Payment Card Industry (PCI)

Point-to-Point Encryption

Template for Report on Validation
for use with P2PE v2.0 (Revision 1.2)
for P2PE Application

Revision 1.2

March 2020

Document Changes

Date	Use with Version	Template Revision	Description
March 2020	For use with P2PE v2.0, Revision 1.2	Revision 1.2	Aligns the revision to the v2.0 r1.2 Standard and P-ROVs that included the following updates: Clarify intent of 6C-3.1 and 6D-1.5 (in both Domain 6 and Annex B) with regards to the use of triple-length TDEA keys and align with key table of Annex C. Clarify domain applicability for CA/RAs.
November 2015	For use with P2PE v2.0, Revision1.1	Revision1.0	To introduce the template for submitting P2PE Reports on Validation for P2PE Applications assessed against the P2PE v2 Standard. *This document serves as both the Reporting Template and Reporting Instructions document; there are not separate documents for this under P2PE v2 as there are still under P2PE v1*

Table of Contents

Introduction to the P-ROV Template for P2PE Applications

This document, the *PCI Point-to-Point Encryption: Template for Report on Validation for use with P2PE v2.0 (Rev 12) for P2PE Application, Revision 1.2* ("Application P-ROV Reporting Template"), is the mandatory template for completing a P2PE Report on Validation (P-ROV) for P2PE Application assessments against the *P2PE: Solution Requirements and Testing Procedures, v2.0 (Rev 1.2)* ("P2PE v2 Standard"). This Reporting Template provides reporting instructions and the template form for PA-QSA (P2PE) assessors to provide a more consistent level of reporting among assessors.

Use of this Reporting Template is mandatory for all P2PE v2 submissions for P2PE Applications.

Tables have been included in this template to facilitate the reporting process for certain lists and other information as appropriate. The tables in this template may be modified to increase/decrease the number of rows, or to change column width. Additional appendices 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. Personalization, such as the addition of company logos, is acceptable but limited to the title page.

Do not delete any content from any place in this document, including this section and the versioning above. These instructions are important for the assessor as they complete reporting, but also provide context for for the report recipient(s). Addition of text or sections is applicable within reason, as noted above.

A P2PE compliance assessment involves thorough testing and assessment activities, from which the assessor will generate detailed work papers. These work papers contain comprehensive records of the assessment activities, including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the course of the assessment. The P-ROV is effectively a ***summary of evidence*** derived from the assessor's work papers to describe how the assessor performed the validation activities and how the resultant findings were reached. At a high level, the P-ROV provides a comprehensive ***summary of testing activities performed and information collected*** during the assessment against the P2PE v2 Standard. The information contained in a P-ROV must provide enough detail and coverage to verify that the P2PE submission is compliant with all applicable P2PE requirements.

P-ROV Sections

The P-ROV includes the following sections that must be completed in their entirety:

- Section 1: Contact Information and Report Date
- Section 2: Summary Overview
- Section 3: Details and Scope of P2PE Assessment
- Section 4: Findings and Observations

This Reporting Template includes tables with Reporting Instructions built-in. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage.

P-ROV Summary of Findings

This version of the P2PE Reporting Template reflects an on-going effort to simplify assessor summary reporting. All summary findings for "In Place," "Not in Place," and "Not Applicable" are found at the beginning of each Domain and are only addressed at that high-level. A summary of all domain findings is also at "2.9 Summary of P2PE Compliance Status."

The following table is a representation when considering which selection to make. Remember, assessors must select only one response at the sub-requirement level, and the selected response must be consistent with reporting within the remainder of the P-ROV and other required documents, such as the relevant P2PE Attestation of Validation (P-AOV).

RESPONSE	WHEN TO USE THIS RESPONSE:
In Place	The expected testing has been performed, and all elements of the requirement have been met as stated. This may be a mix of In Place and Not Applicable responses, but no Not in Place response. Requirements fulfilled by other P2PE Components or Third Parties should be In Place, unless the requirement does not apply.
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.
N/A (Not Applicable)	The requirement does not apply to the P2PE Product. All Not Applicable responses require reporting on testing performed and must explain how it was determined that the requirement does not apply.

Note: *Checkboxes have been added to the "Summary of Assessment Findings" so that the assessor may double click to check the applicable summary result. Hover over the box you'd like to mark and click once to mark with an 'x.' To remove a mark, hover over the box and click again. Mac users may instead need to use the space bar to add the mark*

P-ROV Reporting Details

The reporting instructions in the Reporting Template are clear as to the intention of the response required. There is no need to repeat the testing procedure, the reporting instruction, or such within each assessor response. As noted earlier, responses should be specific, but simple. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage.

Assessor responses will generally fall into categories such as the following:

- **"Identify the P2PE Assessor who confirms…"**

  Indicates only an affirmative response where further reporting is deemed unnecessary by PCI SSC. The P2PE Assessor's name or a Not Applicable response are the two appropriate responses here. A Not Applicable response will require brief reporting to explain how this was confirmed via testing.

- **Document name or interviewee reference**

  At 3.7 Documentation Reviewed and 3.8 Individuals Interviewed, there is a space for a reference number and ***it is the P2PE Assessor's choice*** to use the document name/interviewee job title or the reference number in responses. A listing is sufficient here, no further detail required.

- **Sample reviewed**

  Brief list is expected or sample identifier. Again, where applicable, it is the P2PE Assessor's choice to list out each sample within reporting or to utilize sample identifiers from the sampling summary table.

- **Brief description/short answer – "Describe how…"**

  These are the only reporting instructions that will stretch across half of the table; the above are all a quarter-table's width to serve as a visual indicator of detail expected in response. These responses must be a narrative response that provides explanation as to the observation—both a summary of what was witnessed and how that verified the criteria of the testing procedure.

Do's and Don'ts: Reporting Expectations

DO:	*DON'T:*
▪ Use the corresponding Reporting Template for v2.0 of the P2PE Standard. ▪ Complete all sections in the order specified, with concise detail. ▪ Read and understand the intent of each Requirement and Testing Procedure. ▪ Provide a response for every Testing Procedure, even if N/A. ▪ Provide sufficient detail and information to demonstrate a finding of "in place" or "not applicable." ▪ Describe how a Requirement was verified as the Reporting Instruction directs, not just that it was verified. ▪ Ensure all parts of the Testing Procedure are addressed. ▪ Ensure the response covers all applicable application and/or system components. ▪ Perform an internal quality assurance review of the P-ROV for clarity, accuracy, and quality. ▪ Provide useful, meaningful diagrams, as directed.	▪ Don't report items in the "In Place" column unless they have been verified as being "in place." ▪ Don't include forward-looking statements or project plans in responses. ▪ Don't simply repeat or echo the Testing Procedure in the response. ▪ Don't copy responses from one Testing Procedure to another. ▪ Don't copy responses from previous assessments. ▪ Don't include information irrelevant to the assessment.

P-ROV Application Template for P2PE v2 Standard (Rev 1.2)

This template is to be used for creating a P2PE Report on Validation for submission to PCI SSC for P2PE Applications assessed against P2PE v2. Content and format for this P-ROV is defined as follows:

1. Contact Information and Report Date

1.1 Contact Information

P2PE Application Vendor contact information			
Company name:		Company URL:	
Company contact name:		Contact e-mail address:	
Contact phone number:		Company address:	

P2PE Assessor Company contact information				
Company name:		Assessor Company Credentials:	☐ QSA (P2PE)	☐ PA-QSA (P2PE)
Assessor name:		Assessor Credentials:	☐ QSA (P2PE)	☐ PA-QSA (P2PE)
Assessor phone number:		Assessor e-mail address:		
Confirm that internal QA was fully performed on the entire P2PE submission, per requirements in relevant program documentation.		☐ Yes ☐ No (if no, this is not in accordance with PCI Program requirements)		

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 (should be 2.0):	

2. Summary Overview

2.1 P2PE Application Details				
P2PE application name:		Application version:		
Is the application already listed on the PCI SSC List of Validated P2PE Applications?		☐ Yes ☐ No	If yes, provide PCI SSC Ref #	or ☐ N/A
Has the application been developed in-house by the solution provider for use only in their own solution?		☐ Yes ☐ No *If 'yes,' complete the two questions to the right of this cell.*	Is this application to be listed on the PCI SSC List of Validated P2PE Applications?	☐ Yes ☐ No
			Identify the specific P2PE solution the application is intended for use with (*Include solution provider company name and solution name*):	
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 Versioning Methodology	
Description of how the vendor indicates application changes via their version numbers/versioning methodology:	
Define what types of changes the vendor includes as a "No Impact" change (*refer to the P2PE Program Guide for information on what constitutes a No Impact Change*):	

2.3 Other Third-Party Service Provider entities involved in P2PE Application

This could include third-party service providers in use as applicable, including authorized Integrator/Resellers and such.

"Other details" is to be used as needed. For example, if there is a third-party service provider providing decryption services but it not a P2PE Component at 2.2, use "Other details" to address data such as P2PE endpoint system identifier (e.g., Host System and HSM). Mark as "n/a" if no other details are needed.

Entity Name:	Role/Function:	Entity Location(s):	Other Details, if needed:

2.4 Multi-Acquirer and Multi-Solution Applications

Identify whether the application is capable of supporting multiple P2PE solutions, or multiple acquirers or payment processors, at the same time:	☐ Yes	☐ No
If 'yes,' describe how management of the multi-acquirer or multi-provider application is divided between entities (multiple P2PE solution providers, acquirers, payment processors, etc.):		

2.5 PTS Devices Supported

List of all POI device types supported and tested as part of Application's P2PE Assessment.

PTS Approval #:	Make/ Manufacturer:	Model Name/ Number:	Hardware #:	Firmware #(s):*

Note: *P2PE applications and P2PE non-payment software do not meet the PTS definition of "firmware" and are not reviewed as part of the PTS POI assessment. Additionally, software meeting the PTS definition of "firmware" is not reassessed during a P2PE assessment (PTS firmware is not considered a P2PE payment application, nor is it P2PE non-payment software).*

2.6 Summary of P2PE Compliance Status

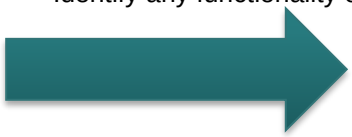
P2PE Domain	Compliant	Comments (optional):
Domain 1 – Encryption Device and Application Management	N/A	
Domain 2 – Application Security	☐ Yes ☐ No	
Domain 3 – P2PE Solution Management	N/A	
Domain 4 – Merchant-managed Solutions	N/A	
Domain 5 – Decryption Environment	N/A	
Domain 6 – P2PE Cryptographic Key Operations and Device Management	N/A	
Domain 6 – Annex A1: Symmetric-Key Distribution using Asymmetric Techniques	N/A	
Domain 6 – Annex A2: Certification and Registration Authority Operations	N/A	
Domain 6 – Annex B: Key-Injection Facilities	N/A	

3. Details and Scope of P2PE 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



<Insert P2PE Application detailed diagram(s)>

3.2 Overview of P2PE Application data flow

For each POI the application was tested on:

- Provide ***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.*

<Insert P2PE Application data flow diagram(s)>

3.3 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

3.4 Application authentication mechanisms

Describe the application's end-to-end authentication methods, as follows:

• Authentication mechanisms:	
• Authentication database:	
• Security of authentication data storage:	

3.5 Facilities

Lab environment used by the P2PE Assessor for this assessment

Identify whether the lab was provided by the P2PE Assessor or the Application Vendor:	☐ P2PE Assessor's Lab ☐ Application Vendor's Lab
Address of the lab environment used for this assessment:	

Describe the lab environment used for this assessment:

List of all application vendor facilities INCLUDED in this Application assessment	
Description and purpose of facility included in assessment	Address of facility

List of application vendor facilities EXCLUDED from this Application assessment		
Description and purpose of facility excluded from assessment	Address of facility	Explanation why the facility was excluded from the assessment

3.6 Documentation Reviewed

Identify and list all reviewed documents below. Add additional rows as needed.

Note: *If the P2PE Application Implementation Guide consists of more than one document, the brief description below should explain the purpose of each document it includes, such as if it is for a different POIs, for different functions, etc.*

P2PE Application Implementation Guide(s) (IG):

Reference # (optional use)	Document Name (Title of the IG)	Version Number of the IG	Document date (latest version date)	Which POI device type(s) is addressed? (Must align with Section 2.5)

All other documentation reviewed for this P2PE Assessment:

Reference # (optional use)	Document Name (including version, if applicable)	Document date (latest version date)	Document Purpose

3.7 Individuals Interviewed

List of all personnel interviewed for this Application assessment:

Reference # (optional use)	Interviewee's Name	Company	Job Title

4. Findings and Observations

Domain 2: Application Security – Summary of Findings

Domain 2: P2PE Validation Requirements		Summary of Findings (check one)		
		In Place	N/A	Not in Place
2A	**Protect PAN and SAD**			
2A-1	*The application executes on a PCI-approved POI device with SRED enabled and active.*	☐	☐	☐
2A-2	*The application does not store PAN and/or SAD for any longer than business processes require.*	☐	☐	☐
2A-3	*The application does not transmit clear-text PAN and/or SAD outside of the POI device, and only uses communication methods included in the scope of the PCI-approved POI device evaluation.*	☐	☐	☐
2B	**Develop and maintain secure applications.**			
2B-1	*The application is developed and tested according to industry-standard software development life cycle practices that incorporate information security.*	☐	☐	☐
2B-2	*The application is implemented securely, including the secure use of any resources shared between different applications.*	☐	☐	☐
2B-3	*The application vendor uses secure protocols, provides guidance on their use, and performs integration testing on the final application.*	☐	☐	☐
2B-4	*Applications do not implement any encryption functions in lieu of SRED encryption. All such functions are performed by the approved SRED firmware of the POI device.*	☐	☐	☐
2C	**Implement secure application-management processes.**			
2C-1	*New vulnerabilities are discovered and applications are tested for those vulnerabilities on an ongoing basis.*	☐	☐	☐
2C-2	*Applications are installed and updates are implemented only via trusted and cryptographically authenticated processes using an approved security mechanism evaluated for the PCI-approved POI device.*	☐	☐	☐
2C-3	*Maintain instructional documentation and training programs for the application's installation, maintenance/upgrades, and use.*	☐	☐	☐

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2A-1.1 The application must be intended for use on a device approved per the PCI PTS program (e.g., a PCI-approved PED or SCR), with SRED (secure reading and exchange of data). The PTS approval listing must match the following characteristics: • Model name and number • Hardware version number • Firmware version number • SRED listed as a function provided.		
2A-1.1 For each POI device type used by the application, examine the POI device configurations and review the PCI SSC list of Approved PTS Devices to verify that all of the following POI device characteristics match the PTS listing: • Model name/number • Hardware version number • Firmware version number • SRED listed as a function provided.	For each POI device type used by the application, describe how the POI device configurations observed verified that all of the POI device characteristics at 2A-1.1 match the PTS listing:	
	<Report Findings Here>	
2A-1.2 The application must only use the PTS SRED-validated account-data capture mechanisms of the underlying POI device for accepting and processing P2PE transactions.		
2A-1.2 For each type of POI device being assessed as part of the application assessment, verify that the application only uses SRED-validated account data capture mechanisms.	For each POI device type used in the application, describe how the application only uses SRED-validated account data capture mechanisms:	
	<Report Findings Here>	
2A-2.1 The application vendor must document all flows and justify all uses of PAN and/or SAD input into, processed by, and output from the application.		
2A-2.1.a Interview software personnel and examine the application's design documentation to verify it documents all flows and justifies all uses of PAN and/or SAD input into, processed by, and output from the application.	Software personnel interviewed:	*<Report Findings Here>*
	Application design documentation reviewed:	*<Report Findings Here>*
2A-2.1.b Perform a source-code review and verify that PAN and/or SAD are only utilized according to the documentation.	Describe how the source-code review verified that PAN and/or SAD are only utilized according to the documentation:	
	<Report Findings Here>	
2A-2.2 The application must not store PAN and/or SAD (even if encrypted) as follows: • Application must not store PAN data after the payment transaction is complete. • Application must not store SAD after authorization is complete. ***Note:*** *Storage of encrypted PAN data is acceptable during the business process of finalizing the payment transaction if needed (e.g., offline transactions). However, at all times, SAD is not stored after authorization is complete.*		

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2A-2.2.a Examine the application's design documentation and verify it includes a description of the following: • How it uses PAN and/or SAD for its application processing. • How it ensures the application does not store PAN after the payment transaction is complete. • How it ensures the application does not store SAD after authorization is complete.	Application design documentation reviewed:	*<Report Findings Here>*
2A-2.2.b Perform a source-code review to verify that the application is designed such that: • PAN is not stored after the payment transaction is completed. • SAD is not stored after authorization is completed.	Describe how the source-code review verified that the application is designed such that PAN is not stored after the payment transaction is completed:	
	<Report Findings Here>	
	Describe how the source-code review verified that the application is designed such that SAD is not stored after authorization is completed:	
	<Report Findings Here>	
2A-2.2.c Install and configure the application according to the application vendor's documentation, including the application's Implementation Guide. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that: • PAN is not stored after the payment transaction is completed. • SAD is not stored after authorization is completed.	Describe test transactions performed (must utilize all functions of the application that handle account data):	
	<Report Findings Here>	
	Describe forensic tools and/or methods used to inspect the test transactions:	
	<Report Findings Here>	
2A-2.3 The application must not retain PAN and/or SAD in working memory any longer than strictly necessary.		
2A-2.3.a Examine the application's design documentation and verify it contains a detailed description of the function of the application, including how it ensures the application does not retain PAN and/or SAD in working memory any longer than strictly necessary.	Application design documentation reviewed:	*<Report Findings Here>*
2A-2.3.b Perform a source-code review and verify that PAN and/or SAD is cleared from all working memory locations after use, including local variables (before exiting the function).	Describe how the source-code review verified that PAN and/or SAD is cleared from all working memory locations after use, including local variables (before exiting the function):	
	<Report Findings Here>	

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2A-2.3.c Install and configure the application according to the application vendor's documentation, including the application's Implementation Guide. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify the application clears all working memory locations utilized for the temporal retention of PAN and/or SAD during processing.	Describe test transactions performed (must utilize all functions of the application that handle account data):	
	<Report Findings Here>	
	Describe forensic tools and/or methods used to inspect the test transactions:	
	<Report Findings Here>	
2A-2.4 The application must securely delete any PAN and/or SAD stored during application processing.		
2A-2.4.a Examine the application's design documentation and verify it describes the process used by the application to securely delete any PAN and/or SAD stored during application processing.	Application design documentation reviewed:	*<Report Findings Here>*
2A-2.4.b Perform a source-code review and verify that the process provided by the application vendor renders all stored PAN and/or SAD irrecoverable once application processing is completed, in accordance with industry-accepted standards for secure deletion of data.	Describe how the source-code renders all stored PAN and/or SAD irrecoverable once application processing is completed, in accordance with industry-accepted standards for secure deletion of data:	
	<Report Findings Here>	
2A-2.4.c Install and configure the application according to the application vendor's documentation, including the application's Implementation Guide. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that the process provided by the application renders all PAN and/or SAD data irrecoverable, in accordance with industry-accepted standards for secure deletion of data, once the business process of the application is completed.	Describe test transactions performed (must utilize all functions of the application that handle account data):	
	<Report Findings Here>	
	Describe forensic tools and/or methods used to inspect the test transactions:	
	<Report Findings Here>	
2A-3.1 The application must not output clear-text account data outside of the POI 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-3.4*		
2A-3.1.a Examine the application's design documentation and verify it contains a description of the application's function, including that the application does not output clear-text account data outside of the POI device.	Application design documentation reviewed:	*<Report Findings Here>*
2A-3.1.b Perform a source-code review and verify the application never outputs clear-text account data outside of the POI device.	Describe how the source-code review verified that the application never outputs clear-text account data outside of the POI device:	
	<Report Findings Here>	

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2A-3.1.c Install and configure the application according to the application vendor's documentation, including the application's Implementation Guide. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify the application does not output clear-text account data outside of the POI device.	Describe test transactions performed (must utilize all functions of the application that handle account data):	
	<Report Findings Here>	
	Describe forensic tools and/or methods used to inspect the test transactions:	
	<Report Findings Here>	
2A-3.1.2 If the application facilitates merchant printing of full PANs on receipts due to a legal or regulatory obligation, this is ONLY allowable if the application includes the following: • The application only transmits clear-text PAN internally within the POI device to an integrated printer that is part of the PCI-approved POI device and is not attached via cabling or other networking mechanisms. • The P2PE application securely deletes the clear-text PAN after completion of printing. *Note that Domain 1 (at 1B.1.1) and Domain 3 (at 3A-1.3) also include requirements that must be met for any POI device and for a P2PE solution provider, respectively, that facilitates merchant printing of full PAN where there is a legal or regulatory obligation to do so.*		
2A-3.1.2.a If the application facilitates merchant printing of full PANs on receipts due to a legal or regulatory obligation, examine the application's design documentation and verify it contains a description of the application's function, including that the printing of full PANs on merchant receipts is a legal/regulatory obligation.	Application design documentation reviewed:	*<Report Findings Here>*
2A-3.1.2.b If the application facilitates merchant printing of full PANs on receipts due to a legal or regulatory obligation, perform a source-code review and verify the following: • The application only transmits clear-text PAN internally within the POI device to an integrated printer that is part of the PCI-approved POI device and does not include any functionality that sends clear-text PANs to any devices attached via cabling or other networking mechanisms. • The P2PE application securely deletes the clear-text PAN after completion of printing.	Describe how the source-code review verified that the application only transmits clear-text PAN internally within the POI device to an integrated printer that is part of the PCI-approved POI device and does not include any functionality that sends clear-text PANs to any devices attached via cabling or other networking mechanisms:	
	<Report Findings Here>	
	Describe how the source-code review verified that the P2PE application securely deletes the clear-text PAN after completion of printing:	
	<Report Findings Here>	
2A-3.1.2.c If the application facilitates merchant printing of full PANs on receipts due to a legal or regulatory obligation, install and configure the application according to the application vendor's documentation, including the application's Implementation Guide. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle	Describe test transactions performed (must utilize all functions of the application that handle account data):	
	<Report Findings Here>	
	Describe forensic tools and/or methods used to inspect the test transactions:	

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that: • The application only transmits clear-text PAN internally within the POI device to an integrated printer that is part of the PCI-approved POI device and is not attached via cabling or other networking mechanisms. • The P2PE application securely deletes the clear-text PAN after completion of printing.	*<Report Findings Here>*	
2A-3.2 The application must not facilitate, via its own logical interface(s), sharing of clear-text account data directly with other applications. ***Note:*** *The application is allowed to share clear-text account data directly with the POI device's SRED-approved firmware.*		
2A-3.2.a Examine the application's Implementation Guide required at 2C-3 of this document and determine that it includes the following: • A list of all logical interfaces for the application, and the function/purpose of each. • The logical interfaces intended for sharing of clear-text account data (e.g., those used to pass clear-text data back to the approved firmware of the POI device). • The logical interfaces not intended for sharing of clear-text account data (e.g., those for communication with other applications). • Examine the logical interfaces used to communicate with other applications and confirm that the application cannot share clear-text account data with other applications via these logical interfaces. *Note that the application may be the only POI-resident application at the time of assessment, but other assessed applications may be added to a P2PE solution at a later date; or the application may be added to a solution that includes pre-approved applications. The assessor must test this requirement with this point in mind.*	Identify the P2PE Assessor who confirms that the application's Implementation Guide includes all details for 2A-3.2.a:	*<Report Findings Here>*
2A-3.2.b Perform a source-code review and verify that the application cannot directly facilitate sharing of clear-text account data with other applications via its logical interfaces.	Describe how the source-code review verified that the application cannot directly facilitate sharing of clear-text account data with other applications via its logical interfaces:	
	<Report Findings Here>	
2A-3.2.c Install and configure the application according to the application vendor's documentation, including the application's Implementation Guide. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that the application cannot directly facilitate sharing of clear-text account data with other applications via its logical interfaces.	Describe test transactions performed (must utilize all functions of the application that handle account data):	
	<Report Findings Here>	
	Describe forensic tools and/or methods used to inspect the test transactions:	
	<Report Findings Here>	

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2A-3.3 The application must only use external communication methods included in the PCI-approved POI device evaluation. For example, the POI device may provide an IP stack approved per the PTS Open Protocols module, 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. ***Note:*** *Using any external communication methods not included the PCI-approved POI device evaluation will invalidate the PTS approval and such use is prohibited in P2PE solutions.*		
2A-3.3.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 design documentation and verify that it contains a description of the application's function including the following: • A list of the external communication methods included in the POI device vendor's security guidance. • A list of which approved external communication methods are used by the application. • A description of where external communications are used by the application.	POI device vendor's security guidance documentation reviewed:	*<Report Findings Here>*
	Application design documentation reviewed:	*<Report Findings Here>*
2A-3.3.b Examine the application's Implementation Guide required at 2C-3 of this document and verify it includes guidance that the use of any other method for external communication is not allowed.	Identify the P2PE Assessor who confirms that the application's Implementation Guide includes guidance that the use of any other method for external communication is not allowed:	*<Report Findings Here>*
2A-3.3.c Perform a source-code review and verify that, when configured appropriately, the application only utilizes the external communication methods included in the POI device vendor's security guidance and does not implement its own external communication methods (e.g., does not implement its own IP stack).	Describe how the source-code review verified that, when configured appropriately, the application only utilizes the external communication methods included in the POI device vendor's security guidance and does not implement its own external communication methods:	
	<Report Findings Here>	
2A-3.3.d Install and configure the application according to the application vendor's documentation, including the application's Implementation Guide. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that: The application uses only the external communication methods included in the POI device vendor's security guidance for all external communications.	Describe test transactions performed (must utilize all functions of the application that handle account data):	
	<Report Findings Here>	
	Describe forensic tools and/or methods used to inspect the test transactions:	
	<Report Findings Here>	

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2A-3.4 Any whitelisting functionality implemented by the application must include guidance in the application's Implementation Guide that includes the following: • How to configure the whitelisting functionality to ensure the output of clear-text account data is prohibited, except for non-PCI payment brand account/card data. • How to perform cryptographic signing (or similar) prior to installation on the POI device by authorized personnel using dual control. • How to perform cryptographic authentication by the POI device's firmware. • That review of whitelist functionality must be performed to confirm it only outputs non-PCI payment brand account/card data. • That such functionality must be approved by authorized personnel prior to implementation. • That all new installations or updates to whitelist functionality must include the following: – Description and justification for the functionality. – Who approved the new installation or updated functionality prior to release. – Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data.		
2A-3.4.a For any whitelisting functionality implemented by the application, examine the application's Implementation Guide required at 2C-3 of this document and verify it contains details to describe any whitelisting functionality and that it provides instructions as follows: • How to configure the application functionality to ensure the output of clear-text account data is prohibited, except for non-PCI payment brand account/card data • How to perform cryptographic signing (or similar) prior to installation on the POI device by authorized personnel using dual control. • How to establish cryptographically authentication by the POI device's firmware. • That review of whitelist functionality must be performed to confirm it only outputs non-PCI payment brand account/card data. • That such functionality must be approved by authorized personnel prior to implementation. • That documentation for all new installations or updates to whitelist functionality includes the following: – Description and justification for the functionality. – Who approved the new installation or updated functionality prior to release. – Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data.	Identify the P2PE Assessor who confirms that the application's Implementation Guide includes all details for 2A-3.4.a:	*<Report Findings Here>*
2B-1.1 Applications must be 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:		

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2B-1.1.a Examine the application vendor's 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. • Applications are developed in accordance with all applicable P2PE requirements. .	Documented software development processes reviewed:	*<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.	POI device vendor's security guidance documentation reviewed:	*<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 (e.g., application configuration settings which are necessary for the application to function with the device).	Identify the P2PE Assessor who confirms that the application's Implementation Guide provides information from the POI device vendor's security guidance applicable to the solution provider:	*<Report Findings Here>*
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 and interview software developers. • Examine testing documentation and samples of test data, observe testing processes, and interview software-testing personnel. • Examine the final application product.	Reporting responses at 2B-1.1.1 and 2B-1.1.2; no further reporting required here.	
2B-1.1.1 Live PANs must not be used for testing or development.		
2B-1.1.1 Live PANs are not used for testing or development.	Documented software development processes reviewed:	*<Report Findings Here>*
	Software developers interviewed:	*<Report Findings Here>*
	Software-testing personnel interviewed:	*<Report Findings Here>*
	Describe how testing documentation, samples of test data and the final application product verified that live PANs are not used for testing or development:	
	<Report Findings Here>	

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2B-1.1.2 Development, test, and/or custom application data/accounts, user IDs, and passwords must be removed before applications are released for production or released to customers.		
2B-1.1.2 Examine written software-development procedures and interview responsible personnel to verify that development, test, and/or custom application data/accounts, user IDs, and passwords are removed before an application is released for production or released to customers.	Documented software development processes reviewed:	*<Report Findings Here>*
	Software developers interviewed:	*<Report Findings Here>*
	Software-testing personnel interviewed:	*<Report Findings Here>*
	Describe how testing documentation samples of test data and the final application product verified that development, test, and/or custom application data/accounts, user IDs, and passwords are removed before an application is released for production or released to customers:	
	<Report Findings Here>	
2B-1.2 Application code and any non-code configuration mechanisms must be reviewed prior to every release or update. The review process includes the following:		
2B-1.2 Examine written software-development procedures and interview responsible personnel to verify the application vendor performs reviews for all application code changes and non-code configuration mechanisms as follows: • Reviews are performed by an individual, other than the code author, who is knowledgeable in code-review techniques and secure coding practices. • Changes to code that manages security-sensitive configuration options are reviewed to confirm that they will not result in the exposure of PCI payment-brand accounts/cards. • Code reviews ensure code is developed according to secure coding guidelines.	Documented software-development procedures reviewed:	*<Report Findings Here>*
	Responsible personnel interviewed:	*<Report Findings Here>*
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 Examine code review results for a sample of code changes to confirm that code reviews are performed by an individual other than the code author who is knowledgeable in code-review techniques and secure coding practices.	Sample of code changes reviewed for 2B-1.2.1 through 1.2.4:	*<Report Findings Here>*
	Describe how code review results for the sample of code changes confirmed that code reviews are performed by an individual other than the code author who is knowledgeable in code-review techniques and secure coding practices:	
	<Report Findings Here>	
2B-1.2.2 Performing code reviews to ensure code is developed according to secure coding guidelines.		

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2B-1.2.2 Examine code-review results for a sample of code changes to verify that code reviews ensure code is developed according to secure coding guidelines.	Describe how code review results for the sample of code changes verified that code reviews ensure code is developed according to secure coding guidelines:	
	<Report Findings Here>	
2B-1.2.3 Confirming that appropriate corrections are implemented prior to release.		
2B-1.2.3 Examine change control documentation for a sample of code changes to verify that appropriate corrections are implemented prior to release.	Change control documentation reviewed:	*<Report Findings Here>*
2B-1.2.4 Review and approval of review results by management prior to release.		
2B-1.2.4 Examine change control documentation for a sample of code changes to verify that review results are reviewed and approved by management prior to release.	Change control documentation reviewed:	*<Report Findings Here>*
2B-1.3 All changes to the application must follow change-control procedures. The procedures must include the following:		
2B-1.3.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	Documented developer change-control procedures for software modifications reviewed:	*<Report Findings Here>*
2B-1.3.b Examine the application's Implementation Guide required at 2C-3 of this document and verify it includes the following: • Documentation detailing the impact of all changes included in the relevant application release • Instructions detailing back-out or de-installation procedures for the application	Identify the P2PE Assessor who confirms that the application's Implementation Guide includes all details for 2B-1.3.b:	*<Report Findings Here>*
2B-1.3.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:	*<Report Findings Here>*
	Related change-control documentation reviewed:	*<Report Findings Here>*
2B-1.3.1 Documentation of impact		
2B-1.3.1 Verify that documentation of customer impact is included in the change-control documentation for each change.	Identify the P2PE Assessor who verified that, for each change examined, this was documented according to the change-control procedures:	*<Report Findings Here>*

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2B-1.3.2 Documented approval of change by appropriate authorized parties		
2B-1.3.2 Verify that documented approval by appropriate authorized parties is present for each change.	Identify the P2PE Assessor who verified that, for each change examined, this was documented according to the change-control procedures:	*<Report Findings Here>*
2B-1.3.3 Functionality testing to verify that the change does not adversely impact the security of the device.		
2B-1.3.3.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.	Identify the P2PE Assessor who verified that, for each change examined, this was documented according to the change-control procedures:	*<Report Findings Here>*
2B-1.3.3.b Verify that all changes (including patches) are tested per secure coding guidance before being released.	Identify the P2PE Assessor who verified that, for each change examined, this was documented according to the change-control procedures:	*<Report Findings Here>*
2B-1.3.4 Back-out, rollback, or application de-installation procedures.		
2B-1.3.4 Verify that back-out, rollback, or application de-installation procedures are prepared for each change.	Identify the P2PE Assessor who verified that, for each change examined, this was documented according to the change-control procedures:	*<Report Findings Here>*
2B-1.4 Applications must be developed according to industry best practices for secure coding techniques, including (but not limited to): • Developing with least privilege. • Developing with fail-safe exception handling. • Developing with defensive (protective) techniques regarding the logical input interfaces of the application.		
2B-1.4 Examine software development processes and interview software developers to verify that secure coding techniques are defined and include: • Developing with least privilege. • Developing with fail-safe defaults. • Developing with defensive (protective) techniques regarding the logical input interfaces of the application.	Documented software processes reviewed:	*<Report Findings Here>*
	Software developers interviewed:	*<Report Findings Here>*
2B-1.4.1 Application development processes must include prevention of common coding vulnerabilities.		

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2B-1.4.1.a Obtain and review software development processes for applications. Verify the process includes prevention of common coding vulnerabilities relevant to the programming languages and platforms in use.	Documented software processes reviewed:	*<Report Findings Here>*
2B-1.4.1.b 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 how manual or automated penetrating testing performed verified that applications are not vulnerable to common coding vulnerabilities:	
	<Report Findings Here>	
2B-1.4.2 Application risk-assessment techniques (e.g., (application threat-modeling) must be used to identify potential application-security design flaws and vulnerabilities during the software-development process. Risk-assessment processes include the following: • Coverage of all functions of the application, including but not limited to, security-impacting features and features that cross trust boundaries. • Assessment of application decision points, process flows, data flows, data storage, and trust boundaries. • Identification of all areas within the application that interact with account data, as well as any process-oriented outcomes that could lead to the exposure of account data. • A list of potential threats and vulnerabilities resulting from account-data flow analyses and assigned risk ratings (e.g., high, medium, or low priority) to each. • Implementation of appropriate corrections and countermeasures during the development process. • Documentation of application risk-assessment results for management review and approval.		
2B-1.4.2 Examine written software development procedures and interview responsible personnel to verify the vendor uses application risk-assessment techniques as part of the software development process, and that the processes include: • Coverage of all functions of the application, including but not limited to, security-impacting features and features that cross trust boundaries. • Assessment of application decision points, process flows, data flows, data storage, and trust boundaries. • Identification of all areas within applications that interact with account data, as well as any process-oriented outcomes that could lead to the exposure of account data. • A list of potential threats and vulnerabilities resulting from account-data flow analyses, and assigned risk ratings (e.g., high, medium, or low priority) to each. • Implementation of appropriate corrections and countermeasures during the development process. • Documentation of application risk-assessment results for management review and approval.	Documented software development procedures reviewed:	*<Report Findings Here>*
	Responsible personnel interviewed:	*<Report Findings Here>*

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2B-1.5 Application vendor must provide training in secure development practices to application developers, as applicable for the developer's job function and technology used, e.g.: • Secure application design. • Secure coding techniques to avoid common coding vulnerabilities (e.g., vendor guidelines, OWASP Top 10, SANS CWE Top 25, CERT Secure Coding, etc.). • Managing sensitive data in memory. • Code reviews. • Security testing (e.g., penetration testing techniques). • Risk-assessment techniques. ***Note:*** *Training for application developers may be provided in-house or by third parties. Examples of how training may be delivered include on-the-job, instructor-led, and computer-based.*		
2B-1.5.a Verify documented software development processes require training in secure development practices for application developers, as applicable for the developer's job function and technology used.	Documented software development processes reviewed:	*<Report Findings Here>*
2B-1.5.b Interview a sample of developers to verify that they are knowledgeable in secure development practices and coding techniques, as applicable to the technology used.	Sample of developers interviewed:	*<Report Findings Here>*
2B-1.5.c Examine records of training to verify that all application developers receive training as applicable for their job function and technology used.	Identify records of training for application developers examined:	*<Report Findings Here>*
2B-1.5.1 Training must be updated as needed to address new development technologies and methods used.		
2B-1.5.1 Examine training materials and interview a sample of developers to verify that training is updated as needed to address new development technologies and methods used.	Identify training materials examined:	*<Report Findings Here>*
	Sample of developers interviewed:	*<Report Findings Here>*
2B-1.6 Secure source-control practices must be implemented to verify integrity of source-code during the development process.		
2B-1.6.a Examine written software-development procedures and interview responsible personnel to verify the vendor maintains secure source-code control practices to verify integrity of source-code during the development process.	Documented software development procedures reviewed:	*<Report Findings Here>*
	Responsible personnel interviewed:	*<Report Findings Here>*
2B-1.6.b Examine mechanisms and observe procedures for securing source-code to verify integrity of source-code is maintained during the development process.	Describe how mechanisms and procedures for securing source-code verified that integrity of source-code is maintained during the development process:	
	<Report Findings Here>	

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2B-1.7 The application vendor must document and follow a software-versioning methodology as part of their system-development lifecycle. The methodology must follow the procedures in the P2PE Program Guide for changes to payment applications and include at least the following:		
2B-1.7.a Examine documented software-development processes to verify they include the application vendor's versioning methodology, and that the versioning methodology must be in accordance with the P2PE Program Guide. Verify that the documented versioning methodology is required to be followed for the application, including all changes to the application.	Documented software development procedures reviewed:	*<Report Findings Here>*
2B-1.7.1 The vendor's software versioning methodology must define the specific version elements used, including at least the following: • Details of how the elements of the version scheme are in accordance with requirements specified in the P2PE Program Guide. • The format of the version scheme, including number of elements, separators, character set, etc. (consisting of alphabetic, numeric, and/or alphanumeric characters). • Definition of what each element represents in the version scheme (e.g., type of change, major, minor, or maintenance release, wildcard, etc.). • Definition of elements that indicate use of wildcards. ***Note:*** *Wildcards may only be substituted for elements of the version number that represent non-security impacting changes. Refer to 2B-6.3 for additional requirements on the use of wildcards.*		
2B-1.7.1.a Examine recent application changes, the version numbers assigned, and the change control documentation that specifies the type of application change and verify that the elements in the version number match the applicable change and the parameters defined in the documented versioning methodology.	Change control documentation reviewed:	*<Report Findings Here>*
	Describe how the recent application changes, version numbers assigned and change control documentation verified that the elements in the version number match the applicable change and the parameters defined in the documented versioning methodology:	
	<Report Findings Here>	
2B-1.7.1.b Interview a sample of developers and verify that they are knowledgeable in the version scheme, including the acceptable use of wildcards in the version number.	Sample of developers interviewed:	*<Report Findings Here>*
2B-1.8 The versioning methodology must indicate the type and impact of all application changes in accordance with the P2PE Program Guide, including: • Description of all types and impacts of application changes (e.g., changes that have no impact, low impact, or high impact to the application). • Specific identification and definition of changes that: – Have no impact on functionality of the application or its dependencies – Have impact on application functionality but no impact on security or P2PE requirements – Have impact to any security functionality or P2PE requirement. • How each type of change ties to a specific version number.		

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2B-1.8.a Examine the software vendor's documented versioning methodology to verify the version methodology includes: • Description of all types and impacts of application changes (e.g., changes that have no impact, low impact, or high impact to the application). • Specific identification and definition of changes that: – Have no impact on functionality of the application or its dependencies – Have impact on application functionality but no impact on security or P2PE requirements – Have impact to any security functionality or P2PE requirement. • How each type of change ties to a specific version number.	Documented versioning methodology reviewed:	*<Report Findings Here>*
2B-1.8.b Verify that the versioning methodology is in accordance with the P2PE Program Guide requirements.	Identify the P2PE Assessor who confirms that the versioning methodology is in accordance with the P2PE Program Guide requirements:	*<Report Findings Here>*
2B-1.8.c Interview personnel and observe processes for each type of change to verify that the documented methodology is being followed for all types of changes.	Personnel interviewed:	*<Report Findings Here>*
	Describe processes observed that verified that the documented methodology is being followed for all types of changes:	
	<Report Findings Here>	
2B-1.8.d Select a sample of recent payment application changes and review the change control documentation that specifies the type of application change to verify that the version assigned to the change matches the type of change according to the documented methodology.	Sample of recent payment application changes reviewed:	*<Report Findings Here>*
	Change control documentation reviewed:	*<Report Findings Here>*
2B-1.9 The versioning methodology must specifically identify whether wildcards are used and, if so, how they are used. The following must be included: • Details of how wildcards are used in the versioning methodology. • Wildcards are never used for any change that has an impact on the security of the application and/or the POI device. • Any element of the version number used to represent a non-security-impacting change (including a wildcard element) must never be used to represent a security impacting change. • Wildcard elements must not precede version elements that could represent security-impacting changes. Any version elements that appear after a wildcard element must not be used to represent security-impacting changes. ***Note:*** *Wildcards may only be used in accordance with the P2PE Program Guide.*		

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2B-1.9.a Examine the software vendor's documented versioning methodology to verify that it includes specific identification of how wildcards are used, including: • Details of how wildcards are used in the versioning methodology. • Wildcards are never used for any change that has an impact on the security of the application and/or the POI device. • Any element of the version number used to represent a non-security-impacting change (including a wildcard element) must never be used to represent a security impacting change. • Any elements to the right of a wildcard cannot be used for a security-impacting change. Version elements reflecting a security-impacting change must appear "to the left of" the first wildcard element.	Documented versioning methodology reviewed:	*<Report Findings Here>*
2B-1.9.b Verify that any use of wildcards is in accordance with the P2PE Program Guide requirements—e.g., elements that appear after a wildcard element cannot be used for a security impacting change.	Identify the P2PE Assessor who confirms that any use of wildcards documented versioning methodology is in accordance with the P2PE Program Guide:	*<Report Findings Here>*
2B-1.9.c Interview personnel and observe processes for each type of change to verify that: • Wildcards are never used for any change that has an impact on security or any P2PE requirements. • Elements of the version number used to represent non-security-impacting changes (including a wildcard element) are never be used to represent a security impacting change.	Personnel interviewed:	*<Report Findings Here>*
	Describe processes observed that verified that wildcards are never used for any change that has an impact on security or any P2PE requirements and that elements of the version number used to represent non-security-impacting changes (including a wildcard element) are never be used to represent a security impacting change:	
	<Report Findings Here>	
2B-1.9.d Select a sample of recent payment application changes and review the change control documentation that specifies the type of application change. Verify that: • Wildcards are not used for any change that has an impact on security or any P2PE requirements. • Elements of the version number used to represent non-security-impacting changes (including a wildcard element) are not used to represent a security impacting change.	Sample of recent payment applications reviewed:	*<Report Findings Here>*
	Change control documentation reviewed:	*<Report Findings Here>*
2B-1.10 The vendor's published versioning methodology must be communicated to customers and integrators/ resellers.		

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2B-1.10 Verify the application's Implementation Guide required at 2C-3 of this document includes a description of the vendor's published versioning methodology for customers and integrators/resellers, and includes the following: • Details of versioning scheme, including the format of the version scheme (number of elements, separators, character set, etc.) • Details of how security-impacting changes will be indicated by the version scheme • Details of how other types of changes will affect the version • Details of any wildcard elements that are used, including confirmation that they will never be used to represent a security-impacting change	Identify the P2PE Assessor who confirms that the application's Implementation Guide includes all details for 2B-1.10:	*<Report Findings Here>*
2B-1.11 If an internal version mapping to published versioning scheme is used, the versioning methodology must include mapping of internal versions to the external versions.		
2B-1.11.a Examine the documented version methodology to verify it includes a mapping of internal versions to published external versions.	Identify the P2PE Assessor who confirms that the documented version methodology includes a mapping of internal versions to published external versions:	*<Report Findings Here>*
2B-1.11.b Examine recent changes to confirm internal version mapping to published versioning scheme match according to the type of change.	Sample of recent changes reviewed:	*<Report Findings Here>*
2B-1.12 Software vendor must have a process in place to review application updates for conformity with the versioning methodology prior to release.		
2B-1.12.a Examine documented software development processes and the versioning methodology to verify there is a process in place to review application updates for conformity with the versioning methodology prior to release.	Documented software development processes reviewed:	*<Report Findings Here>*
2B-1.12.b Interview software developers and observe processes to verify that application updates are reviewed for conformity with the versioning methodology prior to release.	Software developers interviewed:	*<Report Findings Here>*
	Describe processes observed that verified that application updates are reviewed for conformity with the versioning methodology prior to release:	
	<Report Findings Here>	
2B-1.13 Software vendor must implement a process to document and authorize the final release of the application and any application updates. Documentation must include: • Signature by an authorized party to formally approve release of the application or application update. • Confirmation that secure development processes were followed by the vendor.		
2B-1.13.a Examine documented processes to verify that final release of the application and any application updates are formally approved and documented, including a signature by an authorized party to formally approve the release and confirmation that all SDLC processes were followed.	Documented processes reviewed:	*<Report Findings Here>*

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2B-1.13.b For a sample of recent releases of application and application updates, review approval documentation to verify it includes: • Formal approval and signature by an authorized party. • Confirmation that that all secure development processes were followed.	Sample of recent releases of application and application updates reviewed:	*<Report Findings Here>*
	Approval documentation reviewed:	*<Report Findings Here>*
2B-2.1 Where the application relies on the Open Protocol functionality of the POI device firmware, the application must be developed in accordance with the POI device vendor's security guidance. ***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.a Examine documented processes (including design documentation) and verify the application is developed in accordance with the POI device vendor's security guidance.	Documented processes reviewed (including design documentation):	*<Report Findings Here>*
2B-2.1.b 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: • Any instructions on how to securely configure any configurable options, as applicable to the application's specific business processing • Any guidance that the POI device vendor intended for integrators/ resellers, solution providers, and/or end-users	Identify the P2PE Assessor who confirms that the application's Implementation Guide includes all details for 2B-2.1.b:	*<Report Findings Here>*
2B-2.1.1 The application must not circumvent, bypass, or add additional services or protocols to the Open Protocols of the POI device firmware as approved and documented in the POI device vendor's security guidance. This includes the use of: • Link Layer protocols • IP protocols • Security protocols • IP services ***Note:*** *The PTS POI Open Protocols module ensures that open protocols and services in POI devices do not have vulnerabilities that can be remotely exploited and yield access to sensitive data or resources in the device. The POI device vendor defines what protocols and services are supported by the device and provides guidance to their use.* *Adding or enabling additional services or protocols, or failing to follow the issued POI device vendor's security guidance will invalidate the approval status of that device for that implementation.*		

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2B-2.1.1. Perform a source-code review and verify that the application: • Was developed according to the POI device vendor's security guidance with respect to the documented Open Protocols. • Does not circumvent, bypass, or add additional services or protocols to the Open Protocols of the POI device firmware as approved and documented in the POI device's vendor security guidance. This includes the use of: ○ Link Layer protocols ○ IP protocols ○ Security protocols ○ IP services	Describe how the source-code review verified that the application was developed according to the POI device vendor's security guidance with respect to the documented Open Protocols:	
	<Report Findings Here>	
	Describe how the source-code review verified that the application does not circumvent, bypass, or add additional services or protocols to the Open Protocols of the POI device firmware as approved and documented in the POI device's vendor security guidance:	
	<Report Findings Here>	
2B-2.2 The application-development process must include 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. Confirm that the application's Implementation Guide required at 2C-3 of this document is in accordance with 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 P2PE Assessor who confirms that the application's Implementation Guide includes all details for 2B-2.2.a:	*<Report Findings Here>*
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 POI device vendor's security guidance.	Describe how the source-code review verified that any connection to, or use of, shared resources is done securely and in accordance with the POI 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. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify that any connections to, or use of, shared resources are handled securely and in accordance with the POI device vendor's security guidance.	Describe test transactions performed (must utilize all functions of the application that handle account data):	
	<Report Findings Here>	
	Describe forensic tools and/or methods used to inspect the test transactions:	
	<Report Findings Here>	

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2B-2.3 Applications do not bypass or render ineffective any application segregation that is enforced by the POI device.		
2B-2.3 Perform a source-code review and verify that applications do not bypass or render ineffective any application segregation that is enforced by the POI device, in accordance with the POI device vendor's security guidance.	Describe how the source-code review verified that applications do not bypass or render ineffective any application segregation that is enforced by the POI device:	
	<Report Findings Here>	
2B-2.4 Applications do not bypass or render ineffective any OS hardening implemented by the POI device.		
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 device, in accordance with the device vendor's security guidance.	Describe how the source-code review verified that applications do not bypass or render ineffective any OS hardening which is implemented by the POI device:	
	<Report Findings Here>	
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 device, in accordance with the device vendor's security guidance.		
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 device, in accordance with the device vendor's security guidance.	Describe how the source-code review verified that applications do not bypass or render ineffective any encryption or account-data security methods implemented by the POI device:	
	<Report Findings Here>	
2B-2.6 If the application provides configuration/update functionality at-the-terminal (e.g., using an on-screen menu system), the application must not bypass or render ineffective any applicable controls contained within this standard. ***Note:*** *Some applications may provide administrative or other privileged functions at the terminal, such as the ability to load whitelists or change other application configurations. Any such functions provided in this way must meet all applicable P2PE requirements.*		
2B-2.6 If the application provides configuration/update functionality at the terminal, perform a functional test of the application loaded on each applicable POI device type and verify that the application does not bypass or render ineffective any applicable controls contained within this standard.	Describe how functional test of the application loaded on each applicable POI device type verified that the application does not bypass or render ineffective any applicable controls contained within this standard:	
	<Report Findings Here>	
2B-3.1 The application developer's process must include 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:	Application developer's system development documentation reviewed:	*<Report Findings Here>*

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2B-3.1.1 The application developer must provide key-management security guidance describing how cryptographic keys and certificates have to be used. *Examples of guidance include which cryptographic certificates to load, how to load account-data keys (through the firmware of the device), when to roll keys, etc.*		
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 cryptographic keys and certificates have to be used and managed.	Identify the P2PE Assessor who confirms that the application's Implementation Guide includes all details for 2B-3.1.1:	*<Report Findings Here>*
2B-3.1.2 The application developer must perform 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.	Application developers interviewed:	*<Report Findings Here>*
2B-4.1 The application must not encrypt clear-text account data. This means the application must not implement any encryption functions that bypass or are intended to be used instead of the approved SRED functions of the POI device.		
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 encryption of clear-text account-data, nor does it replace the POI device's SRED encryption • A description of the purpose and encryption method for any encryption provided by the application in addition to SRED encryption	Identify the P2PE Assessor who confirms that the application's Implementation Guide includes all details for 2B-4.1.a:	*<Report Findings Here>*
2B-4.1.b Perform a source-code review to verify that any application functionality facilitating the encryption of account data utilizes the approved cryptographic algorithm(s) and associated key-management functions of the POI device's SRED firmware and is not implemented within the application itself.	Describe how the source-code review verified that any application functionality facilitating the encryption of account data utilizes the approved cryptographic algorithm(s) and associated key-management functions of the POI device's SRED firmware and is not implemented within the application itself:	
	<Report Findings Here>	
2B-4.1.c Install and configure the application according to the application vendor's documentation, including the application's Implementation Guide. Using an appropriate "test platform" (if necessary), perform test transactions that utilize all functions of the application that handle account data. Use forensic tools and/or methods (commercial tools, scripts, etc.) to verify the application does not perform encryption of account-data nor does it replace the SRED encryption performed by the underlying POI device's firmware.	Describe test transactions performed (must utilize all functions of the application that handle account data):	
	<Report Findings Here>	
	Describe forensic tools and/or methods used to inspect the test transactions:	
	<Report Findings Here>	

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
2C-1.1 Software developers must establish and implement a process to identify and test their applications for security vulnerabilities and implementation errors prior to every release (including updates or patches) using manual or automated vulnerability assessment processes.		
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.	Documented processes reviewed:	*<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.	Responsible software vendor personnel interviewed:	*<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.	Documented processes reviewed:	*<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.	Responsible software vendor personnel interviewed:	*<Report Findings Here>*
2C-2.1 Ensure that all application installations and updates are cryptographically authenticated as follows:		
2C-2.1 To confirm that all application installations and updates are cryptographically authenticated, verify the following:		
2C-2.1.1 All application installations and updates are cryptographically authenticated using the approved security mechanisms of the POI device's firmware.		
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 is cryptographically authenticated using the approved security mechanisms of the POI device's firmware for any application installations and updates. • Instructions for how to use the approved security mechanisms to perform application installations and updates. • A statement that application installations and updates cannot occur except by using the approved security mechanisms of the POI device's firmware.	Identify the P2PE Assessor who confirms that the application's Implementation Guide includes all details for 2C-2.1.1.a:	*<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 mechanisms of the POI device's firmware.	Describe how the source-code review verified that the application only allows installations and updates using the approved security mechanisms of the POI device's firmware:	

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
	<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 mechanisms of the POI device's firmware.	Describe test transactions performed (must utilize all functions of the application that handle account data):	
	<Report Findings Here>	
	Describe forensic tools and/or methods used to inspect the test transactions:	
	<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 mechanisms, and verify that the POI device will not allow the installation or update to occur.	Describe how attempting to perform an installation and an update using non-approved security mechanisms verified that the POI device will not allow the installation or update to occur:	
	<Report Findings Here>	
2C-2.1.2 The application developer includes guidance for whoever signs the application, including requirements for dual control over the application-signing process.		
2C-2.1.2 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. • 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.	Identify the P2PE Assessor who confirms that the application's Implementation Guide includes all details for 2C-2.1.2:	*<Report Findings Here>*
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).	Documented processes for dissemination reviewed:	*<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.	Identify the P2PE Assessor who confirms that the application's Implementation Guide includes all details for 2C-3.1.1:	*<Report Findings Here>*

Domain 2: Application Security – Reporting		
Requirements and Testing Procedures	**Reporting Instructions and Assessor's Findings**	
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 (e.g., 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 P2PE Assessor who confirms that the application's Implementation Guide includes all details for 2C-3.1.2.a:	*<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 (e.g., device changes/upgrades and major and minor software changes). • Any changes to the Implementation Guide requirements in this document.	Identify the P2PE Assessor who confirms that the application's Implementation Guide includes all details for 2C-3.1.2.b:	*<Report Findings Here>*
2C-3.1.3 Distribution to all new and existing application installers (e.g., 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 P2PE Assessor who confirms that the application's Implementation Guide includes all details for 2C-3.1.3:	*<Report Findings Here>*
2C-3.2 Develop and implement training and communication programs to ensure application installers (e.g., 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.	Training materials and communication program documentation reviewed:	*<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. Update 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.	Training materials and communication program documentation reviewed:	*<Report Findings Here>*