Payment Card Industry (PCI)
Data Security Standard
QSA Qualification Requirements

Supplement for Point-to-Point Encryption
Qualified Security Assessors –
QSA (P2PE) and PA-QSA (P2PE)

Version 1.0
January 2012

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 (defined below) 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 (defined below).

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 such P2PE Solutions. As with all other PCI SSC standards, any mandates, regulations, or rules regarding compliance with these requirements are provided by the participating payment brands.

This *Supplement for Point-to-Point Encryption Qualified Security Assessors (QSA (P2PE) and PA-QSA (P2PE))* (the "P2PE Assessor Supplement") supplements the QSA Qualification Requirements (defined below) for each Qualified Security Assessor ("QSA") company that intends to qualify as a P2PE Assessor (defined below), and describes the minimum qualification requirements and related documentation that a P2PE Assessor must satisfy and provide to PCI SSC in order to qualify to perform P2PE Assessments (defined below) as a participant in the P2PE Assessor program described herein (the "P2PE Assessor Program").

1.1 Terminology

Note that throughout this P2PE Assessor Supplement, the following terms shall have the following meanings.

Term	Meaning
P2PE or P2PE Standard	The then-current versions of (or successor documents to) each component of PCI SSC's solution requirements and assessment procedures for Point-to-Point Encryption, including but not limited to the *Payment Card Industry (PCI) Point-to-Point Encryption Solution Requirements and Assessment Procedures,* any and all appendices, exhibits, schedules, and attachments to any of the foregoing and all materials incorporated therein, in each case, as from time to time amended and made available on the Website.
P2PE Application	An application that is included in a P2PE Solution and is intended for use on a merchant PIN transaction security (PTS) point-of-interaction (POI) device or otherwise by a merchant.
P2PE Application Assessment	Assessment of a P2PE Application in order to validate that such P2PE Application adheres to all P2PE Domain 2 requirements.
P2PE Application Vendor	A software vendor that develops and then sells, distributes, or licenses to any third party any P2PE Application.
P2PE Assessment	Assessment of a P2PE Solution in order to validate compliance with the P2PE Standard as part of the P2PE Assessor Program, and with respect a given PA-QSA (P2PE), includes P2PE Application Assessments of P2PE Applications incorporated into or a part of the P2PE Solutions assessed by such PA-QSA (P2PE).

Term	Meaning
P2PE Assessor	A company qualified by PCI SSC as either a QSA (P2PE) or a PA-QSA (P2PE). Subject to the applicable requirements and restrictions of the P2PE Assessor Supplement and program policies and procedures, P2PE Assessors are qualified by PCI SSC to evaluate P2PE Solutions (and with respect to PA-QSA (P2PE)s, perform P2PE Application Assessments) and submit corresponding P-ROVs on behalf of the applicable P2PE Solution Providers (and with respect to PA-QSA (P2PE)s, the applicable P2PE Application Vendors) directly to PCI SSC for review and acceptance.
P2PE Assessor Addendum	The *Addendum to Qualified Security Assessor (QSA) Agreement for P2PE Assessors* in the form attached as *Appendix A* to the P2PE Assessor Supplement.
P2PE Assessor Employee	Any QSA (P2PE) Employee or PA-QSA (P2PE) Employee.
P2PE Component	A P2PE Application or a device that stores, processes, or transmits payment cardholder data as part of payment authorization or settlement and that is incorporated into or a part of any P2PE Solution.
P2PE Component Vendor	A software or device vendor that develops and then sells, distributes, or licenses to any third party any P2PE Component.
P2PE Domain Requirements	All requirements of the P2PE Standard.
P2PE Domain 2 Requirements	The requirements of the P2PE Standard applicable to P2PE Applications.
P2PE Non-Domain 2 Requirements	P2PE Domain requirements other than P2PE Domain 2 requirements.
P2PE Solution	A point-to-point encryption solution consisting of a point-to-point encryption environment, the configuration and design thereof, and the P2PE Components that are incorporated into, a part of, or interact with such environment.
P2PE Solution Provider	A third-party entity (for example, a processor, acquirer, or payment gateway) that has overall responsibility for the design and implementation of a P2PE Solution for a specific point-to-point encryption implementation, and may (directly, or indirectly through outsourcing) manage P2PE Solutions for its customers and/or manage or perform corresponding responsibilities.
P2PE Vendor Release Agreement	The then-current and applicable form of release agreement that PCI SSC: (a) Requires to be executed by P2PE Solution Providers and/or P2PE Application Vendors (as applicable) in connection with the P2PE Assessor Program, and (b) Makes available on the Website.

Term	Meaning
Payment Application Qualified Security Assessor for Point-to-Point Encryption, or PA-QSA (P2PE)	A PA-QSA company that: (a) Is qualified by PCI SSC to provide services to P2PE Solution Providers and/or P2PE Application Vendors in order to validate that such providers' or vendors' P2PE Solutions and/or P2PE Applications adhere to any and all aspects of the P2PE Standard, including but not limited to, validation that payment applications, when incorporated into or used as part of a P2PE Solution, adhere to all P2PE Domain 2 requirements; and (b) Remains in Good Standing (as defined in Section 1.3 below) as a PA-QSA (P2PE).
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 Supplement.
PA-QSA Supplement	The *Payment Card Industry – Qualified Security Assessor Supplement 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) Employee	An individual employed by a PA-QSA (P2PE) who has satisfied, and continues to satisfy, all PA-QSA (P2PE) Requirements applicable to employees of PA-QSA (P2PE)s who will conduct P2PE Assessments, as described in further detail herein.
PA-QSA (P2PE) Requirements	The requirements and obligations generally applicable to all PA-QSA (P2PE)s as provided for in the P2PE Assessor Supplement, 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)s 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.
P-ROV	A "P2PE Report on Validation" completed by a P2PE Assessor company and submitted directly to PCI SSC for review and acceptance of a P2PE Solution and/or P2PE Application.
QSA Agreement	The *PCI 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 Validation Requirements for Qualified Security Assessors (QSA)* (or successor document), as from time to time amended and made available on the Website.
QSA Requirements	With respect to a given QSA, the requirements and obligations of the QSA pursuant to the *QSA Qualification Requirements*, the *QSA Agreement,* and each addendum, supplement, and other agreement entered into between the QSA and PCI SSC, and any and all other policies, procedures, requirements 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 the QSA is then a participant. These include but are not limited to the requirements of all applicable PCI SSC training programs, quality assurance and remediation programs, program guides, and other related PCI SSC program materials.

Term	Meaning
QSA (P2PE) Employee	An individual employed by a QSA (P2PE) who has satisfied, and continues to satisfy, all QSA (P2PE) Requirements applicable to employees of QSA (P2PE)s who will conduct P2PE Assessments, as described in further detail herein.
QSA (P2PE) Requirements	The requirements and obligations generally applicable to all QSA (P2PE)s as provided for in the P2PE Assessor Supplement, 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)s 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.
Qualified Security Assessor for Point-to-Point Encryption or QSA (P2PE)	A QSA company that: (a) Is qualified by PCI SSC to provide services to P2PE Solution Providers in order to validate that such providers' P2PE Solutions adhere to P2PE non-Domain 2 requirements and (b) Remains in Good Standing (as defined in Section 1.3 below) as a QSA (P2PE).
Website	The then-current PCI SSC web site, which is currently available at http://www.pcisecuritystandards.org.

All capitalized terms used in this P2PE Assessor Supplement without definition shall have the meanings specified in the *QSA Qualification Requirements* or the *QSA Agreement*, as applicable, and if not defined therein, then in the relevant PCI SSC program materials.

1.2 Goal

As described further in Section 1.3 below, in order to qualify and remain in Good Standing as a P2PE Assessor, a P2PE Assessor must, among other things:

- Meet or exceed and then continue to satisfy all applicable requirements of the P2PE Assessor Supplement and the P2PE Assessor Addendum, and
- Have an effective P2PE Assessor Addendum in the form attached hereto as *Appendix A* in place with PCI SSC.

To qualify and remain in Good Standing as a PA-QSA (P2PE), a PA-QSA (P2PE) must, among other things

- Be in PA-QSA Good Standing (as defined in the PA-QSA Addendum) and
- Have an effective PA-QSA Addendum in place with PCI SSC.

Together, the QSA Requirements, the QSA (P2PE) Requirements—and for PA-QSA (P2PE)s, the PA-QSA (P2PE) Requirements and PA-QSA Requirements (as defined in the PA-QSA Supplement)—are intended to serve as a qualification baseline for all P2PE Assessors and provide a transparent process for P2PE Assessor qualification and re-qualification across the payment industry.

1.3 Qualification Process Overview

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

Companies qualified by PCI SSC as QSA (P2PE)s or PA-QSA (P2PE)s will be identified as such on the Council's web-based registry (the "P2PE Assessor List") in accordance with the P2PE Assessor Addendum for a period of one (1) year from the date of such qualification. If a company is not so identified, its work product as a QSA (P2PE) and/or PA-QSA (P2PE) (as applicable) is not recognized by PCI SSC.

1.3.1 Initial Application and Staff Training

To initiate the P2PE Assessor qualification process, the P2PE Assessor candidate company must be in Good Standing as a QSA and must sign the P2PE Assessor Addendum in unmodified form and submit it to PCI SSC along with all other required provisions as part of its completed P2PE Assessor application package. PA-QSA (P2PE) candidates must also be in Good Standing as a PA-QSA at the time of application submission.

As discussed further below, assessor company staff members intending to perform P2PE Assessments must then pass applicable P2PE training examinations, depending on whether they are seeking qualification as a QSA (P2PE) Employee or PA-QSA (P2PE) Employee.

1.3.2 Good Standing

- **QSA (P2PE):** In order to remain qualified as a QSA (P2PE), and accordingly, in order to validate compliance with P2PE non-Domain 2 requirements and otherwise participate as a QSA (P2PE) in the P2PE Assessor Program, the assessor company must, unless otherwise expressly approved by PCI SSC in writing:

  (a) Be in Good Standing as a QSA (as defined in the QSA Agreement),
  (b) Have submitted a complete P2PE Assessor application package to PCI SSC,
  (c) Have an effective P2PE Assessor Addendum in place with PCI SSC,
  (d) Comply with all applicable requirements provided for in the P2PE Assessor Supplement and all QSA 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 P2PE Assessor Requirements (defined in the P2PE Assessor Addendum) or any term, condition, or requirement of P2PE Assessor quality assurance or remediation.

  An assessor company satisfying all of the above requirements is considered to be "in Good Standing" as a QSA (P2PE) and, while it is in such Good Standing, may market itself as a QSA (P2PE).
- **PA-QSA (P2PE):** In order to be and remain qualified as a PA-QSA (P2PE), and accordingly, in order to validate compliance with any and all P2PE Domain requirements (including but not limited to P2PE Domain 2 requirements) and otherwise participate as a PA-QSA (P2PE) in the P2PE Assessor Program, the assessor company must, unless otherwise expressly approved by PCI SSC in writing:

  (a) Be in Good Standing as a QSA (P2PE),
  (b) Be in PA-QSA Good Standing,
  (c) Comply with all requirements applicable to PA-QSAs 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

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

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

1.4 Document Structure

The P2PE Assessor Supplement is structured in five sections as follows.

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

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

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

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

Appendices: The appendices to the P2PE Assessor Supplement include the P2PE Assessor Addendum and several helpful checklists and feedback forms.

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

1.5 Related Publications

The P2PE Assessor Supplement is intended for use with the current version of the *QSA Qualification Requirements,* which should be 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*
- *Supplement for Payment Application Qualified Security Assessors (PA-QSA)*
- *PA-QSA Addendum*

1.6 P2PE Assessor Company Application Process

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

Important Note: *PCI SSC reserves the right to reject any application from any applicant (company or individual) that PCI SSC determines has committed, within two (2) 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 – Application Process Checklist.* All application materials and the signed P2PE Assessor Addendum must be submitted in English. The P2PE Assessor Addendum is binding in English even if the P2PE Assessor Addendum was translated and reviewed in another language. All other documentation provided to PCI SSC by the P2PE Assessor 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 application packages must include a signed P2PE Assessor Addendum and all other required documentation. All application materials must be submitted electronically via secure portal. Applicants should submit their request for access to this secure portal by sending an e-mail to p2pe@pcisecuritystandards.org, attention "Program Manager." Please note that mail and e-mail submissions will not be accepted.

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 Assessors and P2PE Assessor Employees submit additional information or materials in order to demonstrate adherence to applicable requirements or as part of the P2PE Assessor approval process. All such additional information and materials must be submitted in English or with a certified English translation. P2PE Assessors 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 written request.

2 Point-to-Point Encryption Assessor Business Requirements

2.1 Business Legitimacy

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

2.2 Independence

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

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

2.3 Insurance Coverage

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

2.4 P2PE Assessor Fees

2.4.1 Requirement

Each P2PE Assessor applicant must provide to PCI SSC the applicable initial processing fees. Initial processing fees must be paid in advance of PCI SSC reviewing the application materials and are credited toward the initial qualification fee (see below) if the company is qualified as a QSA (P2PE) or PA-QSA (P2PE). Fees may be paid by check or other means approved by PCI SSC. All checks should be made payable to "PCI SSC" and mailed to PCI SSC at the following address or as otherwise indicated by PCI SSC:

PCI Security Standards Council
401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone number: (781) 876-8855

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

- Initial qualification fee, which varies by geographic region or country, must be paid in full within 30 days of notification.
- Annual P2PE Assessor re-qualification fee, which varies by location, for each subsequent year..
- Annual training fees for each P2PE Assessor Employee seeking to be qualified, for training sponsored by PCI SSC.

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

2.5 P2PE Assessor Agreements

As described in further detail in the *QSA Qualification Requirements*, each QSA must have executed and submitted the QSA Agreement to qualify as a QSA. Once qualified as a QSA, there are various other agreements and/or addenda a QSA must execute and submit to PCI SSC, depending on the QSA programs in which the QSA wishes to participate. Please refer to the *QSA Qualification Requirements* for information about other agreements that may be needed, depending on what QSA programs your company is applying for.

In order to participate as a P2PE Assessor, PCI SSC requires that the P2PE Assessor Addendum be signed in unmodified form by a duly authorized officer of the QSA and then submitted by secure portal (see Section 1.6.1) to PCI SSC with the completed P2PE Application package. The P2PE Assessor Addendum requires that all P2PE Assessors comply with this P2PE Assessor Supplement and all additional requirements applicable to QSAs, PA-QSAs, and P2PE Assessors in accordance with applicable PCI SSC policies and procedures.

3 P2PE Assessor Company Capability Requirements

To understand the types and roles of P2PE Assessors, refer to *Appendix D: Assessor Qualification Levels and Applicability.*

3.1 P2PE Assessor Company – Services and Experience

3.1.1 P2PE Assessor Requirements

- Each P2PE Assessor performing or managing any P2PE Assessment must be qualified by PCI SSC as, and in Good Standing as, both a QSA and a QSA (P2PE).
- Each P2PE Assessor must fulfill all QSA Qualification Requirements, all QSA (P2PE) 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 must have completed at least two PCI DSS assessments as a QSA company.
- Each P2PE Assessor 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 at least the following areas:
    - Knowledge of 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
    - Knowledge of public key infrastructure (PKI) and the role and operations of a Certification Authority (CA) and Registration Authority (RA)
    - Knowledge of Hardware Security Modules (HSMs) operations, policies, and procedures
    - Knowledge of POI key-injection systems and techniques including key-loading devices (KLDs) and key-management methods, such as Master/Session or DUKPT
    - Knowledge of physical security techniques for high-security areas
    - Knowledge of relevant PTS Security Requirements (e.g., SRED, SCR, OP)
- All of the above skill sets must be present and fully utilized on every P2PE Assessment

3.1.2 Additional Requirements for PA-QSA (P2PE)s

In addition to the requirements specified at Section 3.1.1 above:

- Each P2PE Assessor performing or managing any P2PE Assessment to validate compliance with P2PE Domain 2 requirements must be qualified by PCI SSC and in Good Standing as a QSA, a PA-QSA (as defined in the PA-QSA Supplement), and a PA-QSA (P2PE). Only PA-QSA (P2PE)s in Good Standing as a QSA, PA-QSA, and PA-QSA (P2PE) may conduct P2PE Assessments to validate compliance with P2PE Domain 2 requirements.

- In addition to satisfying the P2PE Assessor Requirements specified in Section 3.1.1 above, each PA-QSA (P2PE) must:
  - Fulfill all PA-QSA (P2PE) Requirements, all PA-QSA Requirements (including the laboratory requirements attested to and set forth in *Appendix B* to the PA-QSA Supplement); and
  - 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.
- Each PA-QSA (P2PE) must also have demonstrated competence to include at least the following areas:
  - Knowledge of modern, secure embedded systems hardware and software architectures
  - Knowledge of PCI PTS quality and security management requirements related to POI software development
  - Knowledge of POI integration software development, deployment, and updates
  - Knowledge of POI software authenticity and integrity verification techniques and self-tests
  - Understanding of surrogate PAN generation techniques, such as format preserving encryption and tokenization
  - Knowledge of PCI PTS authentication requirements for accessing account data or sensitive services
  - Understanding of attack methodology through exploitation of logical vulnerabilities
- Each PA-QSA (P2PE) must have completed at least two PA-DSS Assessments as a PA-QSA company.
- For each PA-QSA (P2PE) evaluating P2PE Domain 2 requirements, all provisions set forth in Section 3.1.2 of the PA-QSA Supplement must be satisfied.
- All of the above skill sets must be present and fully utilized on every P2PE Assessment.

3.1.3 P2PE Assessor Provisions

The following information must be provided to PCI SSC, in addition to the other information required in Section 3.1 of this P2PE Assessor Supplement:

- A description of relevant experience with both cryptographic and key-management techniques, preferably related to payment functions and including a description of methodology used to perform such reviews equal to at least one year or three separate engagements. Examples of such engagements include, but are not limited to, assessments, implementations, or gap analyses.
- A description of dates and clients for two previous PCI DSS Assessments performed by the P2PE Assessor.
- Description of the P2PE Assessor's relevant areas of specialization within cryptography, key management, and other areas, to include at least the following areas:
  - Knowledge of 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
- Knowledge of public key infrastructure (PKI) and the role and operations of a Certification Authority (CA) and Registration Authority (RA)
- Knowledge of hardware security modules (HSMs) operations, policies, and procedures
- Knowledge of POI key-injection systems and techniques including key-loading devices (KLDs) and key-management methods, such as Master/Session or DUKPT
- Knowledge of physical security techniques for high-security areas
- Knowledge of relevant PTS Security Requirements (e.g., SRED, SCR, OP)

- An attestation that all of the above skill sets will be present and fully utilized on every P2PE Assessment.

3.1.4 Additional Provisions for PA-QSA (P2PE)s

In addition to the provisions specified at Section 3.1.3 above:

- A description of the PA-QSA (P2PE)'s relevant areas of specialization to include at least the following areas:
  - Modern, secure embedded systems hardware and software architectures
  - PCI PTS quality and security management requirements related to POI software development
  - POI integration software development, deployment and updates
  - POI software authenticity and integrity verification techniques and self-tests
  - Understanding of surrogate PAN generation techniques, such as format preserving encryption and tokenization
  - PCI PTS authentication requirements for accessing account data or sensitive services
  - Understanding of attack methodology through exploitation of logical vulnerabilities
- A description of dates and clients for two previous PA-DSS Assessments performed by the PA-QSA
- An attestation that all of the above skill sets will be present and fully utilized on every P2PE Assessment
- Two client references from relevant security engagements within the last 12 months

3.2 P2PE Assessor Company Staff – 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 qualified by PCI SSC are permitted to conduct P2PE Assessments. In addition, each P2PE Assessor Employee performing or managing any P2PE Assessment to validate compliance with P2PE Domain 2 requirements must be qualified by PCI SSC as a QSA employee, a PA-QSA employee, and a PA-QSA (P2PE) Employee. Only PA-QSA (P2PE) Employees qualified by PCI SSC are permitted to conduct

P2PE Assessments to validate compliance with P2PE Domain 2 requirements. P2PE Assessor Employees are responsible for the following:

- Performing the applicable P2PE Assessments
- Verifying that the P2PE Assessor's work product addresses all applicable P2PE requirements and assessment procedures, and supports the compliance status of the P2PE Solution
- Strictly following the P2PE Standard
- Producing the final P-ROV

3.2.1 P2PE Assessor Requirements

The P2PE Assessor Employee(s) performing or managing P2PE Assessments must:

- Be a QSA employee and fulfill all requirements for QSA employees specified in the *QSA Qualification Requirements*
- Have completed at least two PCI DSS Assessments as a QSA employee
- Possess substantial knowledge of:
    - 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)
- Attend annual P2PE Assessor 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.
- Be employees of the P2PE Assessor (meaning this work cannot be subcontracted to non-employees) unless PCI SSC has given prior written consent for each subcontracted worker.
- Be a current QSA in Good Standing for purposes of the QSA Agreement.

In addition:

- Approved subcontractors shall not be permitted to include a company logo other than that of the responsible P2PE Assessor or any reference to another company in the P-ROV or attestation documents while performing work on behalf of the P2PE Assessor.

- If a P2PE Assessor is actively in process with a P2PE Assessment and loses its QSA (P2PE) or PA-QSA (P2PE) status or foundational QSA or PA-QSA status, the company may be required to obtain the services of a valid QSA (P2PE) or PA-QSA (P2PE) (as applicable) to complete any in-process P2PE Assessments and applicable PCI SSC review processes.

3.2.2 Additional Requirements for PA-QSA (P2PE)s

In addition to the requirements specified at Section 3.2.1 above, a PA-QSA (P2PE) must:

- Be a PA-QSA employee and fulfill all requirements for PA-QSA employees specified in the *Supplemental Requirements for PA-QSAs*.
- Have performed at least two PA-DSS Assessments as a PA-QSA employee.
- Possess substantial knowledge of:
  - Modern, secure embedded systems hardware and software architectures
  - PCI PTS quality and security management requirements related to POI software development
  - POI integration software development, deployment and updates
  - POI software authenticity and integrity verification techniques and self-tests
  - Surrogate PAN-generation techniques, such as format-preserving encryption and tokenization
  - PCI PTS authentication requirements for accessing account data or sensitive services
  - Attack methodology through exploitation of logical vulnerabilities
- Be a current PA-QSA in Good Standing.

3.2.3 P2PE Assessor Provisions

The following information must be provided to PCI SSC for each individual seeking to be qualified as a QSA (P2PE) Employee or PA-QSA (P2PE) Employee (each a "Candidate"), in addition to the QSA Staff information required in Section 2.2:

- A description of dates and clients for two previous PCI DSS Assessments performed by the Candidate.
- Description of the Candidate's expertise with cryptography and key management with at least one year (total) in cryptographic techniques including cryptographic algorithms, key management, and key lifecycle.
- Description of additional expertise of the Candidate with cryptography and key management with at least one year (total) in three separate areas, as follows:
  - Public key infrastructure (PKI) and the role and operations of a Certification Authority (CA) and Registration Authority (RA)
  - 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
  - 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 and DUKPT

- Physical security techniques for high-security areas
- Relevant PTS Security Requirements (e.g., SRED, SCR, OP)

3.2.4 Additional Provisions for PA-QSA (P2PE)s

In addition to the provisions specified at Section 3.2.3 above, the following must be provided:

- For PA-QSA (P2PE) applications, a description of dates and clients for two previous PA-DSS Assessments performed by the Candidate.
- For PA-QSA (P2PE) applications, description of additional expertise of the Candidate with all of the following:
  - Modern, secure embedded systems hardware and software architectures
  - PCI PTS quality and security management requirements related to POI software development
  - POI integration software development, deployment and updates
  - POI software authenticity and integrity verification techniques and self-tests
  - Surrogate PAN-generation techniques, such as format preserving encryption and tokenization
  - PCI PTS authentication requirements for accessing account data or sensitive services
  - Attack methodology through exploitation of logical vulnerabilities

3.3 PA-QSA (P2PE) Testing Laboratory

All PA-QSA (P2PE)s and PA-QSA (P2PE) Employees must meet all applicable testing laboratory requirements as set forth in the *PA-QSA Supplement.*

4 P2PE Assessor Administrative Requirements

4.1 Contact Person

4.1.1 Requirement

The P2PE Assessor must provide PCI SSC with primary and secondary contacts (and related contact information) for both:

- Persons responsible for P2PE Assessments
- Persons responsible for oversight of quality assurance of P2PE Assessments

4.1.2 Provisions

The following contact information must be provided to PCI SSC for each primary and secondary contact mentioned above:

- Name
- Title
- Address
- Phone number
- Fax number
- E-mail address

4.2 Background Checks

All P2PE Assessors must satisfy all background check requirements as specified in the *QSA Qualification Requirements.*

4.3 Adherence to PCI Procedures

4.3.1 Requirements

- For each P2PE Assessment, the resulting P2PE Assessor report must follow the applicable P-ROV template and instructions as outlined in the P2PE Standard or otherwise by PCI SSC.
- The P2PE Assessor must prepare each P-ROV based on evidence obtained by following the P2PE Standard and applicable P2PE Assessment procedures.
- The P2PE Assessor must accompany each P-ROV with a "P2PE Attestation of Validation," signed by a duly authorized officer of the P2PE Assessor, in the applicable form available through the Website, that summarizes whether the applicable P2PE Solution and/or P2PE Application (if applicable) is in compliance with the P2PE Standard, and any related findings.
- The P2PE Assessor must only submit P-ROVs and the accompanying "P2PE Attestation of Validation" to PCI SSC where the P2PE Solution (or P2PE Application, if applicable) is fully compliant with P2PE and **all requirements** are noted as "in place."
- Prior to conducting each P2PE Assessment, the P2PE Assessor must:
    - Identify (in accordance with the P2PE Standard) the overall P2PE Solution and each P2PE Component thereof to be assessed as part of that P2PE Assessment (including but not limited

to the overall point-to-point encryption environment, the configuration thereof, and each P2PE Application and point-to-point encryption device that is part of or interacts with the P2PE Solution, regardless of physical location), and

- Inform the P2PE Solution Provider and each P2PE Application Vendor with a P2PE Application to be assessed as part of such P2PE Assessment that in order for their respective P2PE Solutions and P2PE Applications to be accepted by PCI SSC or identified on PCI SSC's applicable registry of validated P2PE Solutions, such P2PE Solution Provider and P2PE Application Vendor(s) (as applicable) must have executed the applicable P2PE Vendor Release Agreement and such executed agreement must have been delivered to PCI SSC.

4.4 P2PE Assessor Internal Quality Assurance

4.4.1 Requirements

- The P2PE Assessor must fulfill all QSA Requirements for quality assurance as defined in Section 4.4 of the *QSA Qualification Requirements*.
- The P2PE Assessor must have implemented a quality assurance program that includes P-ROVs, as documented in the company's quality assurance program manual (as described in Subsection 4.4.2 of the P2PE Assessor Supplement as well as Subsection 4.4.2 of the *QSA Qualification Requirements*).
- The P2PE Assessor must provide a P2PE Assessor Feedback Form to each P2PE Assessment client at the beginning of the P2PE Assessment. See *Appendix C: Sample P2PE Assessor Feedback Form.*
- The P2PE Assessor must adhere to all P2PE Assessor quality assurance requirements mandated or imposed by PCI SSC from time to time, including but not limited to, the following:
  - P-ROV review processes
  - Warnings
  - Oversight
  - Probation and/or Remediation
  - Fines and penalties
  - Revocation, suspension and any reinstatement processes
- PCI SSC reserves the right to conduct site visits and audit any P2PE Assessor at the discretion of PCI SSC.
- The P2PE Assessor must provide its quality assurance program manual to PCI SSC as part of its application for qualification as a P2PE Assessor and upon request thereafter.
- All documentation provided to PCI SSC by the P2PE Assessor in connection with PCI SSC quality assurance requirements must be provided in English or with a certified English translation.

4.4.2 Provisions

Description of a 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 approval of all P-ROVs prior to submission to PCI SSC
- Responsibilities for submitting P-ROVs to PCI SSC
- A requirement that all QSA (P2PE) and, if applicable, PA-QSA (P2PE) Employees must adhere to the P2PE Standard
- 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 Section 4.5 of *QSA Qualification Requirements*)
- Provision for continuous improvement of all P2PE Assessments and P-ROV review processes

4.5 Protection of Confidential and Sensitive Information

P2PE Assessors must adhere to all requirements to protect sensitive and confidential information, as set forth in the *QSA Qualification Requirements* required by PCI SSC.

4.6 Evidence Retention

P2PE Assessors must meet all evidence-retention requirements as set forth in the *QSA Qualification Requirements*. Additionally, all PA-QSA (P2PE)s must meet all evidence-retention requirements applicable to PA-QSAs.

For a minimum of three (3) years from submission of a given P-ROV to PCI SSC, the P2PE Assessor must secure (in accordance with 4.5 above) and maintain documented evidence (whether in digital or hard-copy format) 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.

4.7 P2PE Assessor Company Recognition of Client's Validation Status

4.7.1 Requirements

The P2PE Assessor must **not** provide any formal recognition of P2PE-validation status to a client with respect to a given P2PE Solution or P2PE Application (as applicable) until:

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

4.7.2 Provisions

The P2PE Assessor must provide a statement to PCI SSC (by signing the P2PE Assessor Addendum) that the P2PE Assessor will not recognize the validation status of a given P2PE Solution or P2PE Application assessed by such P2PE Assessor until PCI SSC has notified the P2PE Assessor, the corresponding P2PE Solution Provider, and the P2PE Application Vendor (if applicable), via P2PE Attestation of Validation, and such P2PE Solution and P2PE Application(s) (if applicable) are listed on the applicable registry of validated P2PE Solutions on the Website.

5 P2PE Assessor List, Re-qualification and Revocation

This section describes what happens after initial qualification and items related to the annual P2PE Assessor re-qualification. This section includes: (1) the P2PE Assessor List, (2) annual maintenance of P2PE Assessor qualification, and (3) revocation, if necessary, of P2PE Assessor qualification.

5.1 P2PE Assessor List

Once a company has met all applicable requirements specified in the P2PE Assessor Supplement, PCI SSC will add the P2PE Assessor to the P2PE Assessor List noting whether they are a QSA (P2PE) or PA-QSA (P2PE). Only those P2PE Assessors on the P2PE Assessor List are authorized by PCI SSC to perform P2PE Assessments, and only those identified as PA-QSA (P2PE)s on the P2PE Assessor List are authorized by PCI SSC to perform P2PE Assessments to validate compliance with P2PE Domain 2 requirements.

In the event a company does not meet the requirements specified in the P2PE Assessor Supplement, PCI SSC will notify the company. The company will have 30 days from the date of notification to appeal the decision. Appeals must be addressed to the PCI SSC General Manager and follow the procedures outlined on the Website. If a company's appeal is denied, its name will not be placed on the P2PE Assessor List.

5.2 P2PE Assessor Re-qualification

5.2.1 Requirements

All P2PE Assessors and P2PE Assessor Employees must be re-qualified by PCI SSC on an annual basis, based on the P2PE Assessor's original qualification date. Re-qualification is based on payment of annual fees, proof of training attended, and satisfactory feedback from the P2PE Assessor's clients (i.e., the P2PE Solution Providers and P2PE Application Vendors for which the P2PE Assessor performed P2PE Assessments), from PCI SSC, and from payment brand participants.

5.2.2 Provisions

The following must be provided to PCI SSC and/or will be considered by PCI SSC during the re-qualification process for both the P2PE Assessor and P2PE Assessor Employees:

- Feedback from P2PE Assessor clients (entities that were assessed), from PCI SSC, and from payment brand participants (see *Appendix C, Sample P2PE Assessor Feedback Form*). Significant or excessive unsatisfactory feedback may be cause for revocation;
- Payment of annual re-qualification fees (see Website for fees); and
- Proof of information-systems audit training within the last 12 months to support professional certifications (even if the employee does not yet have professional certifications), of a minimum 20 hours per year and 120 hours over the rolling three-year period. This is in addition to training provided by PCI SSC.

5.3 P2PE Assessor Revocation Process

Each of the following conditions, if determined by PCI SSC in its sole discretion to have occurred, shall constitute a "Violation" for purposes of Section A.9.5 of the QSA Agreement and Section A.7.5 of the

P2PE Assessor Addendum; and accordingly, for a P2PE Assessor or P2PE Assessor Employee, may result in immediate Revocation of QSA (or QSA employee) qualification and/or P2PE Assessor Revocation of P2PE Assessor or P2PE Assessor Employee qualification, including but not limited to removal from the P2PE Assessor List, subject to reinstatement pending a successful appeal in accordance with the QSA Agreement and/or P2PE Assessor Addendum, and/or termination of the QSA Agreement and/or P2PE Assessor Addendum:

- Failure to validate compliance in accordance with applicable PCI SSC standards and procedures.
- Violation any provision or obligation regarding non-disclosure of confidential materials.
- Failure to maintain physical, electronic, and procedural safeguards to protect confidential or sensitive information; and/or failure to report unauthorized access to any system that stores confidential or sensitive information.
- Engaging in unprofessional or unethical business conduct.
- Failure to provide quality services, based on customer feedback or evaluation by PCI SSC or any participating payment brand.
- Cheating on any exam in connection with PCI SSC training, including without limitation: submitting work that is not the work of the P2PE Assessor Employee taking the exam; theft of or unauthorized access to an exam; use of an alternate, stand-in, or proxy during an exam; use of any prohibited or unauthorized materials, notes, or computer programs during an exam; and providing or communicating in any way any unauthorized information to another person during an exam.
- Providing false or intentionally incomplete or misleading information to PCI SSC in any application or other materials.
- Failure to be in Good Standing as a QSA, PA-QSA (if applicable) or P2PE Assessor, in each case including but not limited to failure to successfully complete applicable quality assurance audits and/or comply with all applicable requirements, polices, and procedures of PCI SSC's quality assurance, remediation, and oversight programs and initiatives as established or imposed from time to time by PCI SSC in its sole discretion.
- Failure to promptly notify the Council of any event described above that occurred at any time after the date two (2) years before such P2PE Assessor's or P2PE Assessor Employee's qualification by PCI SSC.

In the event of any Revocation:

- The P2PE Assessor's name may be removed from or annotated on the P2PE Assessor List,
- PCI SSC will notify the P2PE Assessor of the corresponding Violation, and
- The P2PE Assessor will have an opportunity to defend its conduct through an appeal to PCI SSC in accordance with the QSA Agreement.

All appeals must be submitted to PCI SSC in writing, addressed to the PCI SSC General Manager, and follow all applicable procedures as specified by PCI SSC. PCI SSC will review all relevant evidence submitted by the complainant (if any) and P2PE Assessor in connection with such appeals and make a decision as to whether termination of P2PE Assessor qualification is warranted. All decisions of PCI SSC regarding revocation are final.

If a P2PE Assessor's appeal is denied or the P2PE Assessor fails to appeal in accordance with the P2PE Assessor Addendum, PCI SSC may immediately terminate the corresponding QSA Agreement and/or P2PE Assessor Addendum and notify the participating payment brands and/or acquirers.

Appendix A: Addendum to QSA Agreement for P2PE Assessors

A.1 Introduction

This Addendum to Qualified Security Assessor (QSA) Agreement for QSA (P2PE)s and PA-QSA (P2PE)s (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			
Applicant Name:			
Company Name:			
QSA Agreement Date:			
Location/Address:			
State/Province:	Country:	Postal Code:	
Regions Applying For (see Website for list):			
Applicant's Signature			
Applicant's Officer Signature ↑		*Date* ↑	
Applicant Officer Name:	Title:		

For PCI SSC Use Only:	
Application Date:	
Application Approved:	

PCI SSC Officer Signature ↑		
PCI SSC Officer Name:	Title:	

A.3 Terms and Conditions

A.3.1 Definitions

A.3.1.1 Terms in Addendum

While this Addendum is in effect, capitalized terms defined herein shall have the meanings ascribed to them herein for all purposes of this Addendum and the Agreement, and capitalized terms appearing herein without definition shall have the meanings ascribed to them in or pursuant to the Agreement.

The following terms shall have the following meanings:

(a) "Good Standing" is defined in the P2PE Assessor Supplement.

(b) "P-ROV" is defined in the P2PE Assessor Supplement.

(c) "PA-QSA (P2PE)" is defined in the P2PE Assessor Supplement.

(d) "PA-QSA (P2PE) Requirements" is defined in the P2PE Assessor Supplement.

(e) "Payment Application" means a “P2PE Application”, as defined in the P2PE Assessor Supplement.

(f) “P2PE Application Vendor” is defined in the P2PE Assessor Supplement.

(g) "P2PE Standard" is defined in the P2PE Assessor Supplement and is hereby incorporated into this Addendum.

(h) "P2PE Assessment" is defined in the P2PE Assessor Supplement.

(i) "P2PE Assessor" is defined in the P2PE Assessor Supplement.

(j) "P2PE Assessor Program" is defined in the P2PE Assessor Supplement.

(k) "P2PE Assessor 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 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 requirements of applicable PCI SSC training programs, quality assurance, remediation and oversight programs, program guides and other related PCI Materials.

(l) "P2PE Assessor Supplement" means the then-current version of (or successor document to) the *Payment Card Industry (PCI) Data Security Standard QSA Qualification Requirements Supplement for Point-to-Point Encryption Qualified Security Assessors (QSA (P2PE) and PA-QSA (P2PE))*, as from time to time amended and made available on the Website by PCI SSC.

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

(n) "P2PE Domain Requirements" is defined in the P2PE Assessor Supplement.

(o) "P2PE Domain 2 Requirements" is defined in the P2PE Assessor Supplement.

(p) "P2PE Non-Domain 2 Requirements" is defined in the P2PE Assessor Supplement.

(q) "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 Assessor Supplement or participation in the P2PE Assessor Program.

(r) "P2PE Solution" is defined in the P2PE Assessor Supplement.

(s) “P2PE Solution Provider” is defined in the P2PE Assessor Supplement.

(t) "P2PE Vendor Release Agreement" is defined in the P2PE Assessor Supplement.

(u) "QSA Qualification Requirements" is defined in the P2PE Assessor Supplement.

(v) "QSA (P2PE)" is defined in the P2PE Assessor Supplement.

(w) "QSA (P2PE) Requirements" is defined in the P2PE Assessor Supplement.

(x) "Website" is defined in the P2PE Assessor Supplement.

A.3.1.2 Terms in Agreement

While this Addendum is in effect, the following terms appearing in the Agreement are hereby amended as follows for purposes of the Agreement:

(a) The term "Services" shall include the P2PE Services.

(b) The term "QSA Requirements" shall include the P2PE Assessor Requirements.

(c) The term “Subjects” shall include P2PE Customers.

(d) The terms "Report of Compliance", "ROC" and "Attestation of Compliance" shall, where applicable, include the terms "P2PE Report of Validation", "P-ROV" and "P2PE Attestation of Validation", respectively, as those terms are used in the P2PE Assessor Supplement.

A.3.2 P2PE Services

(a) Subject to the terms and conditions of this Addendum and the Agreement, PCI SSC hereby approves QSA to: (i) while QSA is in Good Standing as a QSA (P2PE) (or as otherwise expressly approved by PCI SSC in writing), conduct P2PE Assessments for P2PE Customers solely in order to validate compliance with P2PE Non-Domain 2 Requirements and (ii) while QSA is in Good Standing as a PA-QSA (P2PE) (or as otherwise expressly approved by PCI SSC in writing), conduct P2PE Assessments for P2PE Customers in order to validate compliance with any P2PE Domain Requirements. Notwithstanding the foregoing, QSA agrees that QSA shall not recognize a given P2PE Solution or P2PE Application as validated under the P2PE Standard until (A) the corresponding P2PE Solution Provider and P2PE Application Vendor (if applicable) 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 Solution Provider and P2PE Application Vendor (if any) of such validation via P2PE Attestation of Validation or other applicable acceptance letter signed by PCI SSC and (c) such P2PE Solution or P2PE Application (if applicable) has been listed on PCI SSC's applicable published registry of P2PE validated P2PE Solutions.

(b) QSA agrees to monitor the Website at least weekly for changes to the P2PE Assessor Supplement and the P2PE Standard. QSA will incorporate all such changes into all P2PE Assessments initiated on or after the effective date of such changes. QSA acknowledges that PCI SSC will not accept any P-ROV regarding a P2PE Assessment that is not conducted in accordance with the P2PE Assessor Supplement and P2PE Standard as in effect at the initiation date of such P2PE Assessment.

A.3.3 Performance of P2PE Services

(a) QSA warrants and represents that it will perform each P2PE Assessment in strict compliance with the P2PE Standard and P2PE Assessor Supplement as in effect as of the commencement date of such P2PE Assessment and that QSA shall comply with all P2PE Assessor Requirements. Without limiting the foregoing, 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 (a) in performing the applicable P2PE Assessment, QSA followed the P2PE Standard and P2PE Assessor Supplement without deviation and (b) application of such procedures did not indicate any conditions of non-compliance with the P2PE Standard other

than those noted in the P-ROV.

(b) QSA acknowledges and agrees that, in an effort to maintain the integrity of the P2PE Assessor Program, PCI SSC from time to time may request demonstrated adherence to applicable P2PE Domain Requirements and the requirements of the P2PE Assessor Supplement. Each such request shall be in writing and QSA shall respond thereto with documented evidence of such adherence in form and substance acceptable to PCI SSC no later than three (3) weeks from QSA's receipt of such written request.

(c) QSA agrees that, prior to performing any P2PE Assessment with respect to a given P2PE Solution or P2PE Application, QSA shall obtain an executed VRA from the applicable P2PE Solution Provider and each P2PE Application Vendor the P2PE Application(s) of which are to be reviewed as part of such P2PE Assessment, and QSA shall deliver such executed VRAs to PCI SSC as soon as possible thereafter, but in any event, no later than the date upon which QSA delivers to PCI SSC the corresponding P-ROV generated in connection with such P2PE Assessment.

A.3.4 P2PE Service Staffing

QSA shall ensure that a P2PE Assessor Employee that is fully qualified in accordance with all applicable provisions of the P2PE Assessor Supplement supervises all aspects of each engagement to perform P2PE Services in accordance with the P2PE Assessor Supplement and the P2PE Standard.

A.3.5 P2PE Assessor Requirements

QSA agrees to adhere to all P2PE Assessor Requirements, and in connection therewith, to comply with all requirements and make all provisions as set forth in the P2PE Assessor Supplement, including without limitation, all business, capability, and administrative requirements, as set forth in Sections 2, 3 and 4 of the P2PE Assessor Supplement, and all requirements with respect to P2PE Assessor Employees (as defined in the P2PE Assessor Supplement). Further, QSA warrants that, to the best of QSA's ability to determine, all information provided to PCI SSC in connection with this Addendum and QSA's participation in the P2PE Assessor Program is and shall be accurate and complete as of the date such information is provided. QSA acknowledges that PCI SSC may from time to time require QSA to provide a representative to attend any mandatory training programs in connection with the P2PE Assessor Program, which may require the payment of attendance and other fees.

A.4 P2PE Fees

QSA shall pay all applicable fees in connection with participation in the P2PE Assessor Program as referenced in and in accordance with the P2PE Assessor Supplement. QSA acknowledges that PCI SSC may review and modify such fees at any time and from time to time, provided that PCI SSC shall notify QSA of such change and such change will be effective thirty (30) days after the date of such notification. Should QSA not agree with any such change, QSA may terminate this Addendum upon written notice to PCI SSC at any time within such 30-day period.

A.5 QSA List; Promotional References; Restrictions

(a) So long as QSA is a P2PE Assessor, PCI SSC may, at its sole discretion, identify QSA as such (indicating QSA (P2PE) or PA-QSA (P2PE), as applicable) on the QSA List or in such other publicly available list of P2PE Assessors as PCI SSC may maintain and/or distribute from time to time, whether on the Website or otherwise (for purposes of the Agreement, such other list (if any) shall be deemed to be part of the QSA List). Without limiting the rights of PCI SSC set forth in the preceding sentence or elsewhere, PCI SSC expressly reserves the right to remove QSA from the QSA List or

any such other PCI SSC list at any time during which QSA is not in Good Standing as a P2PE Assessor.

(b) So long as QSA is in Good Standing as a P2PE Assessor and is identified in the QSA List as a QSA (P2PE) or PA-QSA (P2PE), QSA to make reference to such listing and its qualification as a QSA (P2PE) or (if applicable) PA-QSA (P2PE) in advertising or promoting its P2PE Services.

(c) QSA shall not: (i) make any false, misleading or incomplete statements regarding, or misrepresent PCI SSC, its status as a P2PE Assessor or the requirements of the P2PE Standard, including without limitation, any requirement regarding the implementation of the P2PE Standard or the application thereof to any P2PE Customer, or (ii) state or imply that the P2PE Standard requires usage of QSA's products or services.

A.6 P2PE Customer Data; Quality Assurance

(a) To the extent any data or other information obtained by QSA relating to any P2PE Customer in the course of providing P2PE Services thereto may be subject to any confidentiality restrictions between QSA and such P2PE Customer, QSA must provide in each agreement containing such restrictions (and in the absence of any such agreement must agree with such P2PE Customer in writing) that (i) QSA may disclose each P-ROV and other related information to PCI SSC and/or its Members, as requested by the P2PE Customer, (ii) to the extent any Member obtains such information in accordance with the preceding clause A6(a)(i), such Member may disclose (a) such information on an as needed basis to other Members and to such Members' respective Financial Institutions and Issuers and to relevant governmental, regulatory and law enforcement inspectors, regulators and agencies and (b) that such Member has received a P-ROV and other related information with respect to such P2PE Customer (identified by name) and whether the P-ROV was satisfactory, and (iii) QSA may disclose such information as necessary to comply with its obligations and requirements pursuant to Section A.10.2(b) of the Agreement. Accordingly, notwithstanding anything to the contrary in Section A.6.2(a) of the Agreement, to the extent requested by a P2PE Customer, PCI SSC may disclose Confidential Information relating to such P2PE Customer and obtained by PCI SSC in connection with this Addendum to Members in accordance with this Section A.6(a), and such Members may in turn disclose such information to their respective member Financial Institutions and other Members. QSA hereby consents to such disclosure by PCI SSC and its Members. As between any Member, on the one hand, and QSA or any P2PE Customer, on the other hand, the confidentiality of P-ROVs and any other information provided to Members by QSA or any P2PE Customer is outside the scope of the Agreement and may be subject to such confidentiality arrangements as may be established from time to time between such Member, on the one hand, and QSA or such P2PE Customer (as applicable), on the other hand.

(b) Notwithstanding anything to the contrary in Section A.6 of the Agreement or in this Addendum, in order to assist in ensuring the reliability and accuracy of P2PE Assessments, QSA hereby agrees to comply with all quality assurance procedures and requirements established or imposed upon QSA by PCI SSC from time to time (including but not limited to conditions and requirements imposed in connection with remediation, oversight or any other qualification status) and that, accordingly, within 15 days of any written request by PCI SSC or any Member (each a “Requesting Organization”), QSA hereby agrees to provide such Requesting Organization with such P2PE Assessment Results (defined below) as such Requesting Organization may reasonably request with respect to (i) if the Requesting Organization is a Member, any P2PE Customer for which QSA has performed a P2PE Assessment to the extent such P2PE Customer has provided a P2PE Solution to a Financial Institution of such Member, an Issuer of such Member, a Merchant authorized to accept such Member's payment cards, an Acquirer of accounts of Merchants authorized to accept such Member's payment cards or a Processor performing services for such Member's Financial Institutions, Issuers,

Merchants or Acquirers or (ii) if the Requesting Organization is PCI SSC, any P2PE Customer for which QSA has performed a P2PE Assessment. Each agreement between QSA and each of its P2PE Customers (each a "Customer Agreement") shall include such provisions as may be necessary or otherwise required by PCI SSC to ensure that QSA has all rights, licenses and other permissions necessary for QSA to comply with its obligations and requirements pursuant to this Addendum, with no conditions, qualifications or other terms (whether in such Customer Agreement or otherwise) that might tend to nullify, impair or render unenforceable QSA's right to disclose such P2PE Assessment Results as required by this Section. Any failure of QSA to comply with this Section A.6(b) shall be deemed to be a breach of QSA's representations and warranties under the Agreement for purposes of Section A.9.3 thereof, and upon any such failure, PCI SSC may remove QSA's name from the QSA List and/or terminate this Addendum or the Agreement in its sole discretion. Additionally, QSA agrees to comply with all quality assurance standards, requirements, policies and procedures established, mandated or imposed upon QSA or P2PE Assessors generally by PCI SSC from time to time, including without limitation, those relating to probation, fines, penalties, oversight, remediation, suspension and revocation. For purposes of the foregoing, "P2PE Assessment Results" means (1) all P-ROVs and related information, materials and assessment results generated and/or obtained by QSA in connection with P2PE Assessments, including without limitation, all work papers, notes and other materials or information generated or obtained in connection therewith and (2) complete and accurate copies of each Customer Agreement; provided that such materials may be redacted in accordance with applicable PCI SSC policies and procedures, including but not limited to, redaction of pricing, delivery process and/or confidential and proprietary information of the P2PE Customer and/or its customers, so long as (A) such redaction is in accordance with PCI SSC policy, (B) the redacted information does not obscure any language that may tend to nullify, impair or render unenforceable QSA's right to disclose P2PE Assessment Results to PCI SSC as required by this Section, and (C) upon request, QSA provides to PCI SSC a written certification that such redaction complies with the requirements of this Section executed by an executive officer of QSA.

A.7 Term and Termination

A.7.1 Term

This Addendum shall become effective as of the Addendum Effective Date and, unless earlier terminated in accordance with this Section A.7, 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.7.2 Termination by QSA

QSA may terminate this Addendum upon thirty (30) days' written notice to PCI SSC.

A.7.3 Termination by PCI SSC

PCI SSC may terminate this Addendum effective as of the end of any Contract Year by providing QSA with written notice of its intent not to renew this Addendum at least sixty (60) days prior to the end of the then-current Contract Year. Additionally, PCI SSC may immediately terminate this Addendum (i) with written notice upon QSA's breach of any representation or warranty under this Addendum, (ii) with fifteen (15) days' prior written notice following QSA's breach of any other term or provision of this Addendum (including without limitation, QSA's failure to comply with any P2PE Assessor Requirement), provided

such breach remains uncured when such 15-day period has elapsed, or (iii) in accordance with Section A.7.5 below.

A.7.4 Effect of Termination

Upon any termination or expiration of this Addendum: (i) QSA will no longer be identified as a P2PE Assessor on the QSA List; (ii) QSA shall immediately cease all advertising and promotion of its status as a P2PE Assessor and all references to the P2PE Standard and other PCI Materials; (iii) QSA shall immediately cease soliciting for and performing all P2PE Services (including but not limited to processing of P-ROVs), provided that, if and to the extent instructed by PCI SSC in writing, QSA shall complete any and all P2PE Services for which QSA was engaged prior to such expiration or the notice of termination; (iv) to the extent QSA is instructed to complete any P2PE Services pursuant to preceding clause (iii), QSA will deliver all corresponding outstanding P-ROVs within the time contracted with the P2PE Customer; (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, obtain (at QSA's sole cost and expense) the services of a replacement P2PE Assessor acceptable to PCI SSC for purposes of completing those P2PE Services for which QSA was engaged prior to such expiration or the notice of 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 P2PE Services; (viii) QSA shall, within fifteen (15) days of PCI SSC's written request, in a manner acceptable to PCI SSC, notify those of its P2PE Customers with which QSA is then engaged to perform P2PE Assessments or other P2PE Services 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.7.4 shall survive the expiration or termination of this Addendum for any or no reason.

A.7.5 Revocation

(a) Without limiting the rights of PCI SSC as set forth elsewhere herein or in the Agreement, in the event that PCI SSC determines in its sole but reasonable discretion that QSA meets any condition for revocation of P2PE Assessor qualification as established by PCI SSC from time to time (satisfaction of any such condition, a "Violation"), including without limitation, any of the conditions described in Section 5.3 of the *QSA Qualification Requirements* or Section 5.3 of the *P2PE Assessor Supplement*, PCI SSC may, effective immediately upon notice of such Violation to QSA, revoke QSA's P2PE Assessor qualification and/or QSA qualification (each such revocation a "Revocation" for purposes of this Addendum and the Agreement), in each case, subject to reinstatement pending a successful appeal in accordance with Section A.9.5(b) of the Agreement and applicable PCI SSC policies and procedures. In the event of any Revocation: (i) QSA will be removed from the QSA List and/or such listing may be annotated as PCI SSC deems appropriate; (ii) QSA must comply with Section A.7.4 of the Addendum and Section A.9.4 of the Agreement in the manner otherwise required if the Addendum and Agreement had been terminated; (iii) QSA will have a period of thirty (30) days from the date QSA is given notice of the corresponding Violation to submit a written request for appeal to the PCI SSC General Manager; (iv) QSA shall, within fifteen (15) days of such Revocation, in a manner acceptable to PCI SSC, notify those of its Subjects and P2PE Customers with which QSA is then engaged to perform Assessments, P2PE Assessments or other Services or P2PE Services of such Revocation and, if applicable, of any conditions, restrictions or requirements of such Revocation that may impact its ability to perform Assessments, P2PE Assessments or other Services or P2PE Services for Subjects or P2PE Customers going forward; and (v) notwithstanding anything to the

contrary in this Addendum or the Agreement, PCI SSC may notify any of its Members and any acquirers, QSA Subjects, QSA P2PE Customers or others of such Revocation and the reason(s) therefor. In the event QSA fails to submit a request for appeal within the allotted 30-day period, this Agreement shall automatically terminate effective immediately as of the end of such period.

(b) All Revocation appeals proceedings will be conducted in accordance with such procedures as PCI SSC may establish from time to time, PCI SSC will review all relevant evidence submitted by QSA and each complainant (if any) in connection with therewith, and PCI SSC shall determine whether termination of any PCI SSC qualification is warranted or, in the alternative, no action, or specified remedial actions shall be required. All determinations of PCI SSC regarding Revocation and any related appeals shall be final and binding upon QSA. If PCI SSC determines that termination is warranted, then effective immediately and automatically upon such determination, this Addendum and/or the Agreement (as applicable) shall terminate, and accordingly, each corresponding PCI SSC qualification of QSA shall also terminate. If PCI SSC determines that no action is required of QSA, the Revocation shall be lifted and QSA shall be reinstated on the QSA List as appropriate. If PCI SSC determines that remedial action is required, PCI SSC shall notify QSA and may establish a date by which such remedial action must be completed, provided that the Revocation shall not be lifted, and QSA shall not be reinstated on the QSA List, unless and until such time as QSA has completed such remedial action; provided that if QSA fails to complete any required remedial action by the date (if any) established by PCI SSC for completion thereof, PCI SSC may terminate this Addendum and/or the Agreement effective immediately as of such date.

A.8 General Terms

While this Addendum is in effect, the terms and conditions set forth herein 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 writing, 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.

Appendix B: P2PE Assessor – Application Process Checklist

This checklist has been provided as a tool to help you organize the Point-to-Point Encryption Qualified Security Assessor ("P2PE Assessor") application information that must be submitted along with your completed/signed P2PE Assessor Addendum. This checklist is for new P2PE Assessor applications only.

Note: *All application and other materials provided to PCI SSC must be submitted in English or with a certified English translation.*

This checklist is a tool only—please review the detailed requirements in this document to ensure completeness of submitted information.

P2PE Assessor Business Requirements[1]

Reference	Requirement	Information/documentation Needed	
2.1	**Business Legitimacy**	Not applicable for P2PE Assessor documentation; however, this information should already have been submitted as part of original QSA application.	
2.2	**Independence**	Not applicable for P2PE Assessor documentation; however, this information should already have been submitted as part of original QSA application.	
2.3	**Insurance Coverage**	Not applicable for P2PE Assessor documentation; however, this information should already have been submitted as part of original QSA application.	
2.4.1	**P2PE Assessor Fee**		Initial P2PE Assessor processing fee, payable to PCI SSC
2.5	**P2PE Assessor Agreement**		P2PE Assessor Addendum signed by company officer
3.1	**P2PE Assessor Company – Services and Experience**		
3.1.3	**P2PE Assessor Provisions** *Continued on next page*		Description of relevant experience with cryptographic and key-management techniques, equal to at least one year or three separate engagements.
			Dates and clients for two previously completed PCI DSS assessments.

[1] This checklist is for **P2PE Assessors** and details the documentation needed to substantiate the P2PE Assessor's qualifications to perform P2PE Assessments. It is also required that P2PE Assessors are qualified as QSAs as well, and all P2PE Assessor documentation must be previously submitted to PCI SSC, as stated in the *QSA Qualification Requirements*, Appendix B.

Reference	Requirement	Information/documentation Needed	
3.1.3	**P2PE Assessor Provisions** *(continued)*		Description of the P2PE Assessor's relevant areas of specialization within cryptography, key management, and other areas, to include at least the following: ▪ Knowledge of 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. ▪ Knowledge of public key infrastructure (PKI) and the role and operations of a Certification Authority (CA) and Registration Authority (RA). ▪ Knowledge of hardware security modules (HSMs) operations, policies, and procedures. ▪ Knowledge of POI key-injection systems and techniques including key-loading devices (KLDs) and key-management methods, such as Master/Session or DUKPT ▪ Knowledge of physical security techniques for high-security areas ▪ Knowledge of relevant PTS Security Requirements (e.g., SRED, SCR, OP)
			Attestation that all of the above skill sets will be present and fully utilized on every P2PE Assessment.
3.1.4	**Additional Provisions for PA-QSA (P2PE)s**		For PA-QSA (P2PE) Employees, description of relevant areas of specialization in at least: ▪ Modern, secure embedded systems hardware and software architectures ▪ PCI PTS quality and security management requirements related to POI software development ▪ POI integration software development, deployment and updates ▪ POI software authenticity and integrity verification techniques and self-tests ▪ Understanding of surrogate PAN generation techniques, such as format preserving encryption and tokenization ▪ PCI PTS authentication requirements for accessing account data or sensitive services ▪ Understanding of attack methodology through exploitation of logical vulnerabilities
			Description of dates and clients for two previously completed PA-DSS assessments
			Attestation that all of the above skill sets will be present and fully utilized on every P2PE Assessment
			Two client references from relevant security engagements within the last 12 months

Reference	Requirement	Information/documentation Needed	
3.2	**P2PE Assessor Company Staff – Skills and Experience**		
3.2.3	**P2PE Assessor Provisions**	For each individual seeking to be qualified as a QSA (P2PE) Employee or PA-QSA (P2PE) Employee (each a "Candidate"), in addition to the QSA Staff information required in Section 2.2:	
			A description of dates and clients for two previous PCI DSS Assessments performed by the Candidate.
			Description of the Candidate's expertise with cryptography and key management with at least one year (total) in cryptographic techniques including cryptographic algorithms, key management, and key lifecycle.
			Description of additional expertise of the Candidate with cryptography and key management with at least one year (total) in three separate areas, as follows: ▪ Public key infrastructure (PKI) and the role and operations of a Certification Authority (CA) and Registration Authority (RA) ▪ 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 ▪ 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 and DUKPT ▪ Physical security techniques for high-security areas ▪ Relevant PTS Security Requirements (e.g., SRED, SCR, OP)
3.2.4	**Additional Provisions for PA-QSA (P2PE)s**		A description of dates and clients for two previous PA-DSS Assessments performed by the Candidate.
			For PA-QSA (P2PE) applications, description of additional expertise of the Candidate with all of the following: ▪ Modern, secure embedded systems hardware and software architectures ▪ PCI PTS quality and security management requirements related to POI software development ▪ POI integration software development, deployment and updates ▪ POI software authenticity and integrity verification techniques and self-tests ▪ Surrogate PAN-generation techniques, such as format preserving encryption and tokenization ▪ PCI PTS authentication requirements for accessing account data or sensitive services ▪ Attack methodology through exploitation of logical vulnerabilities

Reference	Requirement	Information/documentation Needed			
3.3	**PA-QSA (P2PE) Testing Laboratory**	Not applicable for P2PE Assessor documentation; however, this information should already have been submitted as part of original PA-QSA application.			
4	**P2PE Assessor Administrative Requirements**				
4.1.2	**P2PE Assessor Contact Person – Primary and Secondary**		Name		Phone
			Title		Fax
			Address		E-mail
4.2	**Background Checks**		For each P2PE Assessor Employee to be qualified, statement that employee successfully completed the background check in accordance with the QSA's policies and procedures.		
			Company signature on the P2PE Assessor Addendum		
4.3	**Adherence to PCI Procedures**		Company signature on the P2PE Assessor Addendum		
4.4	**Quality Assurance**		Description of a 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 approval of all P-ROVs prior to submission to PCI SSC ▪ Responsibilities for submitting P-ROVs to PCI SSC ▪ A requirement that all QSA (P2PE) and, if applicable, PA-QSA (P2PE) Employees must adhere to the P2PE Standard ▪ 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 Section 4.5 of *QSA Qualification Requirements*) ▪ Provision for continuous improvement of all P2PE Assessments and P-ROV review processes		
			Company signature on the P2PE Assessor Addendum		
4.5	**Protection of Confidential and Sensitive Information**	Not applicable for P2PE Assessor documentation; however, this information should already have been submitted as part of original QSA application.			
4.6	**Evidence Retention**	Not applicable for P2PE Assessor documentation; however, this information should already have been submitted as part of original QSA application.			

Reference	Requirement	Information/documentation Needed	
4.7	**Recognition of Client's Validation Status**		A statement that the P2PE Assessor will not recognize the validation status of a given P2PE Solution or P2PE Application assessed by such P2PE Assessor until PCI SSC has notified the P2PE Assessor, the corresponding P2PE Solution Provider, and the P2PE Application Vendor (if applicable), via P2PE Attestation of Validation, and such P2PE Solution and P2PE Application(s) (if applicable) are listed on the applicable registry of validated P2PE Solutions.
			Company signature on the P2PE Assessor Addendum.

Appendix C: Sample P2PE Assessor Feedback Forms

The following form is used to review Point-to-Point Encryption Assessors ("P2PE Assessors") and their work product, and is intended to be completed by the client after a P2PE Assessment. While this form is intended for completion by the subjects of the P2PE Assessment (i.e., the P2PE Solution Providers and P2PE Application Vendors), there are several questions at the end, under "P2PE Feedback Form for Payment Brands and Others," to be completed as needed by participating payment brands, banks, and other relevant parties. Information collected from the Feedback Form will be held in strict confidence and used for the sole purpose of improving the Council's standards and the quality of services provided by PCI SSC-qualified assessors.

This form can be obtained directly from the P2PE Assessor during the audit, or can be found online in a useable format at www.pcisecuritystandards.org. **The client, not the QSA, should submit this form to PCI SSC.** Please send this completed form to PCI SSC at: compliance@pcisecuritystandards.org.

P2PE Assessor Feedback Form

	Client (P2PE Solution Provider or P2PE Application Vendor)	***P2PE Assessor Company***	
Company Name			
Contact			
Title			
Telephone			
E-mail			
Location of Assessment		**QSA (P2PE) / PA-QSA (P2PE) Employee(s) who performed Assessment**	
Street Name		Name	
City		Title	
State/Province		ID Number	
Country		Telephone	
Postal Code		E-mail	

For each statement, please indicate the response that best reflects your experience and provide comments.

5 = Strongly Agree 4 = Agree 3 = Neutral 2 = Disagree 1 = Strongly Disagree

Statement	Rating	Comments
1. During the initial engagement, the P2PE Assessor explained the objectives, timing, and review process, and addressed your questions and concerns.		
2. The P2PE Assessor Employee(s) understood your business and technical environment, as well as the cardholder data environment.		
3. The P2PE Assessor Employee(s) had sufficient security and technical skills to effectively perform this assessment.		
4. The P2PE Assessor sufficiently understood the P2PE and all related requirements and assessment procedures.		
5. The P2PE Assessor effectively minimized interruptions to operations and schedules.		
6. The P2PE Assessor provided an accurate estimate for time and resources needed.		
7. The P2PE Assessor provided an accurate estimate for report delivery.		
8. The P2PE Assessor did not attempt to market products or services for your company to attain P2PE Solution validation.		
9. The P2PE Assessor did not imply that use of a specific brand of commercial product or service was necessary to achieve compliance.		
10. In situations where remediation was required, the P2PE Assessor presented product and/or solution options that were not exclusive to their own product set.		
11. The P2PE Assessor used secure transmission to send any confidential reports or data.		
12. The P2PE Assessor demonstrated courtesy, professionalism, and a constructive and positive approach.		

Statement	Rating	Comments
13. There was sufficient opportunity for you to provide explanations and responses during the assessment.		
14. During the review wrap-up, the P2PE Assessor clearly communicated findings and expected next steps.		
15. The P2PE Assessor provided sufficient follow-up during your company's remediation efforts until eventual compliance was achieved.		

Please use the space below to provide any additional comments here about the P2PE Assessor, your assessment experience, or the P2PE documents.

P2PE Assessor Feedback Form for Payment Brands and Others

Client (P2PE Solution Provider or P2PE Application Vendor reviewed)		*P2PE Assessor Company*	
Company Name			
Payment Brand Reviewer		**QSA (P2PE) / PA-QSA (P2PE) Employee(s) who performed Assessment**	
Name			
Title		Employee ID number:	
Telephone			
E-mail			

For each statement, please indicate the response that best reflects your experience and provide comments.

5 = Strongly Agree **4 = Agree** **3 = Neutral** **2 = Disagree** **1 = Strongly Disagree**

Statement	Rating	Comments
1. The P2PE Assessor clearly understood how to notify your payment brand about compliance and non-compliance issues, and the status of merchants, service providers and vendors.		
2. The Client had a positive and professional experience with the P2PE Assessor.		
3. The P2PE Assessor demonstrated sufficient understanding of the P2PE and all related requirements and assessment procedures.		
4. The P2PE Assessor appropriately documented the results related to their findings.		
5. From your understanding, the P2PE Assessor appropriately scoped the payment application's role cardholder data environment.		