Payment Card Industry (PCI)

Point-to-Point Encryption (P2PE)

Reporting Instructions for P2PE Application Report on Validation (Application P-ROV)

Application P-ROV Reporting Instructions

For Applications used with
PCI P2PE Hardware/Hardware Standard v1.1, *and/or*
PCI P2PE Hardware/Hybrid Standard v1.1

July 2013

Document Changes

Date	Document Version	Description	Pages
August 2012	1.0	To introduce Application P-ROV Reporting Instructions for POI applications used in PCI Point-to-Point Encryption (P2PE) solutions. This document is intended for use with version 1.1 of the P2PE Standard, for Hardware/Hardware P2PE solutions.	
July 2013	1.1.1	To accommodate use of these Application P-ROV Reporting Instructions for POI applications used in Hardware/Hardware and/or Hardware/Hybrid PCI P2PE solutions. This document is intended for use with the following P2PE Standards: • P2PE Standard v.1.1.1 for Hardware/Hardware P2PE solutions • P2PE Standard v.1.1.1 for Hardware/Hybrid P2PE solutions.	

Table of Contents

1. Introduction

The PCI Point-To-Point Encryption (P2PE) Standard defines requirements and testing procedures for validating P2PE solutions, including requirements for validating the applications running on point-of-interaction (POI) devices in a P2PE solution. The six domains of P2PE requirements are:

- Domain 1: Encryption Device Management
- Domain 2: Application Security
- Domain 3: Encryption Environment
- Domain 4: Segmentation between Encryption and Decryption Environments
- Domain 5: Decryption Environment and Device Management (Hardware/Hardware) or Decryption Environment, Device and Systems Management (Hardware/Hybrid)
- Domain 6: P2PE Cryptographic Key Operations

Note: *P2PE Domain 2 Application Vendor assessments must be performed by a PA-QSA (P2PE).*

There are two sets of testing procedures for Domain 2: one for the application vendors and the development environment, and one for the solution providers and the solution environment. The Domain 2 application vendor assessment is documented in the Application P-ROV. The Domain 2 solution provider assessment is included in the Solution P-ROV together with assessment findings for all other P2PE domains.

At a high level, the Application P-ROV and Solution P-ROV address the P2PE Domains as follows:

Application P-ROV	Solution P-ROV
▪ Domain 2 – Application Vendor Assessment	▪ Domain 1 ▪ Domain 2 – Solution Provider Assessment ▪ Domain 3 ▪ Domain 4 (not applicable for hardware/hardware or hardware/hybrid) ▪ Domain 5 ▪ Domain 6

Note: *The Domain 2 requirements and testing procedures for Application Vendor Assessments are the same for both hardware/hardware and hardware/hybrid solutions.*

POI applications used in P2PE solutions are assessed as follows:

- POI applications which have access to clear-text account data must be evaluated against all P2PE Domain 2 Requirements. These applications must undergo both an Application Vendor Assessment and also be included in a Solution Provider Assessment for each solution they are used in.
- POI applications that do not have any access to clear-text account data are assessed only as part of the applicable Solution Provider Assessment.

A summary of the Domain 2 assessment processes for Application Vendors and Solution Providers is provided below:

	Domain 2 **Application Vendor Assessment**	**Domain 2** **Solution Provider Assessment**
Assessed entity:	• Application Vendor	• Solution Provider
Domain 2 Testing Procedures:	• Application Vendor Testing Procedures	• Solution Provider Testing Procedures
Report used to document assessment:	• Application P-ROV	• Solution P-ROV
Types of POI applications to be assessed:	• All POI applications with access to clear-text account data	• All POI applications with access to clear-text account data • All POI applications without access to clear-text account data (subset of Domain 2 requirements)
Description of assessment:	• The Domain 2 application vendor assessment covers the development environment and SDLC procedures, application coding, and verification of the application Implementation Guide content.	• The Domain 2 solution provider assessment includes ensuring the application's Implementation Guide is followed, and reviewing operational procedures and controls related to implementation and maintenance of the application within a particular P2PE solution.
Relationship to P2PE solution assessments:	• Domain 2 Application Vendor assessment is performed separately from any P2PE solution assessment that the application may be used in.	• Domain 2 Solution Provider assessment is included as part of the P2PE solution assessment for each solution the application is used in.
*Validation/Listing:**	• Application P-ROV submitted to PCI SSC for applications to be accepted and listed on PCI SSC List of Validated P2PE Applications	• Solution P-ROV submitted to PCI SSC for solutions to be listed on PCI SSC List of Validated P2PE Solutions • All POI applications included in solution listing

Note: *If an application is developed in-house by the solution provider for use only in their own solution, the application vendor testing procedures must be assessed separately to the solution provider testing procedures. Both an Application P-ROV and a Solution P-ROV are required.*

* *Please refer to the P2PE Program Guide for details of the P2PE application listing processes.*

The PA-QSA (P2PE) should complete the P2PE Application P-ROV using the applicable PCI SSC template and these Reporting Instructions. The template for creating and completing a P2PE Application Report on Validation (Application P-ROV) is defined in the *Application P-ROV Template for Applications used with PCI P2PE Hardware/Hardware Standard v1.1 and/or PCI P2PE Hardware/Hybrid Standard v1.1.* PA-QSA (P2PE)s must use the Application P-ROV Template to document the results of a P2PE application vendor assessment when validating an application for use in PCI P2PE solutions.

This document, *Application P-ROV Reporting Instructions for Applications used with PCI P2PE Hardware/Hardware Standard v1.1 and/or PCI P2PE Hardware/Hybrid Standard v1.1*, provides instructions and guidance for the PA-QSA (P2PE) (referred to throughout this document as"P2PE assessor"), to ensure that a consistent level of reporting is maintained.

Application P-ROVs must be completed in accordance with the PCI SSC Template and its corresponding Reporting Instructions.

All details relevant to the P2PE assessor's findings should be clearly identified and documented in the appropriate place within the Application P-ROV. The information recorded in the Application P-ROV must provide enough detail and coverage to verify that the application is compliant with all P2PE Domain 2 requirements.

Note: *The application vendor assessment and resulting Application P-ROV must be completed separately from any P2PE solution the application may be used in.*

Application P-ROV Content

At a high level, the Application P-ROV provides a comprehensive summary of testing activities performed and information collected during the application assessment. The P2PE assessor should clearly describe how the validation activities were performed and how the resultant findings were reached for each section of the P-ROV.

As defined in the *P2PE Application P-ROV Template for Applications used with PCI P2PE Hardware/Hardware Standard v1.1 and/or PCI P2PE Hardware/Hybrid Standard v1.1,* the Application P-ROV includes the following sections:

- Section 1: Contact Information and Report Date
- Section 2: Executive Summary
- Section 3: Details and Scope of Application Assessment
- Section 4: Findings and Observations

Section 1, "Contact Information and Report Date," includes the contact information for all parties involved, as well as the timeframe in which the assessment occurred, and the version of the P2PE Standard used to assess the application.

Section 2, "Executive Summary," contains a high-level overview of the application undergoing the review. The information provided in this section should give the reader an overall understanding of the P2PE application and how the application is typically implemented in a P2PE solution.

Section 3, "Details and Scope of Application Assessment," includes details about the application itself, as well as the application vendor's development environment and versioning methodology.

If these first three sections are not thoroughly and accurately documented, the assessment findings will not have proper context.

Section 4, "Findings and Observations," contains details of the P2PE assessor's findings for each P2PE Domain 2 requirement and testing procedure. The P2PE assessor should document how the testing procedures were performed and how the results of these procedures led the assessor to reach their findings. All findings and observations should be supported by and consistent with the information reported in Sections 1 through 3.

P2PE Assessor Documentation

A P2PE application assessment involves thorough testing and assessment activities from which the P2PE assessor will generate detailed work papers. These work papers contain comprehensive records of the assessment activities, and should be retained and protected in accordance with PCI SSC program requirements.

Not all the information in the work papers will be included in the P-ROV. The P-ROV is effectively a summary of all the evidence collected, and while the information presented in the P-ROV is derived from the work papers, the P-ROV itself should not be a replication of every piece of evidence collected.

P2PE Application Implementation Guide

As defined in Domain 2 of the P2PE Standard, application vendors are required to provide an application Implementation Guide to document the secure configuration specifics required throughout the P2PE Standard, and to instruct their customers (solution providers, integrators/resellers) on secure implementation of the application.

The Implementation Guide must be specific to each application and provide instructions on how to implement the application in a secure and compliant manner. It is not sufficient for the Implementation Guide to simply reiterate requirements from the P2PE Standard.

As part of the application assessment, the P2PE assessor must verify that the Implementation Guide is consistent with POI device vendor security guidance. The assessor must also follow the Implementation Guide instructions to install and configure the application, in order to verify that the instructions are accurate and effective, and that following the instructions results in the requirement being met.

The PA-QSA (P2PE) needs to be fully acquainted with the vendor's Implementation Guide before starting the assessment. The Implementation Guide should meet all requirements outlined in *Domain 2 Annex: Summary of Contents for the Implementation Guide for P2PE Applications*. An incomplete Implementation Guide will make it impossible to determine if the application meets P2PE requirements. An incomplete Implementation Guide must result in a non-compliant P-ROV

2. How to Use the P-ROV Reporting Instructions

These P-ROV Reporting Instructions identify the information and level of detail to be recorded in each section of the Application P-ROV, as defined in the P2PE Application P-ROV Template. Reporting instructions are provided for all sections of the Application P-ROV as follows:

Instructions for P-ROV sections 1-3 are presented in two columns:

- **Application P-ROV Section (P2PE Template) –** Corresponds to the PCI SSC Application P-ROV Template.
- **Reporting Details –** Outlines the information and level of detail to be provided for each item in the Application P-ROV template.

Instructions for P-ROV section 4 (Findings and Observations) are presented as follows:

- **P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures –** Corresponds to the requirements and application vendor testing procedures from Domain 2 of the P2PE Standard. Note that the Requirements are presented in rows and Testing Procedures are presented in the first column.
- **Reporting Details –** Outlines the information and level of detail to be provided for each P2PE testing procedure.

  Note: *The format of responses in an Application P-ROV is not expected to mirror the format in the Reporting Details column. The information provided in the Reporting Details column is bulleted for ease of readability. It is not intended that P2PE assessors follow this format when writing a P-ROV; however, assessors should ensure that all the required information is included in each response.*

- **Reporting Methodology** – Identifies which methods used by the P2PE assessor to collect the requisite evidence are to be reported for each testing procedure. Note that these methods may not be all-inclusive of those used during an assessment, and the P2PE assessor may need to employ additional methods to reach a compliant finding. Where additional methods are used to validate a finding, the P2PE assessor should include details of these in the Application P-ROV.

  Note: *The check marks (✓) in the Reporting Methodology column correspond to the instructions in the Reporting Details column. Together, the Reporting Details and Reporting Methodology provide the detailed reporting instruction for each testing procedure.*

Reporting Methodology

The reporting methodologies to be documented for each testing procedure are identified with a check mark (✓) in the Reporting Methodology column. The different reporting methodologies are described in the following table.

Reporting Methodology	Description
Observe systems, configurations	▪ P2PE assessor observes actual application and/or underlying system components. ▪ May include different configuration files, settings, or other parameters on each system observed. ▪ Observation may require assistance from appropriate personnel (e.g., developers or support personnel). ▪ Observation verifies that such parameters are set to produce a specified outcome.
Review Documentation	▪ P2PE assessor reviews documentation provided by the assessed entity. ▪ Documentation may include, but is not limited to: policies, procedures, processes, configuration standards, network diagrams, POI device vendor security guidance, other vendor documentation, reports, logs, audit trails, training materials, application manuals, and industry standards and best practices. ▪ Reviews of documentation verify the inclusion of items specified in the requirement/testing procedure.
Interview Personnel	▪ P2PE assessor interviews person or persons as appropriate for the requirement/testing procedure. ▪ Results of interviews may demonstrate that an action has or has not been performed, or that the interviewee has particular knowledge or understanding.
Observe processes, action, state	P2PE assessor observations may include, but are not limited to: ▪ Descriptions of testing methods used (for example, penetration testing techniques, forensic tools, etc.) ▪ Actions of people performing or not performing a task or procedures ▪ Behavior of applications or system components in response to an action ▪ Communications and network traffic ▪ Environmental conditions, including physical controls ▪ Walk-through of a process or procedure to verify the steps being performed ▪ Other evidence or output resulting from a task or action ▪ Observation may require assistance from appropriate personnel. ▪ Observation verifies a specified result or outcome.

Reporting Methodology	Description
Identify sample	▪ P2PE assessor selects a representative sample as appropriate for the requirement/testing procedure. ▪ Justification of sample provides assurance that controls are uniformly and consistently applied to all items.
Verify Implementation Guide content	▪ P2PE assessor reviews the application Implementation Guide (IG) provided by the application vendor ▪ Reviews of the Implementation Guide verify the inclusion of proper instructions and guidance as specified in the requirement/testing procedure ▪ Reviews of the application Implementation Guide verify that the included items are relevant to the specific application and provide accurate and effective configuration instructions (where applicable).

Note: *Reporting Methodology checkmarks are presented in orange-colored cells, except for "Verify Implementation Guide content" checkmarks, which are in green-colored cells. This is intended to assist the P2PE assessor identify Implementation Guide requirements from other types of testing methodologies.*

Application P-ROV Reporting Details

Instructions provided in the Reporting Details column correspond with one or more checked columns in the Reporting Methodologies column, for each requirement/testing procedure. Guidance for understanding the instructions used in the Reporting Details column is provided below.

- **Example instructions:** ***"Identify the document that defines…" and/or "Confirm the document includes…"***
  - Identify the reviewed document by name. *(**Note**: The term "document" may refer to multiple documents or documentation sets.)*
  - Where documentation is required to include specific procedures, the assessor must verify that the document contains actual procedures that the application vendor has implemented, and does not simply repeat the requirement or testing procedure.
  - The assessor should confirm that the documented processes, policies, or procedures are in place and being followed, and not merely that a document exists.
  - By identifying a document in the P-ROV, the assessor is attesting that the processes, policies, procedures, or practices contained in that document are sound.
  - Ensure all identified documents are also included in the list of all documentation reviewed, under "Details and Scope of Application Assessment" in the Application P-ROV.

- **Example instruction: *"Identify the personnel interviewed who confirm that…"***
  - Identify the roles or positions of the personnel interviewed.
  - The personnel identified must have confirmed that the requirement has been met—for example, that a process is followed or activities have been performed, etc.
  - If the testing procedure identifies personnel in a specific position to be interviewed, ensure that personnel in those positions are in fact interviewed.
    - If a specific position doesn't exist, the assessor should identify the appropriate personnel to interview. Explain how the identified personnel meet the intent of the specified position. For example, if a testing procedure includes interviewing software developers, the assessor should ensure that they interview personnel who perform software development as part of their job function. Note that such personnel may not have the exact title "Software Developer", but their title may still indicate that they are in fact the appropriate personnel to interview. If the job title does not reflect the specified role, the assessor should verify that the person interviewed does in fact perform the role applicable to the testing procedure.
  - Ensure all interviewed persons are also included in the list of personnel interviewed, under "Details and Scope of Application Assessment" in the Application P-ROV.
- **Example instruction: *"Identify the methods/tools used …"***
  - Identify the specific tools or methods used to perform a particular activity—for example, to perform a source code review, forensic examination or penetration test.
  - Include any details relevant to how the tools/methods were configured or used to provide assurance of their outcome
- **Example instruction: *"Confirm that the application was installed and configured only using the application vendor's documentation and Implementation Guide …"***
  - Provide a statement that the assessor installed and configured the application using only the instructions provided in the application vendor's documentation, including the Implementation Guide, with no additional or alternative configuration
  - This statement confirms that the instructions provided in the Implementation Guide and other vendor documentation result in the application being configured in a compliant manner, and that no further action is necessary for the requirement to be in place. If this is not verified, the requirement cannot be considered in place.
- **Example instruction: *"Describe how findings/results were used to verify that…"***
  - Describe how the results of a defined activity—for example, results from a source code review or forensic examination of application output—provided verification that the requirement has been met.
  - Describe any specific results or observations particularly relevant to the assessor's finding.

- **Example instruction: *"Describe how observation of process verified that…"***
  - Identify and describe the process, procedure, action, or state that was observed.
  - Identify any personnel or system components that were part of the observation.
  - Describe any situational or environmental factors relevant to the observation.
  - Describe how the observations provide assurance that the requirement/testing procedure is satisfied.
- **Example instruction: *"Identify the sample of…"***
  - Identify the number and type of items included in each sample—for example, 20 application change records.
  - Include any other details relevant to the sample—for example, the timeframe covered by the sample of change records.
  - It is not necessary to identify the names of every sampled item in the P-ROV; however, assessors may provide a list if it improves clarity or better explains their findings. Irrespective of whether item names are recorded in the P-ROV, the assessor must maintain a detailed record of each sampled item in their work papers.
  - Samples must be representative of the application vendors processes.
  - The sample size and types of items in the sample must be appropriate to provide assurance that the requirement has been met.
  - The sample size and types of items in the sample must be relevant for the particular requirement/testing procedure.
- **Example instruction: "Confirm the Implementation Guide includes…"**
  - Provide a statement that the assessor verified the application Implementation Guide contains the required information—for example, configuration instructions, guidance, device security information, etc.
  - It is not intended that sections of the Implementation Guide be copied into the P-ROV.
  - It is not sufficient for the Implementation Guide to simply restate requirements from the P2PE Standard: the Implementation Guide must provide details on how to install and/or configure the application to meet the requirement.
  - The assessor must validate that information provided in the Implementation Guide is accurate and effective (for example, instructions work correctly, file locations are accurately identified, etc.)

"Not Applicable" Requirements

If a P2PE requirement or testing procedure is determined to be "not applicable" (N/A), this should be clearly identified in the response. Findings of "in place" due to the control being "N/A" must include an explanation of why the control was determined to be not applicable and a detailed description of the testing and observations performed by the assessor to verify that the control is not applicable for the given application.

General Guidance

Do's and Don'ts:

DO:

- Follow the PCI SSC Application P-ROV template
- Complete all sections in the order specified, with consistent numbering, titles, and headings
- Read and understand the intent of each requirement and testing procedure
- Provide a response for every testing procedure
- Provide sufficient detail and information to demonstrate a finding of "in place"
- Describe how a requirement was verified as being met, not just that it was verified
- Ensure the response addresses all parts of the testing procedure
- Ensure the response covers all applicable application and/or system functions
- Perform an internal quality assurance review of the P-ROV for clarity, accuracy, and quality

DON'T:

- Don't submit an Application P-ROV to PCI SSC until all requirements are verified as being in place
- Don't include forward-looking statements or project plans in the assessment findings
- Don't simply repeat or echo the testing procedure in the response—the response should reflect actual activities performed by the assessor and how the results of those activities led the assessor to an "in place" finding
- Don't copy responses from one testing procedure to another—each response should apply to its corresponding testing procedure
- Don't copy responses from previous assessments
- Don't include information that is not relevant to the assessment or individual findings

3. Application P-ROV Reporting Instructions for PCI P2PE Hardware/Hardware and Hardware/Hybrid v1.1 Standards

Application P-ROV Section (P2PE Template)	Reporting Details
1. Contact Information and Report Date	
1.1 Contact information • Application vendor contact information • P2PE Assessor Company contact information • P2PE Assessor contact information • P2PE Assessor Quality Assurance (QA) primary contact information	**Provide contact details in the table provided for the following:** • P2PE Application Vendor • P2PE Assessor Company • P2PE Assessor who performed the assessment • P2PE Assessor Quality Assurance (QA) primary contact

1.2 Date and timeframe of validation	**Complete the following in the table provided:**
	• Date of Report – Provide the date this Application P-ROV was completed
	• Timeframe of assessment – Identify the timeframe during which the application was validated, including:
	  ○ The total time taken to complete the overall assessment (start date to completion date)
	  ○ Actual time the assessor spent performing assessment activities (including Lab time)

1.3 P2PE Version	**Complete the following in the table provided:** • Identify the version of the *P2PE Solution Requirements and Testing Procedures* used for the application assessment.

Application P-ROV Section (P2PE Template)	Reporting Details
2. Executive Summary	
2.1 Application Overview • Application Name • Application version (Note: wildcard version numbers are not permitted) • Description of application function/purpose • Description of how the application is sold, distributed, or licensed to third parties. • Description of how the application is designed (for example, standalone, in modules or as part of a suite) • Description of how application stores, processes and/or transmits account data	**In the table provided**: • Provide the exact name of the application • Identify the specific version(s) of the application assessed • Provide a brief description of application function/purpose—for example: ○ Types of transactions the application processes ○ Whether the application is designed for specific types of devices (for example, POS terminal, unattended kiosk, etc.) • Provide a brief description of how the application is sold, distributed, or licensed to third parties • Provide a brief description of how the application is designed. If the application is provided in modules or as part of a suite, identify which modules perform payment functions • Provide a brief description of how application stores, processes and/or transmits account data
2.2 Application Listing Details • Has the application been developed in-house by the solution provider for use only in their own solution? *(Yes/No)* ***If Yes, complete the following two bullet points:***	**In the table provided:** • Identify whether the application has been developed in-house by the solution provider for use only in their own solution, and is not going to be used for any other purpose or by any other party.
○ Identify the specific P2PE solution the application is intended for use with (Include solution provider company name and solution name).	○ If the application was developed in-house by the solution provider for use only in their own solution, provide the solution provider's company name and the name of the solution (as it is or will be listed) the application is to be used in.
○ Identify whether the application in this P-ROV is to be listed on the PCI SSC List of Validated P2PE Applications. (Yes/No) *(Continued on next page)*	○ If the application was developed in-house by the solution provider for use only in their own solution, identify whether the application in this P-ROV is to be listed on the PCI SSC List of Validated P2PE Applications. ***Note:*** *If the application is not to be included on the PCI SSC List of Validated P2PE Applications, the application will need to undergo a full Domain 2 Application Vendor assessment each time the solution is revalidated. See the P2PE Program Guide for further details.*

Application P-ROV Section (P2PE Template)	Reporting Details
• Is the application already listed on the PCI SSC List of Validated P2PE Applications? *(Yes/No)* *If Yes, complete the following:* ○ Provide PCI SSC listing number.	• Identify whether the application is already listed on the PCI SSC List of Validated P2PE Applications, and if so, provide the current listing number. *For example, if this application assessment is being performed as part of the application's revalidation or to add an updated version of the application to the PCI SSC list.*
2.3 Point-of-interaction devices (POIs) • Complete the following for all POI devices upon which the application was tested. ○ POI device details (manufacturer, model) ○ PTS approval number ○ POI device Hardware version # ○ POI device Firmware version #	**In the table provided:** • For every type of POI upon which the application was tested: ○ Identify the specific make and model of POI device. ○ Provide the PCI SSC PTS approval number for the POI device, as listed on the PCI SSC website. ○ Provide the POI device hardware version number that corresponds to the approval number, as listed on the PCI SSC website. ○ Provide the POI device firmware version number that corresponds to the approval number, as listed on the PCI SSC website.
2.4 Application data flows For each POI the application was tested on: • Provide a high level data flow diagram(s) that shows details of all flows of account data, including: ○ All flows and locations of encrypted account data (including data input, output and internally within the POI) ○ All flows and locations of cleartext account data (including data input, output and within the POI)	For each POI the application was tested on, provide one or more high level diagrams(s) showing details of all account data flows. • Ensure the diagram(s) are clearly labeled and include the following: ○ All flows and locations of encrypted account data (including data input, output and within the POI) ○ All flows and locations of cleartext account data (including data input, output and within the POI)

Application P-ROV Section (P2PE Template)	Reporting Details

• Identify the following for each data flow:
  ○ How and where account data is transmitted, processed and/or stored
  ○ The types of account data involved (for example, full track, PAN, expiry date, etc.)
  ○ All components involved in the transmission, processing or storage of account data
Note: *Include all types of data flows, including any output to hard copy / paper media.*
	• For each account data flow, ensure the diagram(s) are clearly labeled and that the following is identified (either in the diagrams or through separate descriptions):
	  ○ How and where account data is transmitted, processed and/or stored
	  ○ The types of account data involved (for example, full track, PAN, expiry date, etc.)
	  ○ All components involved in the transmission, processing or storage of account data
	• Ensure all types of data flows are documented, including any output to hard copy / paper media (for example, printing of receipts or transaction reports).

2.5 Versioning Methodology
• Describe vendor's versioning methodology as follows:
  ○ Description of how vendor indicates application changes via their version numbers
  ○ Define what types of changes the vendor includes as a "No Impact" change
	In the table provided:
	• Provide details of the vendor's versioning methodology, to describe/illustrate how the vendor defines changes to the application via their version numbers.
	• Identify what types of changes to the application the vendor includes as No Impact changes.
	Note: *Refer to the P2PE Program Guide for information on what constitutes a No Impact change*

2.6 Multi-Acquirer / Multi-Solution Applications
• Identity if the application is capable of supporting multiple P2PE solutions, or multiple acquirers or payment processors at the same time.
• If Yes, provide a brief description of how management of the application is to be shared between multiple P2PE solution providers / acquirers / payment processors.
	In the table provided:
	• Identify whether the application is capable of supporting multiple P2PE solutions, or multiple acquirers or payment processors at the same time, and briefly describe how the assessor verified this.
	• If the application is capable of supporting multiple P2PE solutions, multiple acquirers, or multiple payment processors at the same time:
	  ○ Describe how the application supports multiple solutions / acquirers / payment processors.
	  ○ Describe how management of the application is to be shared between the multiple parties.
	• Include any controls provided within the application to support and manage the multiple parties

Application P-ROV Section (P2PE Template)	Reporting Details
2.7 Implementation Guide • For each type of POI the application was tested on (as identified in 2.3 above), provide details of the application Implementation Guide used and validated for this assessment: ○ Title of the application Implementation Guide ○ Date of the application Implementation Guide ○ Version of the application Implementation Guide ○ Provide details of any additional vendor documentation that provides guidance or instruction for installing and configuring the application that are not provided within the Implementation Guide (for example, user guides, installation instructions etc.).	**In the table provided:** • For each type of POI the application was tested on (as identified in 2.3): ○ Provide the title of the application Implementation Guide ○ Provide the date of the application Implementation Guide ○ Provide the version of the application Implementation Guide ○ Identify any additional vendor documentation that provides guidance or instruction for installing and configuring the application, that are required by solution providers / installers of the application, including: ▪ Title ▪ Date ▪ Version ***Note:*** *If there is more than one Implementation Guide and/or set of installation instructions—for example, if the application vendor provides separate Implementation Guides and/or installation instructions for different types of POI devices—the assessor should make copies of the table provided as needed to report their findings for each POI device type that was assessed.*

Application P-ROV Section (P2PE Template)	Reporting Details
3. Details and Scope of Application Assessment	
3.1 Application Details For each POI the application was tested on • Provide detailed descriptions and/or diagrams to illustrate how the application functions in a typical implementation.	For each POI the application was tested on: • Use detailed descriptions and/or diagrams to describe how the application functions in a typical implementation. Include all functions of the application, for example: ○ Authorization ○ Capture ○ Settlement ○ Chargeback ○ Any other application functions as applicable
• For all application functions, provide the following: ○ Description of all application processes related to each function	• For all application functions identified, provide the following: ○ Detailed descriptions and/or diagrams that clearly illustrate all application processes, for example: ▪ Inputs and outputs ▪ Error conditions ▪ Encryption and authentication mechanisms ▪ Other processes of the application relevant to the performance of its function
○ Description of all communication channels, connection methods and communication protocols used by the application, for all internal and external communication channels.	○ Include details of communication channels, connection methods and communication protocols for all internal and external communication channels, including: ○ All internal interfaces and communications between the application and POI resources—such as POI firmware, device components, etc. ○ All internal interfaces and communications between the application and other applications or application components on the POI ○ All external interfaces and communications between the application and applications/systems/entities outside of the POI (include all LAN, WAN and Internet connections) ○ The diagrams should identify all relevant systems and the relationship between them.
○ Details of any protection mechanisms (for example, encryption, truncation, masking, etc.) applied to account data by the application	○ Provide a detailed description of any protection mechanisms applied to account data by the application (for example, encryption, truncation, masking, etc.), including where and how they are applied
○ Other necessary application functions or processes, as applicable	○ Provide a detailed description of any other necessary application functions or processes, as applicable

Application P-ROV Section (P2PE Template)	Reporting Details
• Identify any functionality of the application that was not included in the assessment	• Identify any functionality of the application that was not included in the assessment, and explain why it was excluded.

3.2 Application dependencies
• Identify and list all application dependencies, including software and hardware components required for necessary functioning of the application:
  ○ Description of component necessary for application functioning
  ○ Type of component (e.g., software, hardware)
  ○ Role of component
	In the table provided:
	• Identify and list all application dependencies, including software and hardware components, as follows:
	  ○ Provide a description of each component necessary for application functioning—include component vendor, as well as the name and version of the component product
	  ○ Identify the type of component (e.g., software, hardware)
	  ○ Describe the role of each component and how it is necessary for functioning of the application

3.3 Application authentication mechanisms
• Describe the application's end to end authentication methods, as follows:
  ○ Authentication mechanisms
  ○ Authentication database
  ○ Security of authentication data storage
	In the table provided:
	• Describe the application's end to end authentication methods, including details of:
	  ○ The application's authentication mechanism(s),
	  ○ The application's authentication database, and
	  ○ How authentication data (for example, passwords, pins, tokens, etc.) is secured in storage (for example, encryption mechanisms, etc.)

3.4 Facilities
• Assessor Lab environment
  ○ Identify and describe the lab environment used for this assessment, including whether the lab was provided by the P2PE assessor or the application vendor.
  ○ Address of the lab environment used for this assessment
	In the table provided:
	• Provide details of the lab environment used for this assessment, including:
	  ○ A brief description of the lab setup (for example, number and types of systems, platforms, testing tools, etc.), and whether the lab was provided by the P2PE assessor or the application vendor
	  ○ The address of the Lab

• Application vendor facilities INCLUDED in the assessment
  ○ Description and purpose of application vendor facility included in application assessment
  ○ Address of facility
	• Provide details of application vendor facilities included in the assessment, using the table provided as follows:
	  ○ Description and purpose of application vendor facility included in application assessment (for example, development environment)
	  ○ Address of facility

Application P-ROV Section (P2PE Template)	Reporting Details

• Application vendor facilities EXCLUDED from the assessment
  ○ Description and purpose of application vendor facility excluded from application assessment
  ○ Address of facility
  ○ Explanation why the facility was excluded
	• Identify and describe any locations or environments relevant to the application's development that were EXCLUDED from the scope of the review as follows:
	  ○ Provide a description and identify the purpose of the application vendor facility that was excluded from the application assessment
	  ○ Provide the address of facility excluded from the assessment
	  ○ Provide an explanation why the facility was excluded from the assessment

3.5 Documentation and personnel interviews
• Provide list of all documentation reviewed for this application assessment
  ○ Document Name (including version, if applicable)
  ○ Brief description of document purpose
  ○ Document date
	In the table provided:
	• Provide list of all documentation reviewed for this application assessment (including but not limited to application vendor policies and procedures, device vendor security guidance, etc.), as follows:
	  ○ Document Name (including version, if applicable)
	  ○ Brief description of document purpose
	  ○ Document date

• Provide list of all personnel interviewed for this application assessment
  ○ Name
  ○ Company
  ○ Job Title
  ○ Topics covered
	• Provide list of all personnel interviewed for this application assessment, as follows:
	  ○ Name – Provide the individual's first and last name
	  ○ Company – Provide the company/organization where the individual works
	  ○ Job Title – Provide the individual's job title
	  ○ Topics covered – Provide a brief description of all topics covered during interviews with the person

Application P-ROV Section (P2PE Template)	Reporting Details
4. Findings and Observations	

• P2PE assessors must use the PCI SSC template	• Ensure that the PCI SSC defined template is used for the Application P-ROV
	• Ensure that the correct Application P-ROV template is used according to the:
	  ○ Type of P2PE solution that the application is intended for use with
	  ○ Version of P2PE that the assessment was based on

• Include descriptions of tests performed other than those included in the testing procedures column	• Describe tests performed other than those included in the testing procedures column. • Identify any resultant findings that the assessor feels are relevant to the assessment, but that do not fall under a P2PE requirement:
• If the assessor determines that a requirement is not applicable for a given application, an explanation must be included in the "In Place" column for that requirement.	• If a requirement is deemed to be "in place" due to being N/A, document as such in the "Findings" column, and provide details of how the requirement was verified as being N/A.

Reporting Details and Methodology for P2PE Domain 2 Requirements

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2A-1 The application does not retain PAN or SAD after application processing is completed.							
2A-1.1 The application does not store PAN or SAD data after processing is completed (even if encrypted). *Storage of encrypted PAN data is acceptable during the business process of finalizing the payment transaction if needed (for example, offline transactions). However, at all times, SAD is not stored after the completion of the transaction.*							
2A-1.1.a Examine the application's *Implementation Guide* required at 2C-3 of this document and verify it contains a detailed description of the function of the application, including: • How it uses PAN or SAD for its application processing, and • How it ensures the application does not store PAN or SAD after the application's processing is complete.	• Confirm that the application's Implementation Guide includes a detailed description of the function of the application including: ○ How it uses PAN or SAD for its application processing, and ○ How it ensures the application does not store PAN or SAD after the application's processing is complete.						✓
2A-1.1.b Perform a source-code review to verify that the application is coded such that PAN and SAD are not stored after application processing is completed.	• Identify the methods/tools used to review source code • Describe how the findings from the source-code review were used to verify that the application is coded such that PAN and SAD are not stored after application processing is complete.	✓			✓		
2A-1.1.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Use forensic tools and/or methods (commercial tools, scripts, etc.) to examine all output created by the application and verify that, by following the *Implementation Guide* instructions, PAN and SAD are not stored after application processing is completed.	• Confirm that the application was installed and configured using only the application vendor's documentation and the application's Implementation Guide (with no additional configuration required). • Identify the forensic tools and/or methods used to examine all output created by the application. • Identify the application output examined. • Describe how examination of the output using forensic tools and/or methods verified that PAN and SAD are not stored after application processing was complete.	✓			✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	Reporting Methodology					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2A-1.2 A process is in place to securely delete any PAN or SAD stored during application processing.							
2A-1.2.a Examine the application's *Implementation Guide* required at 2C-3 of this document and verify it describes the methodology or process used by the application to securely delete any PAN or SAD if stored during application processing.	• Confirm the Implementation Guide describes the methodology or process used by the application to securely delete any PAN or SAD if stored during application processing.						✓
2A-1.2.b Perform a source-code review and verify that the methodology or process provided by the application vendor renders all stored PAN and SAD irrecoverable once application processing is completed, in accordance with industry-accepted standards for secure deletion of data.	• Identify the methods/tools used to review source code. • Describe how the findings from the source-code review were used to verify that the methodology or process provided by the application vendor renders all stored PAN and SAD irrecoverable once application processing is completed, in accordance with industry-accepted standards for secure deletion of data.	✓			✓		
2A-1.2.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide* Use forensic tools and/or methods (commercial tools, scripts, etc.) to examine all output created by the application and verify that, by following the *Implementation Guide* instructions, that the methodology or process provided by the application vendor renders all PAN and SAD data irrecoverable, in accordance with industry-accepted standards for secure deletion of data, once the business process of the application is completed.	• Confirm that the application was installed and configured only using the application vendor's documentation and the application's Implementation Guide (with no additional configuration required). • Identify the forensic tools and/or methods used to examine all output created by the application. • Identify the application output examined. • Describe how examination of the output using forensic tools and/or methods verified that the methodology or process (described in the Implementation Guide) renders all PAN and SAD data irrecoverable once the business process of the application is completed.	✓			✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2A-2 The application does not transmit clear-text PAN or SAD outside of the device, and only uses communications methods included in the scope of the PCI-approved POI device evaluation.							
2A-2.1 The application only exports PAN or SAD data that has been encrypted by the firmware of the PCI-approved POI device, and does not export clear-text PAN or SAD outside of the device. ***Note:*** *Output of clear-text data that is verified as being unrelated to any of the PCI payment brands is acceptable. The security of this process is assessed at Requirement 2A-2.4.*							
2A-2.1.a Examine the application's *Implementation Guide* required at 2C-3 of this document and verify it contains a description of the application's function including the following: • That the application does not output clear-text account data outside of the device; • Whether the application passes encrypted account data outside of the device; and • If the application passes encrypted account data outside of the device, that the application only exports PAN or SAD that has been encrypted by the approved SRED functions of the PCI-approved POI device.	• Confirm that the Implementation Guide includes a description of the application's function including: ○ The application does not output clear-text data outside of the device. ○ Whether the application passes encrypted account data outside of the device. ○ If the application passes encrypted account data outside of the device, that the application only exports PAN or SAD that has been encrypted by the approved SRED functions of the PCI-approved POI device.						✓
2A-2.1.b Perform a source-code review and verify that the application never outputs clear-text account data outside of the device.	• Identify the methods/tools used to review source code. • Describe how findings from the source-code review were used to verify that the application never outputs clear-text account data outside of the device.	✓			✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	Reporting Methodology					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2A-2.1.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Use forensic tools and/or methods (commercial tools, scripts, etc.) to examine all output created by the application and verify that, by following the *Implementation Guide* instructions, the application does not output clear-text account data outside of the device.	• Confirm that the application was installed and configured only using the application vendor's documentation and the application's Implementation Guide (with no additional configuration required). • Identify the forensic tools and/or methods used to examine all output created by the application. • Identify the application output examined. • Describe how examination of the output using forensic tools and/or methods verified that the application does not output clear-text account data outside of the device.	✓			✓		
2A-2.2 The application only uses internal communication methods (including all inter-process communication and authentication methods) included in the PCI-approved POI device evaluation. These internal communication methods must be documented. ***Note:*** *This applies to all internal communications within the device, including when account data is passed between applications, or to an area of memory or internal file that could be accessed by other applications, or back to the approved firmware of the POI.*							

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2A-2.2.a Examine the POI device vendor's security guidance to determine which internal communication methods (including for authentication) are approved in the PCI-approved POI device evaluation. Review the application's *Implementation Guide* required at 2C-3 of this document and confirm that it includes the following: • A list of internal communication methods included in the POI device vendor's security guidance • A list of which approved internal communications methods are used by the application. • A description of where internal communications are used by the application to pass clear-text account data within the device (for example, from the application to other applications, to an area of memory or internal file that could be accessed by other applications, or back to the approved firmware of the POI) • How to configure the application to use the approved internal communication methods • Guidance that use of any other method for internal communication is not allowed.	• Identify the POI device vendor's security guidance document that defines the internal communication methods (including for authentication) approved in the PCI-approved POI device evaluation. • Confirm that the Implementation Guide includes the following from the POI Device Vendor's Security Guidance: ○ A list of internal communication methods included in the POI device vendor's security guidance. ○ A list of which approved internal communications methods used by the application. ○ A description of where internal communications are used by the application to pass clear-text account data within the device. ○ Instructions on how to configure the application to use the approved internal communication methods. ○ Guidance stating that the use of any other method for internal communication is not allowed.		✓				✓
2A-2.2.b Perform a source-code review and verify that the application only uses those inter-process communication methods approved as part of the PCI-approved POI device evaluation.	• Identify the methods/tools used to review source code. • Describe how findings from the source-code review were used to verify that the application only uses those inter-process communication methods approved as part of the PCI-approved POI device evaluation.	✓			✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2A-2.2.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Use forensic tools and/or methods (commercial tools, scripts, etc.) to examine all output created by the application and verify that, by following the *Implementation Guide*, the application only uses approved inter-process communications methods (including authentication methods) for all communications within the device, including; • All flows and storage of clear-text account data, between applications • All flows and storage of clear-text account data between the application and the approved firmware of the POI.	• Confirm that the application was installed and configured only using the application vendor's documentation and the application's Implementation Guide (with no additional configuration required). • Identify the forensic tools and/or methods used to examine all output created by the application. • Identify the application output examined. • Describe how examination of the output using the forensic tools and/or methods verified that the application only uses approved inter-process communications methods (including authentication methods) for all communications within the device, including: ○ All flows and storage of clear-text account data between applications ○ All flows and storage of clear-text account data between the application and the approved firmware of the POI	✓			✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	Reporting Methodology					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2A-2.3 The application only uses external communication methods included in the PCI-approved POI device evaluation. *For example, the POI may provide an IP stack approved per the PTS Open Protocols module that allows for the use of the SSL/TLS protocol, or the device may provide serial ports or modems approved by the PTS evaluation to communicate transaction data encrypted by its PCI PTS SRED functions.* Security of applications where the POI device implements an IP stack is covered at Requirement 2B-2.1.							
2A-2.3.a Examine the POI device vendor's security guidance to determine which external communication methods are approved via the PCI-approved POI device evaluation. Review the application's *Implementation Guide* required at 2C-3 of this document and verify that it contains the following instructions and that they are consistent with the POI device vendor's security guidance: • A list of the external communication methods included in the POI device vendor's security guidance • A list of which approved external communications methods are used by the application • A description of where external communications are used by the application • Instructions for how to configure the application to use only those approved methods • Guidance that use of any other methods for external communications is not allowed	• Identify the POI Device Vendor's Security Guidance documentation that defines external communication methods approved via the PCI-approved POI device evaluation. • Confirm that the Implementation Guide includes the following from the POI Device Vendor's Security Guidance: ○ A list of the external communication methods included in the POI device vendor's security guidance ○ A list of which approved external communications methods are used by the application ○ A description of where external communications are used by the application ○ Instructions for how to configure the application to use only those approved methods ○ Guidance that use of any other methods for external communications is not allowed		✓				✓
2A-2.3.b Perform a source-code review and verify that the application does not implement its own external communication methods (for example, does not implement its own IP stack).	• Identify methods/tools used to review source code. • Describe how findings from the source-code review were used to verify that the application does not implement its own external communication methods.	✓			✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2A-2.3.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Use forensic tools and/or methods (commercial tools, scripts, etc.) to examine all output created by the application and verify that, by following the *Implementation Guide*: • The application only uses only the external communication methods) included in the POI device vendor's security guidance for all external communications.	• Confirm that the application was installed and configured only using the application vendor's documentation and the application's Implementation Guide (with no additional configuration required). • Identify the forensic tools and/or methods (used to examine all output created by the application. • Identify the application output examined. • Describe how the examination of the output using the forensic tools and/or methods verified that the application only uses only the external communication methods included in the POI device vendor's security guidance for all external communications.	✓			✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2A-2.4 Ensure that any application functions (for example, "whitelists") that allow for the output of clear-text data limits that output to *only* non-PCI payment brand accounts/cards, and that additions or changes to application functions are implemented as follows: • Cryptographically authenticated by the PCI-approved POI device's firmware • Implemented only by authorized personnel • Documented as to purpose and justification • Reviewed and approved prior to implementation ***Note:*** *Requirement 2C-2.1.2 prohibits unauthenticated changes or updates to applications or application functions (for example, "whitelists").*							
2A-2.4.a Examine the application's *Implementation Guide* required at 2C-3 of this document and verify it contains details to describe any application functions that allow for the output of clear-text card data (for example, through the use of 'whitelists' of BIN ranges), and provides instructions as follows: • Any such application functions are only allowed for non-PCI payment brand accounts/cards. • How to establish application authentication using strong cryptography, with the approved SRED firmware of the POI device. • Only authorized personnel must be used for signing and adding application functions for output of clear-text data.	• Confirm that the application's Implementation Guide contains a description of any application functions that allow for the output of clear-text card data. • If any application functions allow for the output of clear-text card data, confirm that the Implementation Guide provides instructions as follows: ○ Any such application functions are *only allowed* for non-PCI payment brand accounts/cards. ○ How to establish application authentication using strong cryptography, with the approved SRED firmware of the POI device. ○ Only authorized personnel must be used for signing and adding application functions for output of clear-text data.						✓

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2A-2.4.b Perform a source-code review and verify that the application functions are limited as follows: • The application is able to limit output to non-PCI payment brand accounts/cards only. • The application requires use of the PCI-approved POI device's firmware for cryptographic authentication.	• Identify methods/tools used to review source code. • Describe how findings from the source-code review were used to verify that the application functions are limited as follows: ○ The application is able to limit output to non-PCI payment brand accounts/cards only. ○ The application requires use of the PCI-approved POI device's firmware for cryptographic authentication.	✓			✓		
2A-2.4.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Use forensic tools and/or methods (commercial tools, scripts, etc.) to examine all output created by the application and verify that, when the *Implementation Guide* is followed, the following is in place: • Output of clear-text data is allowed only for non-PCI payment brand accounts/cards. • Application functions are authenticated using strong cryptography by the approved SRED firmware of the POI device.	• Confirm that the application was installed and configured only using the application vendor's documentation and the application's Implementation Guide (with no additional configuration required). • Identify the forensic tools and/or methods used to examine all output created by the application. • Identify the application output examined. • Describe how examination of the output using the forensic tools and/or methods verified that: ○ Output of clear-text data is allowed only for non-PCI payment brand accounts/cards. ○ Application functions are authenticated using strong cryptography by the approved SRED firmware of the POI device.	✓			✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	Reporting Methodology					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2A-3 All applications without a business need do not have access to account data. ***Note:*** *This Requirement has no applicable testing procedures for the Application Vendor assessment*							
2B-1 The application is developed according to industry-standard software development life cycle practices that incorporate information security.							
2B-1.1 Applications are developed based on industry best practices and in accordance with the POI device vendor's security guidance, and information security is incorporated throughout the software development life cycle. These processes must include the following:							
2B-1.1.a Examine written software development processes to verify the following: • Processes are based on industry standards and/or best practices. • Information security is included throughout the software development life cycle	• Identify the document that defines the application vendor's software development processes. • Confirm that the documented software development processes are defined as follows: ○ Processes are based on industry standards and/or best practices. ○ Information security is included throughout the software development life cycle		✓				
2B-1.1.b Examine the POI device vendor's security guidance, and verify that any specified software development processes are: • Incorporated into the application developer's written software development processes • Implemented per the POI device vendor's security guidance.	• Identify the document that defines the POI device vendor's security guidance. • Identify the document that defines the application vendor's software development processes. • Confirm that any software development practices specified in the POI Device Vendor's Security Guidance are included in the application vendor's written software development processes. • Describe how the software development practices specified in the POI Device Vendor's Security Guidance were observed to be implemented by the application vendor.		✓		✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	Reporting Methodology					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-1.1.c Examine the application's *Implementation Guide* required at 2C-3 of this document and verify it provides information from the POI device vendor's security guidance applicable to the solution provider (for example, application configuration settings which are necessary for the application to function with the device).	• Confirm that the Implementation Guide includes any information from the POI device vendor's security guidance (identified in 2B-1.1.b) applicable to the solution provider.		✓				✓
2B-1.1.d Verify each of the items at 2B-1.1.1 through 2B-1.1.3 by performing the following: • Examine written software development processes • Interview software developers • Examine the application product							
2B-1.1.1 Live PANs are not used for testing or development.							
2B-1.1.1 Live PANs or SAD are not used for testing or development.	• Identify the document that defines processes for live PANs or SAD not to be used for testing or development. • Identify software developers interviewed who confirm that live PAN and SAD are not used for testing or development. • Describe how observation of the application product verified that live PANs or SAD are not used for testing or development.		✓	✓	✓		
2B-1.1.2 Test data and accounts are removed before release to customer.							
2B-1.1.2 Test data and accounts are removed before release to customer.	• Identify the document that defines processes for test data and accounts to be removed before release to customer. • Identify software developers interviewed who confirm that test data and accounts are removed before release to customer. • Describe how observation of the application product verified that test data and accounts are removed before release to customer.		✓	✓	✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-1.1.3 Custom application accounts, user IDs, and passwords are removed before applications are released to customers							
2B-1.1.3 Custom application accounts, user IDs, and passwords are removed before the application is released.	• Identify the document that defines processes for custom application accounts, user IDs, and passwords to be removed before the application is released. • Identify software developers interviewed who confirm that custom application accounts, user IDs, and passwords are removed before the application is released. • Describe how observation of the application product verified that custom application accounts, user IDs, and passwords are removed before the application is released.		✓	✓	✓		
2B-1.2 Application code and any non-code configuration options, such as "whitelists," are reviewed prior to release and after any significant change, using manual or automated vulnerability-assessment processes to identify any potential vulnerabilities or security flaws. The review process includes the following:							
2B-1.2 Confirm the developer performs reviews for all significant application code changes and alterations to code that manages security-sensitive configuration options, such as card '"whitelists" (either using manual or automated processes), as follows:							
2B-1.2.1 Review of code changes by individuals other than the originating author, and by individuals who are knowledgeable in code-review techniques and secure coding practices.							

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-1.2.1 Code changes are reviewed by individuals other than the originating author, and by individuals who are knowledgeable in code-review techniques and secure coding practices.	• Identify the document that defines procedures for performing reviews for all significant application code changes and for alterations to code that manage security-sensitive configuration options. • Confirm that documented procedures include code changes to be reviewed by individuals other than the originating author, and who are knowledgeable in code-review techniques and secure coding practices. • Identify individuals responsible for code reviews interviewed who confirm that code changes are reviewed by individuals other than the originating author. • Describe how the individuals responsible for code reviews demonstrated that they are knowledgeable in code-review techniques and secure coding practices. • Describe how observation of code review processes verified that code changes are reviewed by individuals other than the originating author, and who are knowledgeable in code-review techniques and secure coding practices.		✓	✓	✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-1.2.2 Review of changes to security-sensitive configuration options, such as whitelists, to confirm that they will not result in the exposure of PCI payment-brand accounts/cards.							
2B-1.2.2 Changes to code that manages security-sensitive configuration options, such as whitelists, are reviewed to confirm that they will not result in the exposure of PCI payment-brand accounts/cards.	• Confirm that documented code review procedures (identified in 2B-1.2.1) require that changes to code that manages security-sensitive configuration options, such as whitelists, are reviewed to confirm that they will not result in the exposure of PCI payment-brand accounts/cards. • Identify individuals responsible for code reviews interviewed who confirm that changes to code that manages security-sensitive configuration options, such as whitelists, are reviewed to confirm that they will not result in the exposure of PCI payment-brand accounts/cards. • Describe how observation of code review processes verified that reviews of changes to code that manages security-sensitive configuration options ensures that they will not result in the exposure of PCI payment-brand accounts/cards.		✓	✓	✓		
2B-1.2.3 Performing code reviews to ensure code is developed according to secure coding guidelines.							
2B-1.2.3 Code reviews ensure code is developed according to secure coding guidelines.	• Confirm that documented code review procedures (identified in 2B-1.2.1) require that code reviews are performed to ensure code is developed according to secure coding guidelines. • Identify individuals responsible for code reviews interviewed who confirm that code reviews ensure code is developed according to secure coding guidelines. • Describe how code review processes were observed to ensure that code is developed according to secure coding guidelines.		✓	✓	✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-1.2.4 Confirming that appropriate corrections are implemented prior to release.							
2B-1.2.4 Appropriate corrections are implemented prior to release.	• Confirm that documented code review procedures (identified in 2B-1.2.1) require that appropriate corrections are implemented prior to release. • Identify individuals responsible for code reviews interviewed who confirm that appropriate corrections are implemented prior to release. • Describe how observation of code review processes verified that appropriate corrections to reviewed code are implemented prior to release.		✓	✓	✓		
2B-1.2.5 Review and approval of review results by management prior to release.							
2B-1.2.5 Review results are reviewed and approved by management prior to release.	• Confirm that documented code review procedures (identified in 2B-1.2.1) require that code review results are reviewed and approved by management prior to release. • Identify individuals responsible for code reviews interviewed who confirm code review results are reviewed and approved by management prior to release. • Describe how observation of code review processes verified that code review results are reviewed and approved by management prior to release.		✓	✓	✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-1.3 Develop applications based on secure coding guidelines. Cover prevention of common coding vulnerabilities in software development processes.							
2B-1.3.a Obtain and review software development processes for applications. Verify the process includes training in secure coding techniques for developers, based on industry best practices and guidance.	• Identify the document that defines software development processes for applications. • Confirm the documented processes include training in secure coding techniques for developers, based on industry best practices and guidance. • Identify the industry standards and/or best practices used.		✓				
2B-1.3.b Interview a sample of developers to confirm that they are knowledgeable in secure coding techniques.	• Identify the developers interviewed • Describe how the developers interviewed demonstrated that they are knowledgeable in secure coding techniques.			✓			
2B-1.3.c Verify that applications are not vulnerable to common coding vulnerabilities by performing manual or automated penetration testing that specifically attempts to exploit vulnerabilities relevant to the application (an example of such a vulnerability would include buffer overflows.)	• Describe the penetration testing techniques used (including whether manual or automated (or both) techniques were used) to specifically attempt to exploit vulnerabilities relevant to the application. • Describe how results of the penetration testing verified that the application is not vulnerable to common coding vulnerabilities.				✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	Reporting Methodology					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-1.4 All changes to application must follow change-control procedures. The procedures must include the following:							
2B-1.4.a Obtain and examine the developer's change-control procedures for software modifications, and verify that the procedures require the following: • Documentation of customer impact • Documented approval of change by appropriate authorized parties • Functionality testing to verify that the change does not adversely impact the security of the device • Back-out or application de-installation procedures	• Identify the document that defines the application vendor's change control procedures. • Confirm that procedures are defined to include: ○ Documentation of customer impact ○ Documented approval of change by appropriate authorized parties ○ Functionality testing to verify that the change does not adversely impact the security of the device ○ Back-out or application de-installation procedures		✓				
2B-1.4.b Examine the application's *Implementation Guide* required at 2C-3 of this document and verify it includes the following: • Documentation about the impact of the change • Instructions about how to back out or de-install applications.	• Confirm that the application's Implementation Guide includes details of change-control procedures, including: ○ Documentation about the impact of the change ○ Instructions about how to back out or de-install applications.						✓
2B-1.4.c Examine recent application changes, and trace those changes back to related change-control documentation. Verify that, for each change examined, the following was documented according to the change-control procedures:	• Identify the sample of recent application changes examined for Requirements 2B-1.4.1 through 2B-1.4.4 below. • Describe how, for each change examined, the changes were traced back to related change-control documentation:		✓		✓	✓	

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-1.4.1 Documentation of impact							
2B-1.4.1 Verify that documentation of customer impact is included in the change-control documentation for each change.	• For each examined change: ○ Identify the related change-control documentation examined. ○ Describe how examination of the changes verified that documentation of customer impact is included in the change-control documentation.		✓		✓		
2B-1.4.2 Documented approval of change by appropriate authorized parties							
2B-1.4.2 Verify that documented approval by appropriate authorized parties is present for each change.	• For each examined change: ○ Identify the related change-control documentation examined. ○ Describe how examination of the changes verified that documented approval by appropriate authorized parties is present for each change.		✓		✓		
2B-1.4.3 Functionality testing to verify that the change does not adversely impact the security of the device							
2B-1.4.3.a For each sampled change, verify that functionality testing was performed to verify that the change does not adversely impact the security of the device.	• For each examined change: ○ Identify the related change-control documentation examined. ○ Describe how examination of the changes verified that: ▪ Functionality testing was performed ▪ Functionality testing verified that the change does not adversely impact the security of the device.		✓		✓		
2B-1.4.3.b Verify that all changes (including patches) are tested per secure coding guidance before being released.	• For each examined change: ○ Identify the related change-control documentation examined. ○ Describe how examination of the changes verified that all changes are tested per secure coding guidance before being released.		✓		✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	Reporting Methodology					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-1.4.4 Back-out or application de-installation procedures							
2B-1.4.4 Verify that back-out or product de-installation procedures are prepared for each change.	• For each examined change: ○ Identify the related change-control documentation examined. ○ Describe how examination of the changes verified that back-out or product de-installation procedures are prepared for each change.		✓		✓		
2B-2 The application is implemented securely, including the secure use of any resources shared between different applications.							
2B-2.1 The application is developed in accordance with the POI device vendor's security guidance, including specifying that If an application uses an IP stack, it must use the IP stack approved as part of the PCI-approved POI device evaluation. ***Note:*** *POI device vendor security guidance is intended for application developers, system integrators, and end-users of the platform to meet requirements in the PCI PTS Open Protocols module as part of a PCI-approved POI device evaluation.*							
2B-2.1 Examine the POI device vendor's security guidance to determine which IP stack was approved via the PCI-approved POI device evaluation. Review the application's *Implementation Guide* required at 2C-3 of this document and confirm it includes the following: • A description of the IP stack implemented in the POI device • Confirmation that the IP stack used by the application is the same one included in the POI device vendor's security guidance	• Identify the POI device vendor's security guidance documentation that identifies which IP stack was approved via the PCI-approved POI device evaluation. • Confirm that the application's Implementation Guide includes the following from the POI Device Vendor's Security Guidance: ○ A description of the IP stack implemented in the POI device ○ Confirmation that the IP stack used by the application is the same one included in the POI device vendor's security guidance		✓				✓

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-2.1.1 If an application uses the POI device's IP stack and any of the related OP services, the application must securely use, and integrate with, the following device platform components in accordance with the POI device vendor's security guidance, including but not limited to the following: • IP and link layer (where implemented by the POI) • IP protocols (where implemented by the POI) • Security protocols, including specific mention if specific security protocols or specific configurations of security protocols are not to be used for financial applications and/or platform management • IP services, including specific mention if specific IP services or specific configurations of IP services are not to be used for financial applications and/or platform management (where implemented by the POI) • For each platform component listed above, follow the POI device vendor's security guidance, as applicable to the application's specific business processing, with respect to the following: o Configuration and updates o Key management o Data integrity and confidentiality o Server authentication						

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-2.1.1.a Examine the POI device vendor's security guidance to determine the following: • The IP stack approved via the PCI-approved POI device evaluation • Any specific guidance from the POI device vendor's security guidance that needs to be implemented for the application Review the application's *Implementation Guide* required at 2C-3 of this document and confirm that it includes the following in accordance with the POI device vendor's security guidance: • A description of the IP stack implemented in the POI device and included in the POI device vendor's security guidance • Any instructions on how to securely configure any configurable options, as applicable to the application's specific business processing, including: ○ Vulnerability assessment ○ Configuration and updates ○ Key management ○ Data integrity and confidentiality ○ Server authentication • Any guidance that the device vendor intended for integrators/resellers, solution providers, and/or end-users • Guidance that only IP stacks approved as part of the PTS review can be used	• Identify the POI vendor's device security guidance document that defines the following: ○ The IP stack approved via the PCI-approved POI device evaluation ○ Any specific guidance from the POI device vendor's security guidance that needs to be implemented for the application • Confirm that the application's Implementation Guide includes the following in accordance with the POI device vendor's security guidance: ○ A description of the IP stack implemented in the POI device and included in the POI device vendor's security guidance ○ Any instructions on how to securely configure any configurable options, as applicable to the application's specific business processing, including: ▪ Vulnerability assessment ▪ Configuration and updates ▪ Key management ▪ Data integrity and confidentiality ▪ Server authentication ○ Any guidance that the device vendor intended for integrators/resellers, solution providers, and/or end-users ○ Guidance that only IP stacks approved as part of the PTS review can be used		✓				✓

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-2.1.1.b Perform a source-code review and verify that the application: • Only uses the IP stack approved as part of the PCI-approved POI device evaluation • Was developed according to the device vendor's security guidance • Is securely integrated with the POI device's IP stack and any OP services in accordance with the POI device vendor's security guidance, including the following areas for each platform component used by the POI as it relates to the application's specific processing: ○ Vulnerability assessment ○ Configuration and updates ○ Key management ○ Data integrity and confidentiality ○ Server authentication	• Identify methods/tools used to review source code. • Describe how findings from the source-code review verified that the application: ○ Only uses the IP stack approved as part of the PCI-approved POI device evaluation ○ Was developed according to the device vendor's security guidance ○ Is securely integrated with the POI device's IP stack and any OP services in accordance with the POI device vendor's security guidance, including the following areas for each platform component used by the POI as it relates to the application's specific processing: ▪ Vulnerability assessment ▪ Configuration and updates ▪ Key management ▪ Data integrity and confidentiality ▪ Server authentication	✓			✓		
2B-2.1.1.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Use forensic tools and/or methods (commercial tools, scripts, etc.) to examine all output created by the application and verify that, by following the *Implementation Guide*, the application only uses the IP stack included in the PCI-approved POI device evaluation.	• Confirm that the application was installed and configured only using the application vendor's documentation and the application's Implementation Guide (with no additional configuration required). • Identify the forensic tools and/or methods that were used to examine all output created by the application • Identify the application output examined. • Describe how examination of the output using forensic tests tools and/or methods verified that the application only uses the IP stack included in the PCI-approved POI device evaluation.	✓			✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-2.2 The application-development process includes secure integration with any resources shared with or between applications							
2B-2.2.a Review the POI device vendor's security guidance and the application's *Implementation Guide* required at 2C-3 of this document. Confirm that the application's *Implementation Guide* is in accordance any applicable information in the POI device vendor's security guidance, and includes the following: • A list of shared resources • A description of how the application connects to and/or uses shared resources • Instructions for how the application should be configured to ensure secure integration with shared resources	• Identify the POI device vendor's security guidance documentation that defines the following: ○ A list of shared resources ○ A description of how the application connects to and/or uses shared resources ○ Instructions for how the application should be configured to ensure secure integration with shared resources • Confirm that the application's Implementation Guide includes the following in accordance with the POI device vendor's security guidance: ○ A list of shared resources ○ A description of how the application connects to and/or uses shared resources ○ Instructions for how the application should be configured to ensure secure integration with shared resources		✓				✓
2B-2.2.b Perform a source-code review and verify that any connection to or use of shared resources is done securely and in accordance with the device vendor's security guidance.	• Identify methods/tools used to review source code. • Describe how findings from the source-code review were used to verify that any connection to or use of shared resources is done securely and in accordance with the device vendor's security guidance.	✓	✓		✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	Reporting Methodology					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-2.2.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Use forensic tools and/or methods (commercial tools, scripts, etc.) to examine all output created by the application and verify that, by following the *Implementation Guide*, any connections to or use of shared resources are done securely and in accordance with the device vendor's security guidance.	• Confirm that the application was installed and configured only using the application vendor's documentation and the application's Implementation Guide (with no additional configuration required). • Identify the forensic tools and/or methods used to examine all output created by the application. • Identify the application output examined. • Describe how examination of the output using forensic tests tools and/or methods verified that any connections to or use of shared resources are done securely.	✓			✓		
2B-2.3 Applications do not bypass or render ineffective any application segregation that is enforced by the POI.							
2B-2.3 Perform a source-code review and verify that applications do not bypass or render ineffective any application segregation which is enforced by the POI, in accordance with the device vendor's security guidance.	• Identify the document that defines the device vendor's security guidance. • Identify methods/tools used to review source code. • Describe how the findings from a source-code review were used to verify that applications do not bypass or render ineffective any application segregation which is enforced by the POI, in accordance with the device vendor's security guidance.	✓	✓		✓		
2B-2.4 Applications do not bypass or render ineffective any OS hardening implemented by the POI.							
2B-2.4 Perform a source-code review and verify that applications do not bypass or render ineffective any OS hardening which is implemented by the POI, in accordance with the device vendor's security guidance.	• Identify the document that defines the device vendor's security guidance. • Identify methods/tools used to review source code. • Describe how the findings from a source-code review were used to verify that applications do not bypass or render ineffective any OS hardening which is implemented by the POI, in accordance with the device vendor's security guidance.	✓	✓		✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-2.5 Applications do not bypass or render ineffective any encryption or account-data security methods implemented by the POI.							
2B-2.5 Perform a source-code review and verify that applications do not bypass or render ineffective any encryption or account-data security methods implemented by the POI, in accordance with the device vendor's security guidance.	• Identify the document that defines the device vendor's security guidance. • Identify methods/tools used to review source code. • Describe how the findings from a source-code review were used to verify that applications do not bypass or render ineffective any encryption or account-data security methods implemented by the POI, in accordance with the device vendor's security guidance.	✓	✓		✓		
2B-3 The application vendor uses secure protocols, provides guidance on their use, and has performed integration testing on the final application.							
2B-3.1 The application developer's process includes full documentation, and integration testing of the application and intended platforms, including the following:							

2B-3.1 Through observation and review of the application developer's system development documentation, confirm the application developer's process includes full documentation and integration testing of the application and intended platforms, including the following:	• Identify the document that defines the application developer's system development processes
	• Confirm the documented processes require full documentation and integration testing of the application and intended platforms, and includes:
	  ○ Provision of key-management security guidance describing how keys and certificates have to be used
	  ○ Final integration testing on the device, which includes identification and correction of any residual vulnerabilities stemming from the integration with the vendor's platform
			✓				

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	Reporting Methodology					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-3.1.1 The application developer provides key-management security guidance describing how keys and certificates have to be used. *Examples of guidance include what SSL certificates to load, how to load account-data keys (through the firmware of the device), when to roll keys, etc., The application does not perform account-data encryption since that is performed only in the firmware of the PCI-approved POI device.)*							
2B-3.1.1 Review the application's *Implementation Guide* required at 2C-3 of this document, and confirm it includes key-management security guidance for solution providers, describing how keys and certificates have to be used.	• Confirm the Implementation Guide includes key-management security guidance for solution providers, describing how keys and certificates have to be used.						✓
2B-3.1.2 The application developer has performed final integration testing on the device, which includes identification and correction of any residual vulnerabilities stemming from the integration with the vendor's platform.							
2B-3.1.2 Interview application developers to confirm that final integration testing, which includes identification and correction of any residual vulnerabilities stemming from the integration with the vendor's platform, was performed.	• Identify the application developers interviewed who confirm that: ○ Final integration testing was performed on the device ○ Final integration testing includes identification and correction of any residual vulnerabilities stemming from the integration with the vendor's platform,			✓			
2B-4 Applications do not implement any encryption or key-management functions in lieu of SRED encryption. All such functions are performed by the approved SRED firmware of the device. ***Note:*** *The application may add, for example, SSL encryption to existing SRED encryption, but cannot bypass or replace SRED encryption.*							
2B-4.1 Applications do not bypass or render ineffective any encryption or key-management functions implemented by the approved SRED functions of the device. At no time should clear-text keys or account data be passed through an application that has not undergone SRED evaluation.							

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2B-4.1.a Examine the application's *Implementation Guide* required at 2C-3 of this document and verify the description of the application's function includes the following: • Confirmation that the application does not perform account-data encryption, nor does it replace the device's SRED encryption • A description of the purpose and encryption method for any encryption provided by the application in addition to SRED encryption • Instructions on how to install the application correctly	• Confirm the application's Implementation Guide includes a description of the application's function that includes the following: ○ Confirmation that the application does not perform account-data encryption, nor does it replace the device's SRED encryption ○ A description of the purpose and encryption method for any encryption provided by the application in addition to SRED encryption ○ Instructions on how to install the application correctly.						✓
2B-4.1.b Perform a source-code review to verify that the application's encryption and key-management functions utilize an approved function of the SRED device, and are not implemented within the application itself.	• Identify methods/tools used to review source code. • Describe how findings from a source-code review were used to verify that the application's encryption and key management functions utilize an approved function of the SRED device, and are not implemented within the application itself.	✓			✓		
2B-4.1.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide* and confirm that, by following the *Implementation Guide,* the application does not perform account data encryption that replaces the SRED encryption performed by the device.	• Confirm that the application was installed and configured according to the application vendor's documentation, including the application's Implementation Guide (with no additional configuration required). • Describe how it was observed that the application does not perform account data encryption that replaces the SRED encryption performed by the device	✓			✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	Reporting Methodology					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2C-1 New vulnerabilities are discovered and applications are tested for those vulnerabilities on an ongoing basis.							
2C-1.1 Software developers must establish and implement a process to identify and test their applications for security vulnerabilities.							
2C-1.1.a Obtain and examine processes to identify new vulnerabilities and test applications for vulnerabilities that may affect the application. Verify the processes include the following: • Using outside sources for security vulnerability information • Periodic testing of applications for new vulnerabilities	• Identify the document that defines processes to identify new vulnerabilities and test applications for vulnerabilities that may affect the application. • Confirm that the documented processes include: ○ Using outside sources for security vulnerability information ○ Periodic testing of applications for new vulnerabilities		✓				
2C-1.1.b Interview responsible software vendor personnel to confirm the following: • New vulnerabilities are identified using outside sources of security vulnerability information. • All applications are tested for vulnerabilities.	• Identify the responsible personnel interviewed who confirm that: ○ New vulnerabilities are identified using outside sources of security vulnerability information. ○ All applications are tested for vulnerabilities.			✓			
2C-1.2 Software vendors must establish and implement a process to develop and deploy critical security updates to address discovered security vulnerabilities in a timely manner. ***Note:*** *A "critical security update" is one that addresses an imminent risk to account data.*							
2C-1.2.a Obtain and examine processes to develop and deploy application security upgrades. Verify that processes include the timely development and deployment of critical security updates to customers.	• Identify the document that defines the processes to develop and deploy application security upgrades. • Confirm that the documented processes include: ○ Timely development of critical security updates. ○ Timely deployment of critical security updates to customers		✓				

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	Reporting Methodology					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2C-1.2.b Interview responsible software-vendor personnel to confirm that application security updates are developed and critical security updates are deployed in a timely manner:	• Identify the responsible personnel interviewed who confirm that: ○ Application security updates are developed in a timely manner. ○ Critical security updates are deployed in a timely manner.			✓			
2C-2 Applications are installed and updates are implemented only via trusted, signed, authenticated processes using an approved security protocol evaluated for the PCI-approved POI device.							
2C-2.1 Ensure that all application installations and updates are authenticated as follows:							
2C-2.1 To confirm that all application installations and updates are authenticated, verify the following:							
2C-2.1.1 All application installations and updates only use an approved security protocol of the POI.							
2C-2.1.1.a Examine the application's *Implementation Guide* required at 2C-3 of this document and verify that it includes the following: • A description of how the application uses the approved security protocol of the POI for any application installations and updates • Instructions for how to use the approved security protocol to perform application installations and updates • A statement that application installations and updates cannot occur except by using the approved security protocol of the POI	• Confirm that the application's Implementation Guide includes ○ A description of how the application uses the approved security protocol of the POI for any application installations and updates ○ Instructions for how to use the approved security protocol to perform application installations and updates ○ A statement that application installations and updates cannot occur except by using the approved security protocol of the POI						✓
2C-2.1.1.b Perform a source-code review to verify that the application only allows installations and updates using the approved security protocol of the POI.	• Identify methods/tools used to review source code • Describe how the findings of a source-code review were used to verify that the application only allows installations and updates using the approved security protocol of the POI.	✓			✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2C-2.1.1.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that, by following the *Implementation Guide,* the application only allows installations and updates using the approved security protocol of the POI.	• Confirm that the application was installed and configured only using the application vendor's documentation, including the application's Implementation Guide (with no additional configuration required). • Identify the forensic tools and/or methods used • Describe how use of forensic tools and/or methods verified that the application only allows installations and updates using the approved security protocol of the POI.	✓			✓		
2C-2.1.1.d After the application is installed and configured in accordance with the *Implementation Guide,* attempt to perform an installation and an update using non-approved security protocol, and verify that the application will not allow the installation or update to occur.	• Confirm that the application was installed and configured only using the application vendor's documentation, including the application's Implementation Guide (with no additional configuration required). • Describe how an installation and an update using non-approved security protocol were attempted • Describe how the application was observed to not allow the installation or update to occur.	✓			✓		
2C-2.1.2 Unauthenticated changes are not allowed (for example, all changes to code that manages "whitelists" must be authenticated).							
2C-2.1.2.a Examine the application's *Implementation Guide* required at 2C-3 of this document and verify that it includes the following: • A description of how the application prevents unauthenticated changes or updates • A statement that unauthenticated changes or updates to applications or applications functions (like "whitelists") are not allowed	• Confirm the application's Implementation Guide includes the following: ○ A description of how the application prevents unauthenticated changes or updates ○ A statement that unauthenticated changes or updates to applications or applications functions are not allowed						✓

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2C-2.1.2.b Perform a source-code review to verify that the application does not allow unauthenticated changes or updates.	• Identify methods/tools used to review source code • Describe how the findings of the source-code review were used to verify that the application does not allow unauthenticated changes or updates.	✓			✓		
2C-2.1.2.c Install and configure the application according to the application vendor's documentation, including the application's *Implementation Guide*. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that, by following the *Implementation Guide,* the application does not allow unauthenticated changes or updates.	• Confirm that the application was installed and configured only using the application vendor's documentation, including the application's Implementation Guide (with no additional configuration required). • Identify the forensic tools and/or methods used. • Describe how use of forensic tools and/or methods verified that the application does not allow unauthenticated changes or updates.	✓			✓		
2C-2.1.2.d After the application is installed and configured in accordance with the *Implementation Guide,* attempt to add an unauthenticated "whitelist" and verify that the application will not allow the update to occur.	• Confirm that the application was installed and configured only using the application vendor's documentation, including the application's Implementation Guide (with no additional configuration required). • Describe how addition of an unauthenticated "whitelist" was attempted • Describe how the application was observed to not allow the update to occur.	✓			✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	Reporting Methodology					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2C-2.1.3 The application developer includes guidance for whoever signs the application (including for whitelists), including requirements for dual control over the application-signing process.							
2C-2.1.3 Examine the application's *Implementation Guide* required at 2C-3 of this document and verify that it includes the following: • Instructions for how to sign the application (including "whitelists") • Instructions how to implement the dual control for the application-signing process • A statement that all applications must be signed via the instructions provided in the *Implementation Guide.*	• Confirm that the application's Implementation Guide includes the following: ○ Instructions for how to sign the application (including "whitelists") ○ Instructions how to implement the dual control for the application-signing process ○ A statement that all applications must be signed via the instructions provided in the Implementation Guide.						✓
2C-3 Maintain instructional documentation and training programs for the application's installation, maintenance/upgrades, and use.							
2C-3.1 The process to develop, maintain, and disseminate an *Implementation Guide* for the application's installation, maintenance, upgrades and general use includes the following:							
2C-3.1 Examine the *Implementation Guide* and related processes, and verify the guide is disseminated to all relevant application installers and users (including customers, resellers, and integrators).	• Identify the document that defines related processes for dissemination of the Implementation Guide. • Describe how examination of the Implementation Guide and related processes verified that the Implementation Guide is disseminated to all relevant application installers and users (including customers, resellers, and integrators)		✓				✓
2C-3.1.1 Addresses all requirements in P2PE Domain 2 wherever the *Implementation Guide* is referenced.							
2C-3.1.1 Verify the *Implementation Guide* covers all related requirements in P2PE Domain 2.	• Confirm that the Implementation Guide covers all related requirements in P2PE Domain 2.						✓

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2C-3.1.2 Review of the *Implementation Guide* at least annually and upon changes to the application or the P2PE Domain 2 requirements, and update as needed to keep the documentation current with: • Any changes to the application (for example, device changes/upgrades and major and minor software changes). • Any changes to the *Implementation Guide* requirements in this document.							
2C-3.1.2.a Verify the *Implementation Guide* is reviewed at least annually and upon changes to the application or the P2PE Domain 2 requirements.	• Identify the document that defines procedures for the Implementation Guide to be reviewed: ○ At least annually, and ○ Upon changes to the application or to the P2PE Domain 2 Requirements. • Describe how processes were observed to be implemented to review the Implementation Guide ○ At least annually, and ○ Upon changes to the application or the P2PE Domain 2 requirements.		✓		✓		
2C-3.1.2.b Verify the *Implementation Guide* is updated as needed to keep the documentation current with: • Any changes to the application (for example, device changes/upgrades and major and minor software changes). • Any changes to the Implementation Guide requirements in this document.	• Identify the document that defines procedures for the Implementation Guide to be updated as needed to keep the documentation current with: ○ Any changes to the application. ○ Any changes to the Implementation Guide requirements in this document. • Describe how processes were observed to be implemented to update the Implementation Guide as needed to keep the documentation current with: ○ Any changes to the application. ○ Any changes to the Implementation Guide requirements in this document.		✓		✓		

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2C-3.1.3 Distribution to all new and existing application installers (for example, solution providers, integrator/resellers, etc.), and re-distribution to all existing application installers every time the guide is updated.							

2C-3.1.3 Verify the *Implementation Guide* is distributed to new application installers, and re-distributed to all application installers every time the guide is updated.	• Identify the document that defines procedures for the Implementation Guide to be:
	  ○ Distributed to new application installers, and
	  ○ Re-distributed to all application installers every time the guide is updated.
	• Describe how processes were observed to be implemented to ensure that the Implementation Guide is:
	  ○ Distributed to new application installers, and
	  ○ Re-distributed to all application installers every time the guide is updated.
			✓		✓		

2C-3.2 Develop and implement training and communication programs to ensure application installers (for example, solution providers or integrators/resellers) know how to implement the application according to the *Implementation Guide*.							
2C-3.2 Examine the training materials and communication program, and confirm the materials cover all items noted for the *Implementation Guide* throughout P2PE Domain 2.	• Identify the document that contains the training materials and communication programs. • Confirm the materials cover all items noted for the Implementation Guide throughout P2PE Domain2.		✓				

P2PE Domain 2 Application Vendor Assessment Requirements and Testing Procedures	Reporting Details	*Reporting Methodology*					
		Observe systems, configurations	Review documentation	Interview personnel	Observe processes, action, state	Identify sample	Verify Implementation Guide content
2C-3.2.1 Review the training materials for application installers on an annual basis and whenever new application versions are released. Updated as needed to ensure materials are current with the *Implementation Guide*.							
2C-3.2.1 Examine the training materials for resellers and integrators and verify the materials are reviewed on an annual basis and when new application versions are released, and updated as needed.	• Identify the document that contains the training materials for application installers (including resellers and integrators). • Confirm the documented materials are reviewed on an annual basis and when new application versions are released, and updated as needed. • Describe how processes were observed to be implemented to ensure that the materials are reviewed on an annual basis and when new application versions are released, and updated as needed.		✓		✓		