assessment must follow the procedures documented in the *P2PE Program Guide.*
- The P2PE Assessor Company must provide a *QSA Feedback Form* (available on the Website) to each P2PE Assessment client at the beginning of each P2PE Assessment.

***Note:*** *Appendix B contains a list of all deliverables to be provided to PCI SSC to meet this requirement.*

## 4.4 Protection of Confidential and Sensitive Information

P2PE Assessor Companies must adhere to all applicable requirements to protect sensitive and confidential information, including but not limited to those required by PCI SSC pursuant to the *QSA Qualification Requirements.*

## 4.5 Evidence (Assessment Workpaper) Retention

P2PE Assessor Companies must meet all evidence-retention requirements as set forth in the *QSA Qualification Requirements* with respect to all P2PE Assessments and related work. Additionally, for a minimum of three (3) years the P2PE Assessor Company must secure (in accordance with 4.4 of the *QSA Qualification Requirements*) and maintain Assessment Results and Related Materials (defined in the QSA Agreement) substantiating all conclusions in the P-ROV, including but not limited to copies of any and all case logs, audit results, work papers, notes, and technical information created and/or obtained in connection with the applicable P2PE Assessment.

## 4.6 Security Incident Response

P2PE Assessor Companies must have and adhere to a documented process for notifying the applicable customer where breach of cardholder data in a customer's environment has or is suspected to have occurred, including but not limited to those required by PCI SSC pursuant to the *QSA Qualification Requirements.*

## 4.7 P2PE Assessor Company Recognition of Client's Validation Status

Where a P2PE Assessment is undertaken for the purposes of listing a P2PE Product on the Website, the P2PE Assessor Company must **not** provide (and must ensure that its P2PE Assessor Employees do not provide) any formal recognition of P2PE-validation status to a client until:

- PCI SSC has issued a corresponding P2PE Attestation of Validation for such P2PE Assessment signed by PCI SSC, to the P2PE Assessor Company, the corresponding P2PE Solution Provider, P2PE Component Provider, or P2PE Application Vendor (as applicable); **and**
- PCI SSC has included the P2PE Solution, P2PE Component, or P2PE Application (as applicable) on the applicable published list of validated P2PE Solutions, P2PE Components, or P2PE Applications.

***Note:*** *Appendix B contains a list of all deliverables to be provided to PCI SSC to meet this requirement.*

# 5 P2PE Assessor List and Annual Re-qualification

This section describes what happens after initial qualification, and activities related to annual re-qualification.

## 5.1 P2PE Assessor List

Once a company has met all applicable requirements specified in this document, it is added to the P2PE Assessor List on the Website, noting QSA (P2PE) Company and/or PA-QSA (P2PE) Company status as applicable.

Once an individual has met all applicable requirements specified in this document, PCI SSC will add such individual to the applicable P2PE Assessor Employee search tool on the Website.

Only those P2PE Assessor Companies and P2PE Assessor Employees identified on the P2PE Assessor List or in such search tool (as applicable) are authorized by PCI SSC to perform P2PE Solution Assessments and P2PE Component Assessments, and only those identified as PA-QSA (P2PE) Companies or PA-QSA (P2PE) Employees on the P2PE Assessor List or in such search tool (as applicable) are additionally authorized by PCI SSC to perform P2PE Application Assessments.

Companies that fail to meet application requirements will be notified, and will have 30 days to appeal PCI SSC's decision. All appeals must be addressed to the P2PE Program Manager at p2pe@pcisecuritystandards.org.

## 5.2 P2PE Assessor Annual Re-qualification

All P2PE Assessor Companies and P2PE Assessor Employees must be re-qualified by PCI SSC on an annual basis, based on original qualification date. Re-qualification requires payment of annual fees, successful completion of annual re-qualification training and training exams, and maintaining Good Standing status (for P2PE Assessor Program and all prerequisite PCI SSC programs).

All annual re-qualification fees (specified on the Website – *PCI SSC Programs Fee Schedule*) must be paid to PCI SSC during the re-qualification process, for both the P2PE Assessor Company and P2PE Assessor Employees.

# 6 Assessor Quality Management Program

Except as otherwise expressly provided below or established by PCI SSC from time to time, the Assessor Quality Management Program for the P2PE Assessor Program is part of, operated in the same manner as, and governed by the same terms, provisions, rules, requirements, policies, procedures, concepts, and mechanisms as the Assessor Quality Management Program described in the QSA Qualification Requirements (subject to appropriate adjustments to reflect specific program differences or terminology, as determined by PCI SCC in its sole discretion).

# Appendix A: Addendum to QSA Agreement for P2PE Assessor Companies

## A.1 Introduction

This Addendum to Qualified Security Assessor (QSA) Agreement for P2PE Assessor Companies, as amended and in effect from time to time (the "Addendum"), is entered into by and between PCI Security Standards Council, LLC ("PCI SSC") and the undersigned Applicant ("QSA") as of the date of PCI SSC's signature below (the "Addendum Effective Date"), for purposes of adding and modifying certain terms of the Qualified Security Assessor (QSA) Agreement between PCI SSC and QSA dated as of the QSA Agreement Date below, as in effect on the Addendum Effective Date (the "Agreement").

In consideration of the mutual covenants herein set forth, the adequacy and sufficiency of which is acknowledged, QSA and PCI SSC agree as follows.

## A.2 General Information

| **Applicant** | | | | | |
|---|---|---|---|---|---|
| Company Name: | | | | | |
| QSA Agreement Date: | | | | | |
| PA-QSA Addendum Date (if applicable): | | | | | |
| Location/Address: | | | | | |
| State/Province: | | Country: | | Postal Code: | |
| Regions Applying For (see Website for list): | | | | | |
| **Applicant's Signature** | | | | | |
| Applicant's Officer Name: | | Job Title: | | | |
| | | | | | |
| *Applicant's Officer Signature* ↑ | | | *Date* ↑ | | |

| **For PCI SSC Use Only:** | | | |
|---|---|---|---|
| Application Date: | | | |
| Application Approved: | | | |
| PCI SSC Officer Name: | | Job Title: | |
| | | | |
| *PCI SSC Officer Signature* ↑ | | | |

# A.3 Terms and Conditions

## A.3.1 Definitions

While this Addendum is in effect:

(a) Capitalized terms defined in this Addendum shall have the meanings ascribed to them herein for all purposes of this Addendum and the Agreement.

(b) Capitalized terms used in this Addendum without definition shall have the meanings ascribed to them in or pursuant to the Agreement or the *P2PE Qualification Requirements*, as applicable.

(c) The following terms shall have the following meanings:

(i) "P2PE Customer" means a P2PE Solution Provider, P2PE Component Provider, or P2PE Application Vendor for which QSA provides P2PE Services.

(ii) "P2PE Product" means a P2PE Solution, P2PE Component, or P2PE Application with respect to which QSA performs a P2PE Assessment.

(iii) "P2PE Services" means P2PE Assessments and any and all other services provided by QSA to its customers or PCI SSC in connection with this Addendum, the *P2PE Qualification Requirements*, or participation in the P2PE Assessor Program, other than TSP Services (as defined in and subject to the provisions of Schedule 1 hereto).

(iv) "Program Requirements" means all requirements and obligations of QSA pursuant to this Addendum, each other agreement entered into between QSA and PCI SSC, and any and all other applicable policies, procedures, requirements, standards, or obligations imposed, mandated, provided for, or otherwise established by PCI SSC from time to time in connection with any PCI SSC program in which QSA is a participant, including but not limited to all QSA Requirements, all QSA (P2PE) Requirements, all PA-QSA (P2PE) Requirements (if QSA has been qualified as a PA-QSA (P2PE)), and all policies, procedures, requirements, standards, or obligations of applicable PCI SSC training programs, quality assurance programs, remediation programs, program guides, and other related PCI Materials, including without limitation those relating to probation, fines, penalties, oversight, remediation, suspension, and/or revocation.

(d) The following terms appearing in the Agreement are hereby amended as follows:

(i) "QSA Requirements" shall include (without limitation) the Program Requirements.

(ii) "Report of Compliance," "ROC," and "Attestation of Compliance" shall, where applicable, include (without limitation) the terms "P2PE Report of Validation," "P-ROV," and "P2PE Attestation of Validation," respectively, as those terms are used in the *P2PE Qualification Requirements*.

(iii) "Services" shall include (without limitation) the P2PE Services.

(iv) "QSA Company clients" shall include (without limitation) P2PE Customers.

## A.3.2 P2PE Services

(a) Subject to the terms and conditions of this Addendum and the Agreement, for P2PE Assessor Program purposes, PCI SSC hereby approves QSA to: (i) while QSA is in Good Standing (or in compliance with the terms of remediation) as a QSA (P2PE) Company or PA-QSA (P2PE) Company, conduct P2PE Solution Assessments and/or P2PE Component Assessments for P2PE Customers solely in order to validate compliance of P2PE Solutions and/or P2PE Components with the P2PE Standard and (ii) while QSA is in Good Standing (or in compliance with the terms of remediation) as a PA-QSA (P2PE) Company, conduct P2PE Assessments (including but not limited

to P2PE Application Assessments) for P2PE Customers in order to validate compliance with the P2PE Standard. Notwithstanding the foregoing, QSA agrees that QSA shall not recognize a given P2PE Product as validated under the P2PE Standard unless (A) the corresponding P2PE Customer has signed an applicable P2PE Vendor Release Agreement ("VRA") on the form approved by PCI SSC, (B) PCI SSC has notified QSA and such P2PE Customer of such validation via P2PE Attestation of Validation or other applicable Acceptance (defined in the P2PE Program Guide) letter signed by PCI SSC, and (C) such P2PE Product is at the time listed on PCI SSC's applicable published registry of P2PE validated P2PE Products. Except with respect to merchant-managed solutions (as defined in the P2PE Program Guide), under no circumstances shall QSA recognize, state, or imply (or permit any of its P2PE Customers to recognize, state, or imply) that any version of any product, device, payment application, component, service, or solution is then validated under the P2PE Standard, other than those versions that, at such time, satisfy each of the requirements of the preceding sentence.

(b) QSA agrees to monitor the Website at least weekly for changes to the Program Requirements and PCI SSC Standards that are relevant to each PCI SSC Assessment and PCI SSC Program in which QSA participates. QSA will incorporate all such changes into all such PCI SSC Assessments initiated on or after the effective date of such changes. QSA acknowledges that any P-ROV or other report regarding any PCI SSC Assessment that is not conducted in accordance with the relevant Program Requirements and PCI SSC Standards as in effect at the initiation date of such PCI SSC Assessment may be rejected.

(c) QSA will include along with each P-ROV submitted to PCI SSC a P2PE Attestation of Validation in the form available through the Website signed by a duly authorized officer of QSA, in which QSA certifies without qualification that (i) in performing the applicable P2PE Assessment, QSA followed the P2PE Standard and *P2PE Qualification Requirements* without deviation and (b) application of such requirements and procedures did not indicate any conditions of non-compliance with the P2PE Standard other than those expressly noted in the P-ROV.

## A.4 Term and Termination

### A.4.1 Term

This Addendum shall become effective as of the Addendum Effective Date and, unless earlier terminated in accordance with the Agreement, shall continue for an initial term of one (1) year, and thereafter shall renew for additional subsequent terms of one year, subject to QSA's successful completion of qualification and re-qualification requirements for each such one-year term (each a "Contract Year"). This Addendum shall immediately terminate upon termination of the Agreement.

### A.4.2 Effect of Termination

Upon any termination or expiration of this Addendum: (i) QSA will no longer be identified as a P2PE Assessor Company on the QSA List; (ii) QSA shall immediately cease all advertising and promotion of its status as a P2PE Assessor Company; (iii) QSA shall immediately cease soliciting for and performing all Services (including but not limited to processing of P-ROVs and TSP Services) hereunder, provided that, if and to the extent instructed by PCI SSC in writing, QSA shall complete any and all such Services for which QSA was engaged prior to such expiration or termination; (iv) to the extent QSA is instructed to complete any such Services pursuant to preceding clause (iii), QSA will deliver all corresponding outstanding P-ROVs and other reports within the time contracted with the applicable client or customer of QSA; (v) QSA shall remain responsible for all of the obligations, representations, and warranties hereunder with respect to all P-ROVs submitted to PCI SSC; (vi) if requested by PCI SSC, QSA shall obtain (at QSA's sole cost and expense) the services of a replacement P2PE Assessor Company

acceptable to PCI SSC for purposes of completing those Services hereunder for which QSA was engaged prior to such expiration or termination but which QSA has not been instructed to complete pursuant to clause (iii) above; (vii) QSA shall return or destroy, in accordance with the terms of Section A.6 of the Agreement, all PCI SSC and third-party property and Confidential Information obtained in connection with this Addendum and the performance of any Services hereunder; (viii) QSA shall, within fifteen (15) days of PCI SSC's written request, in a manner acceptable to PCI SSC, notify those of its clients or customers with which QSA is then engaged to perform Services hereunder of such expiration or termination; and (ix) notwithstanding anything to the contrary in this Addendum, the Agreement or elsewhere, PCI SSC may notify any of its Members and any acquirers, QSA P2PE Customers, or others of such expiration or termination and the reason(s) therefore. The provisions of this Section A.4.2 shall survive the expiration or termination of this Addendum for any or no reason.

## A.5 General Terms

While this Addendum is in effect, the terms and conditions set forth herein and in Schedule 1 hereto (which Schedule 1 is hereby incorporated into and made a part of this Addendum) shall be deemed incorporated into and a part of the Agreement. This Addendum may be signed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. Except as expressly modified by this Addendum or hereafter by the parties in accordance with its terms, the Agreement, as modified and in effect immediately prior to the effectiveness of this Addendum, shall remain in full force and effect in accordance with its terms.

**Schedule 1**

**TSP Services**

To the extent QSA engages in TSP Services on or after the date of the effectiveness of the provisions of this Schedule 1 (the "Schedule Effective Date"), the following additional provisions shall apply:

1. Definitions.

(a) "TDE" means "Token Data Environment", as further described in the *TSP Requirements*.

(b) "TSP" means "Token Service Provider", as further described in the *TSP Requirements*. A TSP is deemed to be a QSA Company client for purposes of the Agreement and a client and customer of QSA for purposes of the *QSA Qualification Requirements* and *P2PE Qualification Requirements*.

(c) "TSP Assessment" means an assessment of a TDE of a TSP in order to validate compliance with the *TSP Requirements* as part of the P2PE Assessor Program. A TSP Assessment is deemed to be a PCI SSC Assessment for purposes of the *QSA Qualification Requirements* and the Agreement, and a P2PE Assessment for purposes of Sections 3.1, 3.2 (introduction), 3.2.1, 4.1 and 4.3 of the *P2PE Qualification Requirements*.

(d) "*TSP Requirements*" means the then-current version of (or successor document to) the *Payment Card Industry (PCI) Token Service Providers Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens)*, as from time to time amended and made available on the Website. The *TSP Requirements* are deemed to be a PCI SSC Standard for purposes of the Agreement and *QSA Qualification Requirements*, and part of the Program Requirements for purposes of the Addendum and *P2PE Qualification Requirements*.

(d) "TSP Services" means TSP Assessments and any and all other services provided by QSA to its clients or customers or PCI SSC in connection with TSP Assessments, this Schedule 1 or the *TSP Requirements*. The TSP Services are deemed to be part of the Services for purposes of the Agreement.

2. TSP Services. Subject to the terms and conditions of this Schedule 1, the Addendum, and the Agreement, and to QSA's compliance with all applicable Program Requirements relating to the performance of TSP Assessments:

(a) QSA is hereby authorized to conduct TSP Assessments for TSPs solely in order to validate the compliance of the TDE(s) of such TSPs with the *TSP Requirements*.

(b) QSA shall perform each TSP Assessment in accordance with the *TSP Requirements* and applicable Program Requirements, including but not limited to (i) documenting each TSP Assessment in a report using (and in accordance with the instructions for) the corresponding TSP Report on Compliance template available on the Website (each a "TSP Report") and (ii) preparing each such TSP Report in accordance with applicable Program Requirements and based on evidence obtained by following the *TSP Requirements*.

(c) Under no circumstances shall QSA (i) recognize, state, or imply (or permit any of its TSP clients or customers to recognize, state, or imply) that a given TDE is or has been validated under the *TSP Requirements* when such statement is incorrect or may be misleading or (ii) for purposes of any PCI SSC Program, conduct any TSP Assessment of any TDE of any entity that QSA controls, is controlled by, is under common control with, or in which QSA holds any investment.

(d) Only P2PE Assessor Companies and P2PE Assessor Employees identified on the P2PE Assessor List or in the applicable search tool on the Website (as applicable) are authorized by PCI SSC to perform TSP Assessments.

(e) To the extent QSA is in remediation as a QSA Company or P2PE Assessor Company but otherwise satisfies the requirements of Sections 1.3(a) through 1.3(e) of the *P2PE Qualification Requirements*, QSA shall nonetheless be permitted to perform TSP Assessments.

3. QSA and PCI SSC each acknowledge and agree that, as of the Schedule Effective Date, PCI SSC does not intend to perform quality assurance reviews of TSP Assessments, "Accept" or require the submission of corresponding TSP Reports to PCI SSC, or "list" or otherwise designate TDEs that have been validated against the *TSP Requirements* on the Website. Accordingly, as of the Schedule Effective Date, the corresponding provisions of the Addendum, Agreement, *QSA Qualification Requirements*, *P2PE Qualification Requirements*, and *P2PE Program Guide*, as such provisions would otherwise relate to such TSP Assessment reviews, "Acceptance", required submissions, "listings" or designations, generally are not intended to apply in connection with TSP Assessments. Notwithstanding the foregoing, however, PCI SSC hereby expressly reserves all rights with respect to the foregoing, including without limitation, the right to (a) perform such quality assurance reviews and, upon notice to QSA, require QSA to cooperate with and make required submissions of TSP Reports and related TSP Assessment materials and work papers to PCI SSC in connection with such reviews (and QSA hereby agrees to so cooperate comply with all such reviews and requirements), and (b) offer remediation and/or revoke any QSA Company qualification or QSA Employee qualification in connection with any breach or other failure to satisfy any applicable Program Requirements.

# Appendix B: P2PE Assessor Company – Application

| Applicant QSA Company (the "Company") Information | | | | | |
|---|---|---|---|---|---|
| Company Name: | | | | | |
| **Primary Contact Name:** | | Job Title: | | | |
| Telephone: | | E-mail: | | | |
| Business Address: | | City: | | | |
| State/Province: | | Country: | | ZIP: | |
| URL: | | | | | |
| **QA Contact Name:** | | Job Title: | | | |
| Telephone: | | E-mail: | | | |
| Business Address: | | City: | | | |
| State/Province: | | Country: | | ZIP: | |
| **Secondary Contact Name:** | | Job Title: | | | |
| Telephone: | | E-mail: | | | |
| Business Address: | | City: | | | |
| State/Province: | | Country: | | ZIP: | |

☐ The Company acknowledges and agrees that in order to participate as a P2PE Assessor Company in the P2PE Assessor Program, it must satisfy all of the requirements specified in the P2PE Qualification Requirements and supporting documents.

In addition to all QSA requirements specified in the *QSA Qualification Requirements*, each P2PE Assessor Company must meet all P2PE Assessor Requirements applicable to QSA (P2PE) Companies, including but not limited to the requirements set forth in this application. Each applicant P2PE Assessor Company must complete the following:

## 3.1 P2PE Assessor Company Services and Experience

***Note:*** *These sections are intended to draw out specific experience about the company. The company must provide examples (including the timeframe) of how its work experience meets the P2PE Assessor Program requirements.'*

**3.1.1.A** Provide a description of clients and dates for two previous PCI DSS Assessments performed by the Company in its capacity as a QSA Company.

***Note:*** *Only PCI DSS Assessments performed by the applicant P2PE Assessor Company are eligible to meet this requirement; PCI DSS Assessments performed by a QSA Employee for another QSA Company will not be considered toward this requirement.*

| Client: | From (date): | To (date): |
|---|---|---|
| Client: | From (date): | To (date): |

**3.1.1.B Knowledge of cryptographic techniques including cryptographic algorithms, key management, and key lifecycle:**

*Describe the company's knowledge and expertise of cryptographic techniques and the Company's role ((e.g., implementation, developer, management, etc.). For example, the types of cryptography, such as hashing, symmetric, asymmetric; the algorithms, such as Diffie-Hellman, elliptic curve, DES, Blowfish, MD5; key management implementations or assessments including descriptions of how keys are stored, access privileges, expected incident response when/if keys were compromised; and lifecycle management (rotation, destruction, revocation).*

Total time: Years Months

**Knowledge of industry standards for cryptographic techniques and key management, including but not limited to ISO 11568 and 13491, ANSI X9.24 and X9.97, and NIST 140-2 Level 3:**

*Describe the Company's expertise and direct responsibility for implementing, operating, and/or assessing cryptographic systems and/or key management functions. For example, implementing and managing key-management functions, or performing lab evaluations of cryptographic systems against NIST, ANSI, or ISO standards.*

Total time: Years Months

**Knowledge of Public Key Infrastructure (PKI) and the role and operations of a Certification Authority (CA) and Registration Authority (RA):**

*Describe the Company's expertise with digital certificates. For example, obtaining, generating, and deploying digital certificates, methods to protect or store digital certificates, certificate revocation, etc.*

Total time: Years Months

**Knowledge of Hardware Security Modules (HSMs) operations, policies, and procedures:**

*Describe the Company's expertise with HSMs. For example, HSM configuration, deployment, use, and developing related policies/procedures.*

Total time: Years Months

**Knowledge of POI key-injection systems and techniques including Key Loading Devices (KLDs) and key management methods, such as "Master/Session Key," "DUKPT":**

*Describe the Company's expertise with key injection. For example, types of keys loaded, KLDs, key management methods, etc.*

Total time: Years Months

**Knowledge of physical security techniques for high-security areas:**

*Describe the Company's expertise with physically securing systems and rooms such as badge systems, entry logs, man-traps, physical keys, etc.*

Total time: Years Months

**Knowledge of relevant PTS Security Requirements (e.g., SRED, SCR, OP):**

*Describe the Company's expertise with SRED, SCR, and/or OP including the type(s) of devices configured to or tested against the Standard.*

Total time: Years Months

**POI integration software development, deployment, and updates:**

*Describe any software and related functionality that the Company has experience developing. For example, language(s) used, software deployment, POI integration, platforms, databases, and operating systems with which the Company has expertise, etc.*

Total time: Years Months

**PCI PTS authentication requirements for accessing account data or sensitive services:**

*Describe the Company's knowledge or expertise with verifying PTS device authentication. For example, data or services with which the Company has knowledge or expertise testing to ensure that PTS authentication requirements were met.*

Total time: Years Months

| |
|---|
| **Knowledge of modern, secure embedded systems hardware and software architectures:**<br>*Describe the Company's knowledge or expertise with secure embedded systems architectures. For example, operating systems configured, functionality of software written or installed, hardware implemented, etc.*<br><br>Total time: Years Months |
| **Knowledge of PCI PTS quality and security management requirements related to POI software development:**<br>*Describe the Company's knowledge or expertise with POI software development quality assurance measures. For example, managing security during POI software development.*<br><br>Total time: Years Months |
| **Knowledge of POI software authenticity and integrity verification techniques and self-tests:**<br>*Describe the Company's knowledge or expertise with tools and techniques to validate the authenticity of POI software. For example, how POI software integrity is verified and how self-testing of a device is observed.*<br><br>Total time: Years Months |
| **Knowledge of attack methodologies through exploitation of logical vulnerabilities:**<br>*Describe the Company's expertise with various attack methods and vulnerability exploitation.*<br><br>Total time: Years Months |
| **Knowledge of application penetration testing methodologies, to include use of forensic tools/methods, ability to exploit vulnerabilities, and ability to execute arbitrary code to test processes:**<br>*Describe the Company's expertise exploiting vulnerabilities. For example, methods employed to exploit vulnerabilities, penetration tests performed at the application layer and use of arbitrary code during testing.*<br><br>Total time: Years Months |
| **3.1.1.C Company acknowledgements** |
| ☐ The Company acknowledges and agrees that all of the above skill sets will be present and fully utilized on every P2PE Assessment. |
| ☐ The Company acknowledges and agrees that in order to perform or manage any P2PE Assessment it must be qualified by PCI SSC as, and in Good Standing or in compliance with remediation as, both a QSA Company and a QSA (P2PE) Company. |
| ☐ The Company acknowledges and agrees that it must fulfill all QSA Qualification Requirements, all QSA (P2PE) Company Requirements, and comply with all terms and provisions of the QSA Agreement, the P2PE Assessor Addendum, any other agreements executed with PCI SSC, and all other applicable policies and requirements of the P2PE Assessor Program, as mandated or imposed by PCI SSC from time to time, including but not limited to all requirements in connection with PCI SSC's quality assurance initiatives, remediation, and revocation. |

**3.1.1.C Company acknowledgements**
*(continued)*

☐ The Company acknowledges and agrees that it must 1.) adhere to all quality assurance requirements described in the P2PE Assessor Qualification Requirements and supporting documentation, 2.) have a quality assurance program documented in its quality assurance manual, and 3.) maintain and adhere to the documented quality assurance process and quality assurance program manual that addresses (at a minimum) the following:

- Oversight of quality assurance for all P2PE Assessments, including reviews of performed audit procedures, supporting documentation, and information documented in the P-ROV related to the appropriate selection of system components, sampling procedures, proper use of payment definitions, consistent findings, and documentation of results
- Overview of the P-ROV review processes, including roles and responsibilities
- Responsibilities for review of all P-ROVs for quality assurance purposes
- Responsibilities for approval of all P-ROVs prior to submission to PCI SSC
- Responsibilities for submitting P-ROVs to PCI SSC
- A requirement that all P2PE Assessor Employees must adhere to the P2PE Standard and all applicable P2PE Assessor Requirements
- Evidence-retention policy and procedures including physical, electronic, and procedural safeguards consistent with industry-accepted standards for the retention of sensitive and confidential information obtained during the course of P2PE Assessments (consistent with Sections 4.4 and 4.5 of *QSA Qualification Requirements*)

☐ Where a P2PE Assessment is undertaken for the purposes of listing a P2PE Product on the Website, the Company acknowledges and agrees (by signing the *P2PE Assessor Addendum*) that it will not (and will ensure that its P2PE Assessor Employees do not) recognize the validation status of a given P2PE Solution, P2PE Component, or P2PE Application assessed by such P2PE Assessor Company until PCI SSC has notified the P2PE Assessor Company, the corresponding P2PE Solution Provider, the P2PE Component Provider (if applicable), and the P2PE Application Vendor (if applicable), via P2PE Attestation of Validation, and such P2PE Solution, P2PE Component(s) (if applicable), and P2PE Application(s) (if applicable) are listed on the applicable registry of validated P2PE Solutions on the Website.

*P2PE Assessor Addendum* signed: ☐ Yes ☐ No

## 3.1.2 Additional Deliverables for PA-QSA (P2PE) Companies

**3.1.2.A** Description of clients and dates for two previous PCI PA-DSS Assessments performed by the Company in its capacity as a PA-QSA Company.
***Note:*** *PA-DSS Assessments performed by a current PA-QSA Employee for another PA-QSA Company will not be considered toward this requirement*.

| | | |
|---|---|---|
| Client: | From (date): | To (date): |
| Client: | From (date): | To (date): |

**3.1.2.B** Description of the Company's relevant areas of specialization in understanding:

**Surrogate PAN generation techniques, such as format-preserving encryption and tokenization:**

*Describe any knowledge or expertise the Company has with surrogate PANs generation techniques, including the Company's role and specifics about the techniques implemented or reviewed.*

Total time: Years Months

**3.1.2.C** Attestation that all of the above skill sets will be present and fully utilized on every P2PE Application Assessment:

☐ The Company acknowledges and agrees that all of the above skill sets will be present and fully utilized on every P2PE Assessment.

| **3.1.2.D** Two client references from relevant security engagements within the last 12 months: | | | |
|---|---|---|---|
| Client Company Name: | | From (date): | To (date): |
| Contact Name: | | Job Title: | |
| Telephone *or* e-mail: | | | |
| State/Province: | | Country: | |
| | | | |
| Client Company Name: | | From (date): | To (date): |
| Contact Name: | | Job Title: | |
| Telephone *or* e-mail: | | | |
| State/Province: | | Country: | |

# Appendix C: P2PE Assessor Employee – Application

| P2PE Assessor Company and Employee Information | | | | | |
|---|---|---|---|---|---|
| Applicant ("Company") Name: | | | | | |
| Employee ("Candidate") Name: | | Job Title: | | | |
| Telephone: | | E-mail: | | | |
| Business Address: | | City: | | | |
| State/Province: | | Country: | | ZIP: | |
| URL: | | | | | |

In addition to all requirements applicable to QSA Employees pursuant to the QSA Qualification Requirements, each P2PE Assessor Employee must meet all requirements applicable to QSA (P2PE) Employees pursuant to the P2PE Qualification Requirements, including but not limited to the requirements set forth in this application. Each applicant P2PE Assessor Employee must complete the following:

## 3.2 P2PE Assessor Employee – Skills and Experience

*Note: These sections are intended to draw out specific experience from the Candidate. The Candidate must provide examples (including the timeframe) of how his or her knowledge and work experience meets the P2PE Assessor Program requirements. These sections are intended to measure the Candidate's skills against the required skills.*

| **3.2.1.A** Provide a description of clients and duties performed for two previous PCI DSS Assessments performed by the Candidate – include dates for each: | | |
|---|---|---|
| Client: | From (date): | To (date): |
| Description of work/specific duties performed: | | |
| Client: | From (date): | To (date): |
| Description of work/specific duties performed: | | |

**3.2.1.B** Provide examples of work or a description of the Candidate's experience with cryptography and key management (at least one year total within the past 10 years) in cryptographic techniques including cryptographic algorithms, key management, and key lifecycle:

**Examples of work or description of the Candidate's experience with *cryptographic algorithms*:**

*Describe the types of cryptography the Candidate has used, such as hashing, symmetric, asymmetric, and algorithms used such as Diffie-Hellman, elliptic curve, DES, Blowfish, MD5.*

From (date): To (date): Total time: Years Months

**Examples of work or description of the Candidate's experience with *key management*:**

*Describe the Candidate's knowledge of implementing key management, for example, key storage, access control, incident response in the event of compromise, and lifecycle management (rotation, destruction, revocation).*

From (date): To (date): Total time: Years Months

**Description of the Candidate's experience with or knowledge of any other cryptographic techniques:**

From (date): To (date): Total time: Years Months

**3.2.1.C** Provide examples of work or a description of the Candidate's knowledge and experience with cryptography and key management with a minimum of one year (total) in ***at least four*** of the following disciplines:

| |
|---|
| **Knowledge of industry standards for cryptographic techniques and key management, including but not limited to ISO 11568 and 13491, ANSI X9.24 and X9.97, and NIST 140-2 Level 3:**<br>*Describe specific standards with which the Candidate has knowledge and/or experience and how they were used to design solutions, test for compliance, etc.*<br><br>Total time: Years Months |
| **Knowledge of Public Key Infrastructure (PKI) and the role and operations of a Certification Authority (CA) and Registration Authority (RA):**<br>*Describe the Candidate's experience with digital certificates. For example, obtaining, generating, and deploying digital certificates, methods to protect or store digital certificates, certificate revocation, etc.*<br><br>Total time: Years Months |
| **Knowledge of Hardware Security Modules (HSMs) operations, policies, and procedures:**<br>*Describe the Candidate's experience with HSMs. For example, HSM configuration, deployment, use, and developing related policies and procedures.*<br><br>Total time: Years Months |
| **Knowledge of POI key-injection systems and techniques including Key Loading Devices (KLDs) and key management methods, such as "Master/Session Key," "DUKPT":**<br>*Describe the Candidate's experience with key injection. For example, types of keys loaded, KLDs, key management methods, etc.*<br><br>Total time: Years Months |
| **Knowledge of physical security techniques for high-security areas:**<br>*Describe the Candidate's experience with physically securing systems and rooms. For example, badge systems, entry logs, man-traps, physical keys, etc.*<br><br>Total time: Years Months |
| **Knowledge of relevant PTS Security Requirements (e.g., SRED, SCR, OP):**<br>*Describe the Candidate's experience with SRED, SCR, and/or OP including the type(s) of devices configured to or tested against the Standard.*<br><br>Total time: Years Months |
| **Provide examples of work or a description of the Candidate's experience *in each of the following*:** |
| **POI integration software development, deployment, and updates:**<br>*Describe the Candidate's software development experience. For example, language(s) used, software deployment, POI integration, platforms, databases, and operating systems with which the Candidate has experience, etc.*<br><br>Total time: Years Months |
| **PCI PTS authentication requirements for accessing account data or sensitive services:**<br>*Describe the Candidate's experience with verifying PTS device authentication. For example, data or services with which the Candidate has knowledge and experience testing to ensure that PTS authentication requirements were met.*<br><br>Total time: Years Months |

| **Provide examples of work or a description of the Candidate's experience in *at least three* of the following:** |
|---|
| **Knowledge of modern, secure embedded systems hardware and software architectures:**<br>*Describe the Candidate's knowledge and experience with secure embedded systems architectures. For example, operating systems configured, functionality of software written or installed, hardware implemented, etc.*<br><br>Total time: Years Months |
| **Knowledge of PCI PTS quality and security management requirements related to POI software development:**<br>*Describe the Candidate's knowledge and experience with POI software development quality assurance measures. For example, managing security during POI software development.*<br><br>Total time: Years Months |
| **Knowledge of POI software authenticity and integrity verification techniques and self-tests:**<br>*Describe the Candidate's knowledge and experience with tools and techniques to validate the authenticity of POI software. For example, how POI software integrity is verified and how self-testing of a device is observed.*<br><br>Total time: Years Months |
| **Knowledge of attack methodologies through exploitation of logical vulnerabilities:**<br>*Describe the Candidate's knowledge and experience with various attack methods and vulnerability exploitation.*<br><br>Total time: Years Months |
| **Knowledge of application penetration testing methodologies, to *include* use of forensic tools/methods, ability to exploit vulnerabilities, and ability to execute arbitrary code to test processes:**<br>*Describe the Candidate's knowledge and experience with application-layer penetration testing. For example, tools and methods employed to exploit vulnerabilities and use of arbitrary code during testing.*<br><br>Total time: Years Months |

| **3.2.1.D** A current copy of the Candidate's resume or Curriculum Vitae |
|---|
| *Paste text into the field provided below or transmit the file separately from this form.* |

| **3.2.2 Additional expertise – PA-QSA (P2PE) Employee Candidates only** | | |
|---|---|---|
| **3.2.2.A** Provide a description of clients and duties performed for two previous PA-DSS Assessments performed by the Candidate – include dates for each. | | |
| Client: | From (date): | To (date): |
| Description of work/specific duties performed: | | |
| Client: | From (date): | To (date): |
| Description of work/specific duties performed: | | |

| **3.2.2.B** Provide examples of work or a description of the Candidate's additional expertise with the following: |
|---|
| **Surrogate PAN-generation techniques, such as format-preserving encryption and tokenization:**<br>*Describe any knowledge or experience the Candidate has with surrogate PANs generation techniques, including the Candidate's role and specifics about the techniques implemented or reviewed.*<br><br>Total time: Years Months |

# Appendix D: Types of P2PE Assessor Companies and Applicability to the P2PE Standard

### QSA (P2PE) Company

- Can assess all P2PE Domains, excluding P2PE Domain 2.

### PA-QSA (P2PE) Company

- Can assess all P2PE Domains.

| Domain | QSA (P2PE) Company | PA-QSA (P2PE) Company |
|---|---|---|
| Domain 1 | **Yes** | **Yes** |
| Domain 2 | **No** | **Yes** |
| Domain 3 | **Yes** | **Yes** |
| Domain 4 | **Yes** | **Yes** |
| Domain 5 | **Yes** | **Yes** |
| Domain 6 | **Yes** | **Yes** |