Payment Card Industry (PCI)

Point-to-Point Encryption (P2PE)

Template for P2PE Application Report on Validation (Application P-ROV)

Application P-ROV Template

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 the template for submitting Application P-ROVs 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

Introduction to P2PE Application P-ROV Template

This document provides the template for completing an Application P-ROV to report compliance of a POI application intended for use with PCI P2PE solutions. This template is accompanied by Application P-ROV Reporting Instructions - *Application P-ROV Reporting Instructions For Application used with PCI P2PE Hardware/Hardware Standard v1.1 and/or PCI P2PE Hardware/Hybrid Standard v1.1.* P2PE assessors should refer to the Reporting Instructions before beginning an Application P-ROV.

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

Tables have been included in this template to facilitate the reporting process for certain lists and other information as appropriate. The *Application P-ROV Reporting Instructions* provide further instruction on how to complete the Application P-ROV, including the use of tables.

Note: *The tables in this template may be modified to increase/decrease the number of rows, or to change column width. Additional columns may be added if the assessor feels there is relevant information to be included that is not addressed in the current format. However, the assessor must not remove any details from the tables provided in this document.*

Application P-ROV Template for PCI P2PE Hardware/Hardware and Hardware/Hybrid Standard v1.1

This template is to be used for creating an Application P-ROV for submission to PCI SSC. Content and format for an Application P-ROV is defined as follows:

1. Contact Information and Report Date

1.1 Contact Information	
Application Vendor contact information	
Company name:	
Company address:	
Company URL:	
Company contact name:	
Contact phone number:	
Contact e-mail address:	

P2PE Assessor Company contact information	
Company name:	
Company address:	
Company PCI credentials:	

P2PE Assessor contact information	
Assessor name:	
Assessor PCI credentials:	
Assessor phone number:	
Assessor e-mail address:	

1.1 Contact Information (continued)	
P2PE Assessor Quality Assurance (QA) primary contact information	
QA primary contact name:	
QA primary contact phone number:	
QA primary contact e-mail address:	

1.2 Date and Timeframe of Assessment	
Date of Report:	
Timeframe of assessment:	

1.3 P2PE Version	
Version of the P2PE Standard used for the assessment:	

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, as a standalone application, in modules, or as part of a suite of applications):	
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: ▪ Identify the specific P2PE solution the application is intended for use with *(Include solution provider company name and solution name):*		
▪ Identify whether the application in this P-ROV is to be listed on the PCI SSC List of Validated P2PE Applications:*	☐ Yes	☐ No
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:		

** Refer to the P2PE Program Guide for details on application listing processes*

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 #**

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 within the POI)
  - All flows and locations of cleartext account data (including data input, output, and within the POI)
- 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.*

2.5 Versioning Methodology	
Describe vendor's versioning methodology as follows:	
▪ Description of how the vendor indicates application changes via their version numbers:	
▪ Define what types of changes the vendor includes as a "No Impact" change:	

Note: *Refer to* the P2PE Program Guide *for information on what constitutes a No Impact change*

2.6 Multi-Acquirer / Multi-Solution Applications		
Identity whether the application is capable of supporting multiple P2PE solutions, or multiple acquirers or payment processors, at the same time:	☐ Yes	☐ No
If Yes, provide a brief description of how management of the application is to be shared between multiple P2PE solution providers / acquirers / payment processors:		

2.7 Implementation Guide Details	
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:	
▪ POI device type:	
▪ 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 included within the Implementation Guide (for example, user guides, installation instructions etc.):	

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 all application functions, provide the following:
  - Description of all application processes related to each function
  - Description of all communication channels, connection methods and communication protocols used by the application, for all internal and external communication channels
  - Details of any protection mechanisms (for example, encryption, truncation, masking, etc.) applied to account data by the application
  - Other necessary application functions or processes, as applicable
- Identify any functionality of the application that was not included in the assessment

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 (for example, software, hardware)**	**Role of component**

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:	

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:	

Application vendor facilities INCLUDED in assessment	
Description and purpose of application vendor facility included in application assessment	**Address of facility**

Application vendor facilities EXCLUDED from assessment		
Description and purpose of application vendor facility excluded from application assessment	**Address of facility**	**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**

3.5 Documentation and Personnel Interviews *(continued)*			
Provide list of all personnel interviewed for this application assessment:			
Name	**Company**	**Job Title**	**Topics covered**

4. Findings and Observations

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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.	<Report Findings Here>
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 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.	<Report Findings Here>
2A-2.1.b Perform a source-code review and verify that the application never outputs clear-text account data outside of the device.	<Report Findings Here>
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.	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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.*	
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.	<Report Findings Here>
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.	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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.	<Report Findings Here>
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	<Report Findings Here>
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).	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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.	<Report Findings Here>
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	<Report Findings Here>
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.	<Report Findings Here>
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).	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	
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.	<Report Findings Here>
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.	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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.	<Report Findings Here>
2B-1.2.4 Confirming that appropriate corrections are implemented prior to release.	
2B-1.2.4 Appropriate corrections are implemented prior to release.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>
2B-1.3.b Interview a sample of developers to confirm that they are knowledgeable in secure coding techniques.	<Report Findings Here>
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.)	<Report Findings Here>
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	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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.	<Report Findings Here>
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:	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>
2B-1.4.3.b Verify that all changes (including patches) are tested for per secure coding guidance before being released.	<Report Findings Here>
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.	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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.	<Report Findings Here>
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: ○ Configuration and updates ○ Key management ○ Data integrity and confidentiality ○ Server authentication	

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment

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
	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment

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
	<Report Findings Here>

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.	<Report Findings Here>
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	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>
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:	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	
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	<Report Findings Here>
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.	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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.	<Report Findings Here>
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	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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	<Report Findings Here>
2C-2.1.2.b Perform a source-code review to verify that the application does not allow unauthenticated changes or updates.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>
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.*	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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).	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>
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.	<Report Findings Here>

P2PE Domain 2 Requirements and Application Vendor Testing Procedures	PA-QSA (P2PE) Findings from Application Vendor Assessment
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.	<Report Findings Here>
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.	<Report Findings Here>