Payment Card Industry (PCI)

Point-to-Point Encryption (P2PE)

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

Solution P-ROV Template

For PCI P2PE Standard v1.1.1
Hardware/Hardware P2PE solutions

July 2013

Document Changes

Date	Document Version	Description	Pages
September 2012	1.0	To introduce the template for submitting Solution P-ROVs for 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 for Hardware/Hardware P2PE solutions	

Copyright 2012 PCI Security Standards Council LLC

Table of Contents

Copyright 2012 PCI Security Standards Council LLC

Introduction to P2PE Solution P-ROV Template

This document provides the template for completing a Solution P-ROV to report compliance of a PCI P2PE solution. This template is accompanied by Solution P-ROV Reporting Instructions - *Solution P-ROV Reporting Instructions for PCI P2PE Standard v1.1*. P2PE assessors should refer to the Reporting Instructions before beginning a Solution P-ROV.

Solution 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 Solution P-ROV Reporting Instructions provide further instruction on how to complete the Solution 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.*

Copyright 2012 PCI Security Standards Council LLC

Solution P-ROV Template for PCI P2PE Standard v1.1

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

1. Contact Information and Report Date

1.1 Contact Information			
Solution Provider 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:	

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

Copyright 2012 PCI Security Standards Council LLC

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 P2PE Solution Details	
P2PE solution name:	
Description of P2PE solution provider (e.g., payment gateway, acquirer, multi-acquirer payment processor, etc.):	
Description of the types of POI devices used in solution (e.g., unattended kiosks, payment terminals for use with in-store POS, etc.):	
Description of the typical merchant that uses this solution (Include specific industries or channels the solution is intended for):	

Copyright 2012 PCI Security Standards Council LLC

2.2 Entities involved in P2PE solution	
Entities performing key injection	
Entity Name:	Entity Location(s):
Entities performing remote key distribution	
Entity Name:	Entity Location(s):
Entities performing Certificate Authority (CA) function	
Entity Name:	Entity Location(s):
Entities performing Registration Authority (RA) function	
Entity Name:	Entity Location(s):
P2PE Solution Provider-authorized Integrator/Resellers (if applicable)	
Entity Name:	Entity Location(s):

Other entities involved in P2PE solution (if applicable)		
Entity Name:	Role/Function:	Entity Location(s):

Copyright 2012 PCI Security Standards Council LLC

2.3 P2PE Solution Listing Details		
Is the solution already listed on the PCI SSC List of Validated P2PE Solutions?	☐ Yes	☐ No
If Yes, provide PCI SSC listing number:		

List of POI devices and applications for inclusion in solution listing *(Complete a separate table for all POI device types used in P2PE solution)*			
• POI device type name/ identifier:			
• POI device manufacturer, model and number:			
• PTS approval number for POI device:			
• POI Hardware version #:			
• POI Firmware version #:			
List of all Applications on the POI device	Application version #	Application has access to clear-text account data (Yes/No)	For all applications with access to clear-text account data: PCI SSC listing number (if applicable), or status of Application P-ROV (if known)*

***Note:** An Application P-ROV must be submitted and accepted by PCI SSC for all applications with access to clear-text account data.*

2.4 P2PE Decryption Environments			
Entity	Location	Date of last PCI DSS validation	P2PE endpoint system identifier/description (e.g., HSM)

Copyright 2012 PCI Security Standards Council LLC

2.5 Overview of P2PE solution data flow

Provide a ***high-level*** data flow diagram of the solution that illustrates:

- Flows and locations of P2PE-encrypted account data
- Flows and locations of cleartext account data
- Location of critical system components (e.g., HSMs, host processing systems)
- All entities the solution connects to for payment transmission or processing, including processors/acquirers.

Note: *the diagram should identify where merchant entities fit into the data flow, without attempting to identify individual merchants. For example P2PE-encrypted account data could be illustrated as flowing between an icon that represents all merchant customers to an icon that represents the solution provider's decryption environment.*

2.6 Multi-Acquirer and Multi-Solution Implementations

Do multiple acquirers or multiple solution providers manage one or more P2PE solutions on the same POI device?	☐ Yes	☐ No
If Yes, complete the following: Describe how management of the multi-acquirer or multi-provider solutions is divided between entities:		

If multiple acquirers or multiple solution providers manage one or more P2PE solutions on the same POI device, complete the following:

POI name/ identifier	Identify other P2PE solutions on the POI device	Is the other solution already listed, currently being assessed in a separate P2PE assessment, or included with this P2PE assessment?	If solution is already listed, provide PCI SSC listing number	If solution being assessed separately, identify P2PE assessor company performing assessment (if known)

Copyright 2012 PCI Security Standards Council LLC

2.7 P2PE Instruction Manual (PIM) Details	
For each type of POI included in the P2PE solution (as identified in 2.3 above), provide details of the PIM used and validated for this assessment:	
• POI device type name(s) / identifier(s)	
• Title of the PIM:	
• Date of the PIM:	
• Version of the PIM:	

2.8 Summary of P2PE Solution Compliance Status		
P2PE Domain	**Compliant**	
	Yes	**No**
Domain 1 – Encryption Device Management		
Domain 2 – Application Security		
Domain 3 – Encryption Environment		
Domain 4 – Segmentation between Encryption and Decryption Environments	N/A	
Domain 5 – Decryption Environment and Device Management		
Domain 6 – P2PE Cryptographic Key Operations		
Domain 6 – Annex A: Symmetric-Key Distribution using Asymmetric Techniques		
Domain 6 – Annex B: Key-Injection Facilities		

**** Note:** Only compliant P2PE solutions will be reviewed by PCI SSC for acceptance and listing.*

Copyright 2012 PCI Security Standards Council LLC

3. Details and Scope of Solution Assessment

3.1 Scoping Details	
Document how the P2PE assessor validated the accuracy of the P2PE scope for the assessment, including:	
The methods or processes used to identify all elements in scope of the P2PE solution assessment:	
Confirm that the scope of the assessment is accurate and covers all components and facilities for the P2PE solution:	

3.2 Segmentation at Solution Provider	
Identify coverage of PCI DSS compliance to solution provider environment (e.g., all solution provider environments, decryption environment only, decryption environment and some other environments, etc.):	
If the solution provider's PCI DSS compliance does not cover all solution provider environments:	
• Describe how the solution provider has implemented network segmentation to isolate P2PE decryption environments from any non-PCI DSS compliant environments:	
• Describe how the P2PE assessor validated the effectiveness of the segmentation:	

Copyright 2012 PCI Security Standards Council LLC

3.3 Solution Network Diagram

Provide one or more ***high-level*** network diagrams to illustrate the functioning of the P2PE solution, including:

- Locations of critical facilities, including the solution provider's decryption environment, key-injection and loading facilities, etc.
- Location of critical components within the P2PE decryption environment, such as HSMs and other SCDs, host systems, cryptographic key stores, etc., as applicable
- Location of systems performing key management functions
- Connections into and out of the decryption environment
- Other necessary components, as applicable to the particular solution

3.4 Facilities

Lab environment	
Identify and describe the lab environment used for this assessment, including whether the lab was provided by the P2PE assessor or the solution provider.	
Address of the lab environment used for this assessment:	

List of all facilities INCLUDED in this solution assessment	
Description and purpose of facility included in assessment	Address of facility

Copyright 2012 PCI Security Standards Council LLC

*List of facilities used in P2PE solution that were EXCLUDED from this solution assessment**			
Description and purpose of facility excluded from assessment	Address of facility	Explanation why the facility was excluded from the assessment	Details of any separate assessments performed for the facility, including how the other assessment was verified to cover all components in scope for this solution

***Note:** Does not include merchant locations.*

3.5 Key management processes

Description of Cryptographic Key Management Processes

Provide one or more ***high-level*** diagrams showing all key management processes, including:

- Key Generation
- Key Distribution / Loading / Injection onto POI devices
- Other Key Distribution / Loading / Injection activities
- Key Storage
- Key Usage
- Key Archiving (if applicable)

***Note:** include both logical and physical components – e.g., network traffic flows, locations of safes, use of secure couriers, etc.*

Description of Cryptographic Keys used in P2PE Solution	
Provide a brief description of all types of cryptographic keys used in the solution, as follows:*	
Key type / description	Purpose/ function of the key

* ***Note:** A detailed Key Matrix is included in Domain 6.*

Copyright 2012 PCI Security Standards Council LLC

3.6 Documentation and Personnel Interviews

List of all documentation reviewed for this solution assessment:

Document Name (including version, if applicable)	Brief description of document purpose	Document date

List of all personnel interviewed for this solution assessment:

Name	Company	Job Title	Topics covered

Copyright 2012 PCI Security Standards Council LLC

4. Findings and Observations

Domain 1: Encryption Device Management

Note: *Tables are provided to assist with the reporting process. Please see the P2PE Reporting Instructions for guidance on their use.*

Table 1.1 – List of all POI device types used in P2PE solution ***Note:*** *POI device types must be identified separately for each hardware version and for each firmware version*							
POI device type name/ identifier*	POI manufacturer	POI model name and number	PTS approval number	POI Hardware version # with SRED listed as a "function provided"	POI Firmware version # with SRED listed as a "function provided"	Application name and version number for all applications included in the PTS assessment	Total number of POI devices used in solution

**** Note:*** *Variations in POI device characteristics must not be combined into a single row; each specific POI device type must be individually listed in this table. POI details should be consistent with those identified for listing in Executive Summary section 2.3.*

Table 1.2 – Samples of POI Devices assessed for Domain 1 Testing Procedures ***Note:*** *Every POI device type listed in Table 1.1 must be included in every sample set in Table 1.2*			
POI device type name/ identifier (per Table 1.1)	**Sample Size** (Number of each device type assessed for Domain 1 Testing Procedures)	**Sampling Rationale** How sample size was determined to be appropriate and representative of the overall population	**Domain 1 Testing Procedures this sample was assessed against**
POI Sample Set #1– Description:			
POI Sample Set #2– Description:			

Copyright 2012 PCI Security Standards Council LLC

POI Sample Set #3 – Description:			

Table 1.3 – List of SCD device types used for Domain 1 operations

This includes SCDs used to generate or load cryptographic keys, encrypt keys, or sign applications to be loaded onto POI devices. Examples include HSMs, key-injection/loading devices (KLDs) and other devices that generate or load keys or sign applications and/or whitelists.

SCD device type identifier	SCD manufacturer	SCD model name and number	Brief description of device function/ purpose in P2PE solution	Device location(s)	Number of devices at each location

Table 1.4 – Samples of SCDs assessed for Domain 1 Testing Procedures

SCD device type identifier (per Table 1.3)	Device location	**Sample Size for each location** (Number of devices assessed at each location)	**Sampling Rationale** How sample size was determined to be appropriate and representative of the overall population	**Domain 1 Testing Procedures this sample was assessed against**
SCD Sample Set #1– Description:				
SCD Sample Set #2 – Description:				
SCD Sample Set #3 – Description:				

Copyright 2012 PCI Security Standards Council LLC

Table 1.5 – Samples of Transactions and POI Devices assessed for Domain 1 Testing Procedures ***Note:*** *Every POI device type listed in Table 1.1 must be included in every sample set in Table 1.5*				
POI device name/ identifier *	Transaction type (all supported transaction types to be included—e.g., purchase, refund, cancellation, clearing, etc.)	Brief description of sampled transaction	Number of transactions observed for each transaction type	**Domain 1 Testing Procedures this sample was assessed against**
Transaction Sample Set #1 – Description:				
Transaction Sample Set #2 – Description:				

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 1 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
1A-1 The security characteristics of secure cryptographic devices (SCDs) provide tamper-resistance, detection, and response features to help prevent successful attacks involving penetration, monitoring, manipulation, modification, or substitution of the devices to recover protected data.	
1A-1.1 Encryption operations must be performed using a device approved per the PCI PTS program (for example, a PCI-approved PED or SCR), with SRED (secure reading and exchange of data) listed as a "function provided." The PTS approval listing must match the deployed devices in the following characteristics: • Model name and number • Hardware version number • Firmware version number • Name and application version number of any applications resident within the device that were included in the PTS assess	
1A-1.1.a For all types of POI devices used in the solution, examine a sample of devices and device configurations, and review the list of approved PTS devices at www.pcisecuritystandards.org to verify that all POI devices used in this solution are listed, with a valid SSC listing number, on the PCI SSC website as Approved PCI PTS Devices with SRED listed as a "function provided."	*<Report Findings Here>*
1A-1.1.b Examine POI device configurations and review the PCI SSC list of Approved PCI PTS Devices to verify that all of the following POI device characteristics match the PCI PTS listing for the SRED function of each device: • Model name/number • Hardware version number • Firmware version number • Name and application version number of any applications resident within the device that were included in the PTS assessment	*<Report Findings Here>*
1A-1.1.1 SRED capabilities must be enabled and active.	
1A-1.1.1.a Examine the solution provider's documented procedures to verify that procedures are defined to ensure that SRED capabilities are enabled and active on all POI devices prior to devices being deployed to merchant environments.	*<Report Findings Here>*
1A-1.1.1.b Interview personnel and observe processes to verify that the implemented processes include ensuring that SRED capabilities are enabled and active on all devices prior to devices being deployed to merchant environments.	*<Report Findings Here>*
1A-1.1.1.c For a sample of all POI devices used in the solution, review POI device configurations to verify that all POI devices used in the solution have SRED capabilities enabled and active (that is, the POI devices are operating in "encrypting mode") prior to devices being deployed to merchant environments.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 1 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
1A-1.2 POIs must be configured to use only SRED-validated capture mechanisms for accepting and processing P2PE transactions. *For example, if a PCI-approved secure card reader (SCR) is provided with other POI components, the PCI-approved SCR must be the only capture mechanism used for P2PE transactions.*	
1A-1.2.a Examine documented deployment procedures to verify that POIs must be configured to use only SRED-validated capture mechanisms for accepting and processing P2PE transactions.	*<Report Findings Here>*
1A-1.2.b For all types of POI devices used in the solution, examine a sample of device configurations to verify that only SRED-validated capture mechanisms are configured to accept P2PE transactions.	*<Report Findings Here>*
1A-1.2.1 All capture mechanisms provided by the solution provider that are not SRED validated must be disabled or otherwise prevented from being used for P2PE transactions, and cannot be enabled by the merchant.	
1A-1.2.1.a Examine POI configuration and deployment procedures to verify they include either: Disabling all capture mechanisms that are not SRED validated, or Implementing configurations that prevent all non-SRED validated capture mechanisms from being used for P2PE transactions.	*<Report Findings Here>*
1A-1.2.1.b Verify that the documented procedures include ensuring that all non-SRED validated capture mechanisms are disabled or otherwise prevented from being used for P2PE transactions prior to devices being deployed to merchant environments.	*<Report Findings Here>*
1A-1.2.1.c For all types of POI devices used in the solution, examine a sample of device configurations to verify: All non-validated capture mechanisms are either disabled or configured to prevent their use for P2PE transactions, prior to devices being deployed to merchant environments. Disabled capture mechanism cannot be enabled by the merchant, and/or the configurations that prevent capture mechanisms from being used for P2PE transactions cannot be enabled by the merchant.	*<Report Findings Here>*
1A-1.3 Clear-text account data must not be disclosed to any component or device outside of the PCI-approved POI device prior to being transmitted to the solution provider's decryption environment.	
1A-1.3.a Examine documented transaction processes and data flows to verify that clear-text account data is not disclosed to any component or device outside of the PCI-approved POI prior to being transmitted to the solution provider's decryption environment.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 1 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
1A-1.3.b Using forensic tools and/or other data tracing methods, inspect a sample of transactions to verify that clear-text account data is not disclosed to any component or device outside of the PCI-approved POI prior to being transmitted to the solution provider's decryption environment.	*<Report Findings Here>*
1A-1.3.1 Any cryptographic keys that can be used to decrypt account data must not exist on any device outside of the PCI-approved POI device or the solution provider's decryption environment.	
1A-1.3.1.a Examine documented key-management policies and procedures to verify cryptographic keys that can be used to decrypt account data must not exist on any device outside of the PCI-approved POI or the solution provider's decryption environment.	*<Report Findings Here>*
1A-1.3.1.b Examine documented data flows and observe a sample of transactions to verify cryptographic keys that can be used to decrypt account data do not exist on any device outside of the PCI-approved POI, other than within the solution provider's decryption environment.	*<Report Findings Here>*
1B-1 Employ device management at initial key-loading facility and pre-use until placed into service, and for any POI devices returned to the key-management facility, or the vendor or their agent, for repair or other disposition.	
1B-1.1 POIs and other SCDs must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorized modifications or tampering prior to the loading of cryptographic keys.	
1B-1.1.a Review documented procedures to confirm that processes are defined to provide the following assurances prior to the loading of cryptographic keys: • POIs have not been substituted or subjected to unauthorized modifications or tampering. • SCDs used for key injection/loading or signing have not been substituted or subjected to unauthorized modifications or tampering.	*<Report Findings Here>*
1B-1.1.b Observe processes and interview personnel to verify that processes are followed to provide the following assurances prior to the loading of cryptographic keys: • POIs have not been substituted or subjected to unauthorized modifications or tampering. • SCDs used for key injection/loading or signing have not been substituted or subjected to unauthorized modifications or tampering.	*<Report Findings Here>*
1B-1.1.1 Controls must be implemented to protect POIs and other SCDs from unauthorized access up to point of deployment. Controls must include the following:	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 1 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
1B-1.1.1.a Review documented procedures to verify controls are defined to protect POIs and other SCDs from unauthorized access up to point of deployment.	*<Report Findings Here>*
1B-1.1.1.b Verify that documented procedures include 1B-1.1.1.1 through 1B-1.1.1.3 below.	*<Report Findings Here>*
1B-1.1.1.1 Access to all POIs and other SCDs is documented, defined, logged, and controlled such that unauthorized individuals cannot access, modify, or substitute any device.	
1B-1.1.1.1.a Examine access-control documentation and device configurations to verify that access to all POIs and key injection/loading devices is defined and documented.	*<Report Findings Here>*
1B-1.1.1.1.b For a sample of POIs and other SCDs, observe authorized personnel accessing devices and examine access logs to verify that access to all POIs and other SCDs is logged.	*<Report Findings Here>*
1B-1.1.1.1.c Examine implemented access controls to verify that unauthorized individuals cannot access, modify, or substitute any POI or other SCD.	*<Report Findings Here>*
1B-1.1.1.2 POIs and other SCDs do not use default keys (such as keys that are pre-installed for testing purposes) or passwords.	
1B-1.1.1.2 Examine vendor documentation or other information sources to identify default keys (such as keys that are pre-installed for testing purposes), passwords, or data. Observe implemented processes and interview personnel to verify that default keys or passwords are not used.	*<Report Findings Here>*
1B-1.1.1.3 All personnel with access to POIs and other SCDs are documented in a formal list and authorized by management.	
1B-1.1.1.3.a Examine documented authorizations to verify: • All personnel with access to POIs and other SCDs are documented in a formal list • All personnel with access to POIs and other SCDs are authorized by management.	*<Report Findings Here>*
1B-1.1.1.3.b For a sample of POIs and other SCDs, examine implemented access controls to verify that only personnel documented and authorized in the formal list have access to devices.	*<Report Findings Here>*
1B-1.2 Protect SCDs from unauthorized access, modification, or substitution, from receipt through to installation and use.	
1B-1.2.1 A documented "chain-of-custody" process must be in place to ensure that all POIs and other SCDs are controlled from receipt through to installation and use. The chain of custody must include records to identify personnel responsible for each interaction with the devices.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 1 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
1B-1.2.1.a Examine documented procedures to verify that a chain-of-custody process is required for all POIs and other SCDs from receipt through to installation and use.	*<Report Findings Here>*
1B-1.2.1.b For a sample of POIs and other SCDs, review documented records and interview responsible personnel to verify that chain of custody is maintained from receipt through to installation and use for: All POIs All devices used for key injection/loading or signing	*<Report Findings Here>*
1B-1.2.1.c Verify the chain-of-custody records identify personnel responsible for each interaction with the devices.	*<Report Findings Here>*
1B-1.2.2 Controls, including the following, must be in place to ensure that all installed devices are from a legitimate source:	
1B-1.2.2.a Examine documented purchasing, receipt, and deployment procedures to confirm that controls are defined for ensuring that all received devices are from a legitimate source.	*<Report Findings Here>*
1B-1.2.2.b Confirm that the documented procedures include 1B-1.2.2.1 through 1B-1.2.2.2 below.	*<Report Findings Here>*
1B-1.2.2.1 Device serial numbers must be compared to the serial numbers documented by the sender to ensure device substitution has not occurred. A record of device serial-number validations must be maintained. ***Note:*** *Examples of how serial numbers may be documented by the sender include but are not limited to: purchase order, shipping waybill, manufacturer's invoice, or similar document.*	
1B-1.2.2.1.a Interview responsible personnel to verify that device serial numbers are compared to the serial number documented by the sender for all POIs and other SCDs.	*<Report Findings Here>*
1B-1.2.2.1.b For a sample of received POIs and other SCDs, observe records of serial-number validations to verify: • Device serial numbers for the received device were verified to match that documented by the sender. • Records of serial-number verifications are maintained.	*<Report Findings Here>*
1B-1.2.2.2 Documentation used for validating device serial numbers must be received via a separate communication channel and must not have arrived with the device shipment.	
1B-1.2.2.2 For a sample of received POIs and other SCDs, review delivery records and interview responsible personnel to verify that documentation used to validate the device serial numbers was received via a separate communication channel than the device and was not received in the same shipment as the device.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 1 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
1B-1.3 Dual-control mechanisms must exist to help prevent substitution of POIs and other SCDs. This applies to both in-service and spare or backup devices. ***Note:*** *Procedural controls, which may be a combination of physical barriers and logical controls, may exist to support the prevention and detection of substituted cryptographic devices, but cannot supplant the implementation of dual-control mechanisms.*	
1B-1.3.a Examine documented procedures to verify that dual-control mechanisms are defined to: • Prevent substitution of POIs, both in-service and spare or backup devices. • Prevent substitution of SCDs, both in-service and spare or backup devices.	*<Report Findings Here>*
1B-1.3.b Examine dual-control mechanisms in use to verify that the mechanisms: • Prevent substitution of POIs, both in-service and spare or backup devices. • Prevent substitution of key injection/loading devices, both in-service and spare or backup devices.	*<Report Findings Here>*
1B-1.4 Implement physical protection of POIs and other SCDs from the manufacturer's facility up to the point of key-insertion or inspection, through one or more of the following. • Transportation using a trusted courier service (for example, via bonded carrier). The devices are then securely stored until key-insertion occurs. • Use of physically secure and trackable packaging (for example, pre-serialized, counterfeit-resistant, tamper-evident packaging). The devices are then stored in such packaging, or in secure storage, until key-insertion occurs. • A secret, device-unique "transport-protection token" is loaded into the secure storage area of each SCD at the manufacturer's facility. Before key-insertion, the SCD used for key-insertion verifies the presence of the correct "transport-protection token" before overwriting this value with the initial key.	
1B-1.4.a Examine documented procedures to verify they require physical protection of POIs and other SCDs, from the manufacturer's facility up to the point of key-insertion or inspection, through one or more of the defined methods.	*<Report Findings Here>*
1B-1.4.b Interview responsible personnel to verify that one or more of the defined methods are in place to provide physical device protection for POIs and other SCDs, from the manufacturer's facility up to the point of key-insertion.	*<Report Findings Here>*
1B-1.4.c For a sample of received POIs and other SCDs, observe processes and physical protections in use (for example, storage locations, packaging, device configurations), to verify that the defined methods are implemented for POIs and other SCDs, up to the point of key-insertion.	*<Report Findings Here>*
1B-1.5 Inspect and test all POIs and other SCDs immediately prior to key-insertion to ensure that devices are legitimate and have not been subject to any unauthorized modifications. Procedures must include the following:	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 1 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
1B-1.5.a Examine documented procedures to verify they require inspection and testing of POIs and other SCDs immediately prior to key-insertion, to ensure that devices are legitimate and have not been subject to any unauthorized modifications.	*<Report Findings Here>*
1B-1.5.b Verify documented procedures include 1B-1.5.1 through 1B-1.5.4 below.	*<Report Findings Here>*
1B-1.5.1 Running self-tests to ensure the correct operation of the device.	
1B-1.5.1 Examine records of device inspections and tests, and observe tests in progress to verify that self-tests are run on POIs and other SCDs to ensure the correct operation of the device.	*<Report Findings Here>*
1B-1.5.2 Installing (or re-installing) devices only after confirming that the device has not been tampered with or compromised.	
1B-1.5.2 Observe inspection processes and interview responsible personnel to verify that devices are installed, or reinstalled, only after confirming that the device has not been tampered with or compromised.	*<Report Findings Here>*
1B-1.5.3 Physical and/or functional tests and visual inspection to confirm that physical and logical controls and anti-tamper mechanisms are not modified or removed.	
1B-1.5.3 Observe inspection processes and interview responsible personnel to confirm processes include physical and/or functional tests and visual inspection to verify that physical and logical controls and anti-tamper mechanisms are not modified or removed.	*<Report Findings Here>*
1B-1.5.4 Maintaining records of the tests and inspections, and retaining records for at least one year.	
1B-1.5.4.a Examine records of inspections and interview responsible personnel to verify records of the tests and inspections are maintained.	*<Report Findings Here>*
1B-1.5.4.b Examine records of inspections to verify records are retained for at least one year.	*<Report Findings Here>*
1B-1.6 Maintain inventory-control and monitoring procedures to accurately track device locations from receipt of the device until ready to ship. The inventory-control and monitoring procedures must provide for the following:	
1B-1.6.a Examine documented inventory-control and monitoring procedures to confirm they define methods for tracking device locations from receipt until the device is ready to ship.	*<Report Findings Here>*
1B-1.6.b Verify documented procedures include 1B-1.6.1 through 1B-1.6.3 below.	*<Report Findings Here>*
1B-1.6.c For a sample of devices, review the documented device inventory and observe device locations to verify that the inventory-control and monitoring procedures accurately track device locations.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 1 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
1B-1.6.1 As soon as possible upon receipt and no later than key loading, the device serial number is entered into the inventory-control system.	
1B-1.6.1 Review documented device inventories and interview personnel to verify that devices are entered into the inventory-control system as soon as possible after receipt of the device, and no later than key loading.	*<Report Findings Here>*
1B-1.6.2 Devices are protected against unauthorized substitution or modification until all applicable keys have been loaded. ***Note**: This includes any cryptographic keys needed for the operation of the device and any keys used to encrypt account data.*	
1B-1.6.2 Review implemented controls and interview personnel to verify that devices are protected against unauthorized substitution or modification until all applicable keys have been loaded.	*<Report Findings Here>*
1B-1.6.3 Control and monitoring procedures must provide for detection of lost or stolen equipment and notification to authorized personnel.	
1B-1.6.3 Review implemented controls and interview personnel to verify that procedures are implemented to detect lost or stolen devices and notify authorized personnel.	*<Report Findings Here>*
1B-1.7 When the POI is shipped from the key-loading facility to the initial point of use (or an intermediary facility), procedures are implemented to ensure that the device is tracked and that it arrives unaltered at its destination.	
1B-1.7 Examine documented procedures, interview responsible personnel, and observe processes for shipping POI devices to verify that the following are in place: • Controls to ensure that device location is known and tracked throughout the entire shipping process • Controls to ensure devices arrive unaltered	*<Report Findings Here>*
1B-1.7.1 If POI devices are stored en route, processes must be in place to account for the location of every device at any point in time.	
1B-1.7.1 Examine device shipping procedures and records, and interview personnel to determine if POI devices are stored en route. If devices are stored en route, examine device shipping records for a sample of POIs and interview personnel to verify processes are in place to account for the location of every device at any point in time.	*<Report Findings Here>*
1B-1.7.2 Documented procedures are in place and implemented to transfer accountability for POI devices from the key-loading facility.	
1B-1.7.2 For a sample of POI devices, examine device shipping records and interview personnel to verify accountability for the device is formally transferred from the key-loading facility to the destination.	*<Report Findings Here>*
1B-2 Procedures must be in place and implemented to protect any SCDs, and ensure the destruction of any cryptographic keys or key material within such devices, when removed from service, retired at the end of the deployment lifecycle, or returned for repair.	
1B-2.1 Procedures are in place to ensure that any SCDs to be removed from service, retired, or returned for repair are not intercepted or used in an unauthorized manner, as follows:	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 1 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
1B-2.1.a Examine documented procedures to verify that procedures are defined for any SCDs to be removed from service, retired, or returned for repair.	*<Report Findings Here>*
1B-2.1.b Verify documented procedures include 1B-2.1.1 through1B-2.1.5 below.	*<Report Findings Here>*
1B-2.1.1 Affected entities are notified before devices are returned.	
1B-2.1.1 Interview responsible personnel and examine device-return records to verify that affected entities are notified before devices are returned.	*<Report Findings Here>*
1B-2.1.2 Devices are transported via trusted carrier service—for example, bonded carrier.	
1B-2.1.2 Interview responsible personnel and examine device-return records to verify that devices are transported via trusted carrier service—for example, bonded carrier.	*<Report Findings Here>*
1B-2.1.3 Devices are shipped in serialized, counterfeit-resistant, and tamper-evident packaging.	
1B-2.1.3 Interview responsible personnel and observe device-return processes and packaging to verify that devices are shipped in serialized, counterfeit-resistant, and tamper-evident packaging.	*<Report Findings Here>*
1B-2.1.4 Devices are tracked during the return process.	
1B-2.1.4 Interview responsible personnel and examine device-return records to verify that devices are tracked during the return process	*<Report Findings Here>*
1B-2.1.5 Once received, devices remain in their packaging (as defined in 1B-2.1.3) until ready for repair or destruction.	
1B-2.1.5 Interview responsible personnel and observe device-return processes to verify that once received, devices remain in their packaging (defined in 1B-2.1.3) until ready for destruction.	*<Report Findings Here>*
1B-2.2 When SCDs are removed from service, permanently or for repair, all keys and key material, and all account data stored within the device must be rendered irrecoverable. Processes must include the following: ***Note:*** *Without proactive key-removal processes, devices removed from service can retain cryptographic keys in battery-backed RAM for days or weeks. Likewise, host/hardware security modules (HSMs) can also retain keys—and more critically, the master file key—resident within these devices. Proactive key-removal procedures must be in place to delete all such keys from any SCD being removed from the network.*	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 1 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
1B-2.2 Verify that documented procedures for removing SCDs from service include the following: • Procedures require that all keys and key material, and all account data stored within the device be securely destroyed. • Procedures cover all devices removed from service permanently or for repair. • Procedures include 1B-2.2.1 through 1B-2.2.4 below.	*<Report Findings Here>*
1B-2.2.1 Dual control is implemented for all critical decommissioning processes.	
1B-2.2.1 Interview personnel and observe processes for removing SCDs from service to verify that dual control is implemented for all critical decommissioning processes.	*<Report Findings Here>*
1B-2.2.2 Key and data storage (including account data) are rendered irrecoverable (for example, zeroized). If data cannot be rendered irrecoverable, devices must be physically destroyed to prevent the disclosure of any sensitive data or keys.	
1B-2.2.2 Interview personnel and observe processes for removing SCDs from service to verify that all key and data storage (including account data) is rendered irrecoverable (for example, zeroized), or that devices are physically destroyed to prevent the disclosure of any sensitive data or keys.	*<Report Findings Here>*
1B-2.2.3 SCDs being decommissioned are tested and inspected to ensure keys and account data have been rendered irrecoverable.	
1B-2.2.3 Interview personnel and observe processes for removing SCDs from service to verify that tests and inspections of devices are performed to confirm that keys and account data have been rendered irrecoverable.	*<Report Findings Here>*
1B-2.2.4 Records of the tests and inspections (as required in 1B-2.2.3) are maintained for at least one year.	
1B-2.2.4 Interview personnel and observe records to verify that records of the tests and inspections (as required in 1B-2.2.43) are maintained for at least one year.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 1 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
1B-3 Any SCD capable of generating or loading cryptographic keys, encrypting keys, or signing applications to be loaded onto a POI device, is protected against unauthorized use. *This requirement applies to HSMs, key-injection/loading devices (KLDs) and any other devices used to generate or load keys or to sign applications or whitelists for loading onto POIs.*	
1B-3.1 For HSMs and other SCDs used for the generation or loading of cryptographic keys for use in POI devices, or for signing applications and/or whitelists to be loaded into a POI device, procedures must be documented and implemented to protect against unauthorized access and use. Required procedures and processes include the following:	
1B-3.1.a Examine documented procedures to confirm that they specify protection against unauthorized access and use for HSMs and other devices used for the generation or loading of cryptographic keys for use in POI devices, or for signing applications and/or whitelists to be loaded into a POI device.	*<Report Findings Here>*
1B-3.1.b Verify that documented procedures include 1B-3.1.1 through 1B-3.1.4 below.	*<Report Findings Here>*
1B-3.1.1 Devices must not be authorized for use except under the dual control of at least two authorized people. ***Note:*** *Dual control consists of logical and/or physical characteristics. For example, dual control may be implemented for logical access via two individuals with two different passwords, or for physical access via a physical lock that requires two individuals each with a different high-security key.*	
1B-3.1.1 Observe dual-control mechanisms and device-authorization processes to confirm that logical and/or physical characteristics are in place that prevent the device being authorized for use except under the dual control of at least two authorized people.	*<Report Findings Here>*
1B-3.1.1.1 Passwords used for dual control must each be of at least five decimal digits (or an equivalent size).	
1B-3.1.1.1 Observe password policies and configuration settings to confirm that passwords used for dual control must be at least five decimal digits (or an equivalent size).	*<Report Findings Here>*
1B-3.1.2 Dual control must be implemented for the following: To enable any manual key-encryption functions and any key-encryption functions that occur outside of normal transaction processing; To enable application-signing functions; To place the device into a state that allows for the input or output of clear-text key components; For all access to key-loading devices (KLDs) and authenticated application-signing devices.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 1 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
1B-3.1.2 Examine dual-control mechanisms and observe authorized personnel performing the defined activities to confirm that dual control is implemented for the following: To enable any manual key-encryption functions, and any key-encryption functions that occur outside of normal transaction processing; To enable application-signing functions; To place the device into a state that allows for the input or output of clear-text key components; For all access to KLDs and authenticated application-signing devices.	*<Report Findings Here>*
1B-3.1.3 Devices must not use default passwords.	
1B-3.1.3.a Examine password policies and documented procedures to confirm default passwords must not be used for HSMs, KLDs, and other SCDs used to generate or load cryptographic keys, or to sign applications or whitelists.	*<Report Findings Here>*
1B-3.1.3.b Observe device configurations and interview device administrators to verify HSMs, KLDs and other SCDs used to generate or load cryptographic keys, or to sign applications or whitelists, do not use default passwords.	*<Report Findings Here>*
1B-3.1.4 To detect any unauthorized use, devices are at all times either: Locked in a secure cabinet and/or sealed in tamper-evident packaging, or Under the continuous supervision of at least two authorized people.	
1B-3.1.4.a Examine documented procedures to confirm that they require devices are either: Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or Under the continuous supervision of at least two authorized people at all times.	*<Report Findings Here>*
1B-3.1.4.b Interview responsible personnel and observe devices and processes to confirm that devices are either: Locked in a secure cabinet and/or sealed in tamper-evident packaging at all times, or Under the continuous supervision of at least two authorized people at all times.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 1 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
1B-4 Documented procedures exist and are demonstrably in use to ensure the security and integrity of SCDs placed into service, initialized, deployed, used, and decommissioned.	
1B-4.1 All affected parties are aware of required processes and provided suitable guidance on the secure procedures for devices placed into service, initialized, deployed, used, and decommissioned.	
1B-4.1 Examine documented procedures/processes and interview responsible personnel to verify that all affected parties are aware of required processes and are provided suitable guidance on procedures for devices placed into service, initialized, deployed, used, and decommissioned.	*<Report Findings Here>*
1B-4.2 Procedures that govern access to SCDs, including HSMs, key-injection/loading devices (KLDs), and any other devices used to generate or load keys or sign applications for loading onto POIs, must be documented, implemented, and known to data-center personnel and any others involved with the physical security of such devices. HSM protections must include at least the following:	
1B-4.2.a Examine documented procedures to verify that procedures are defined that govern access to all SCDs.	*<Report Findings Here>*
1B-4.2.b Verify that procedures governing access to HSMs include at least those defined in Requirements 1B-4.2.1 – 1B-4.2.4 below.	*<Report Findings Here>*
1B-4.2.c Interview data-center personnel and others responsible for the physical security of the devices to verify that the documented procedures are known.	*<Report Findings Here>*
1B-4.2.1 Any physical keys needed to activate the HSM are stored securely.	
1B-4.2.1 Interview responsible personnel and observe key-storage locations and security controls to verify that any physical keys needed to activate the HSM are stored securely.	*<Report Findings Here>*
1B-4.2.2 If multiple physical keys are needed to activate the HSM: They are assigned to separate designated custodians, and Copies of individual keys are separated and stored such that two authorized individuals are required to gain access to these keys.	
1B-4.2.2 If multiple physical keys are needed to activate the HSM, interview responsible personnel and observe key operations to verify that: Keys are assigned to separate designated custodians, and Copies of individual keys are separated and stored such that two authorized individuals are required to gain access to these keys	*<Report Findings Here>*
1B-4.2.3 Anti-tamper sensors are enabled as required by the security policy of the HSM.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 1 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
1B-4.2.3 Examine HSM security policy and HSM anti-tamper controls to verify that anti-tamper sensors are enabled as required by the security policy of the HSM.	*<Report Findings Here>*
1B-4.2.4 When HSMs are connected to online systems, they are not enabled in a sensitive state. ***Note:*** *A "sensitive state" allows an HSM to perform privileged or sensitive functions that are not available during routine HSM operations. Examples of sensitive functions include but are not limited to: loading of key components, outputting clear-text key components, and altering HSM configuration.*	
1B-4.2.4 Examine HSM configurations and observe processes to verify that HSMs are not enabled in a sensitive state when connected to online systems.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

Domain 2: Application Security – Solution Provider Findings

Table 2.1 – List of POI Applications with access to clear-text account data *(All Domain 2 Requirements apply.)*				
Application Name	Application version #	Application vendor name	Brief description of application function/purpose	POI device type name/identifier application is installed on

Table 2.2 – List of POI Applications with <u>NO ACCESS</u> to clear-text account data *(Domain 2 Requirements 2A-3 apply.)*				
Application Name	Application version #	Application vendor name	Brief description of application function/purpose	POI device type name/identifier application is installed on

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 2 Requirements and Solution Provider Testing Procedures	P2PE Assessor Findings from Solution Provider 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 For all devices on which the application will be used in the solution, observe application and device operations as implemented in the solution (that is, all applications are installed on the device), and perform test transactions that simulate all functions of the application. Examine device-storage locations and device logs to verify that 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 For all devices on which the application will be used in the solution, observe application and device operations as implemented in the solution (that is, all applications are installed on the device), and perform test transactions that simulate all functions of the application. Examine device-storage locations and device logs to verify that all stored PAN and SAD are rendered irrecoverable.	*<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 For all devices on which the application will be used in the solution, observe application and device operations as implemented in the solution (that is, all applications are installed on the device), and perform test transactions that simulate all functions of the application. Examine device-storage locations and device logs to verify that the application does not output clear-text account data outside of the device.	*<Report Findings Here>*
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 solution provider's documentation that shows all applications, data flows, interactions, etc., within POI devices to verify that all internal communication and authentication methods are documented in accordance with the application's *Implementation Guide*.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 2 Requirements and Solution Provider Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
2A-2.2.b For all devices on which the application will be used in the solution, observe application and device operations as implemented in the solution (that is, all applications are installed on the device), and perform test transactions that simulate all functions of the application. Examine the dataflow during transactions to verify that the application only uses inter-process communication methods approved as part of the PCI-approved POI device evaluation.	*<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 solution provider's documentation that shows all applications, data flows, interactions, etc., within POI device to verify that all external communication methods are documented and in accordance with the application's *Implementation Guide*.	*<Report Findings Here>*
2A-2.3.b For all devices on which the application will be used in the solution, observe application and device operations as implemented in the solution (that is, all applications are installed on the device), and perform test transactions that simulate all functions of the application. Examine communication methods to verify that the application does not use any communication methods that were not approved as part of the PCI-approved POI device evaluation.	*<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").*	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 2 Requirements and Solution Provider Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
2A-2.4.a Interview solution-provider personnel and review documented procedures to verify that any application functions that output clear-text card data are implemented as follows: • Only non-PCI payment brand accounts/cards are output in clear-text from such application functions • Cryptographic authentication between the device and the application functions are established in accordance with device vendor's security guidance. • Only authorized personnel are allowed to initiate cryptographic authentication to sign or add application functions for output of clear-text data. • Records are maintained of any changes/additions, including description and justification for the function added, who authorized it, and confirmation that it was reviewed to only output non-PCI payment accounts/cards.	*<Report Findings Here>*
2A-2.4.b For all devices on which the application will be used in the solution, observe application and device operations as implemented in the solution (that is, all applications are installed on the device), and perform test transactions that simulate all functions of the application. Examine device output sources to verify the application meets the following: • Only outputs clear-text data for non-PCI payment brand accounts/cards. • Cryptographic authentication is correctly established for any application functions, using the PCI-approved POI device's firmware for cryptographic authentication.	*<Report Findings Here>*
2A-2.4.c Review records of changes/additions, and confirm that all changes/additions to application functions are documented, and that the documentation includes description and justification for the function added, who authorized it, and confirmation that it was reviewed to only output non-PCI payment accounts/cards.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 2 Requirements and Solution Provider Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
2A-3 All applications without a business need do not have access to account data. ***Note:*** *Requirements at 2A-3 are the only requirements applicable to applications on PCI-approved POI devices with no access to account data (for example, a loyalty or advertising application).*	
2A-3.1 Applications on the device that do not have a business need to access account data must only communicate with the device via application program interfaces (APIs) provided by the SRED firmware that do not provide access to account data.	
2A-3.1.a Examine the POI device vendor's security guidance to identify which APIs are intended for use by applications that do not need access to account data. Review the solution provider's documented processes, and confirm the following is included: • A list of all APIs and their functions, including which give access to account data and which do not • Confirmation that the function of each API in the solution provider's documentation matches the POI device vendor's security guidance • A list of all applications and which APIs each use • Documented business need for all applications on the device with access to account data • Confirmation that any applications without a business need for access to account data only use those APIs that do not give access to account data	*<Report Findings Here>*
2A-3.1.b Interview solution-provider personnel and observe device operations to verify that that any applications that do not have a need to access clear-text account data only use the APIs specified in the POI device vendor's security guidance that do not provide access to clear-text account data.	*<Report Findings Here>*
2A-3.2 All applications on the device that do not have a business need to access account data are authenticated with an approved security protocol of the POI.	
2A-3.2.a Review the solution provider's documented processes to confirm that applications with no need to see clear-text data must be authenticated using an approved security protocol of the POI.	*<Report Findings Here>*
2A-3.2.b Interview solution-provider personnel and observe device operations to verify that applications with no need to access clear-text account data are authenticated to the device using an approved security protocol.	*<Report Findings Here>*
2A-3.3 For applications that do not need access to account data, dual control is required for the application-signing process.	
2A-3.3.a Review the solution provider's documented processes to confirm that dual control is required to authenticate applications with no need to see clear-text data.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 2 Requirements and Solution Provider Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
2A-3.3.b Interview solution-provider personnel and observe an application update to confirm that application-signing is done under dual control.	*<Report Findings Here>*
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 Review the solution provider's documented processes, and confirm they follow any guidance specified in the *Implementation Guide* related to configuring the application on the device.	*<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 Review the solution provider's documented processes and interview solution-provider personnel, and confirm the following processes are in place: • Changes to application "whitelists" are reviewed prior to release and after any significant change to confirm that they will not result in the exposure of PCI payment-brand accounts/cards. • Changes to application "whitelists" are reviewed for any potential vulnerabilities or security flaws, using manual or automated vulnerability-assessment processes. • Found vulnerabilities are corrected and updated for applications in the field (installed on devices) after vulnerabilities are found, when the application vendor provides an update, or when the software vendor notifies the solution provider of a vulnerability that the solution provider needs to address.	*<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 For all devices on which the application will be used in the solution, observe application and device operations as implemented in the solution (that is, all applications are installed on the device), and perform test transactions that simulate all functions of the application. Examine device output sources to verify that any changes to "whitelists" do not result in the exposure of PCI payment-brand accounts/cards.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 2 Requirements and Solution Provider Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
2B-1.3 Develop applications based on secure coding guidelines. Cover prevention of common coding vulnerabilities in software development processes.	
2B-1.3 For all devices on which the application will be used in the solution, observe application and device operations as implemented in the solution (that is, all applications are installed on the device). Verify that the device and applications are not vulnerable to common 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 Review the solution provider's documented processes for implementing changes to applications, and interview solution-provider personnel, and confirm the following processes are in place: • Guidance in the *Implementation Guide* is followed. • Any changes to applications include documented approval by appropriate authorized solution-provider personnel. • Any changes to applications are documented as to reason and impact of the change.	*<Report Findings Here>*
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 Interview solution-provider personnel to determine that they have used only the approved IP stack, and that they have implemented the application in accordance with the *Implementation Guide.*	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 2 Requirements and Solution Provider Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
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	
2B-2.1.1 Interview solution-provider personnel to determine that they have used only the approved IP stack, and that they have implemented the application in accordance with the *Implementation Guide.*	*<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 solution provider's documentation to confirm that any shared resources they integrated into the application meet the following: • That any guidance from the *Implementation Guide* is included • Shared resources are identified and documented • Instructions for how the application should be configured to ensure secure integration with shared resources (where the integration has been done by the solution provider).	*<Report Findings Here>*
2B-2.2.b Interview solution-provider personnel to determine that they have integrated any shared resources in accordance with the *Implementation Guide.*	*<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-3.1.1 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.)*	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 2 Requirements and Solution Provider Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
2B-3.1.1.a Review the solution provider's documentation and confirm their documented processes include application developer key-management security guidance.	*<Report Findings Here>*
2B-3.1.1.b Interview solution-provider personnel to confirm that they follow key-management security guidance in accordance with the *Implementation Guide*	*<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 Interview solution-provider personnel and observe implementation processes to confirm that the application is installed in accordance with the *Implementation Guide.*	*<Report Findings Here>*
2C-1 New vulnerabilities are discovered and applications are tested for those vulnerabilities on an ongoing basis.	
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 for deploying application security upgrades, and verify they include deployment of critical security updates within 30 days of receipt from the software vendor.	*<Report Findings Here>*
2C-1.2.b Interview responsible solution-provider personnel to confirm that critical application security updates are deployed within 30 days of receipt from the software vendor.	*<Report Findings Here>*
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.a Review the solution provider's documentation and confirm their documented processes include using the guidance in the application's *Implementation Guide* for any application installations and updates.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 2 Requirements and Solution Provider Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
2C-2.1.1.b Interview responsible personnel and observe installation and update processes to confirm that installations and updates are only done using an approved security protocol.	*<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 Confirm the following through interview with solution provider and by observing an application update: • Application-signing processes specified in the Implementation Guide are followed. • Updates to applications are signed. • Application-signing is done under dual control.	*<Report Findings Here>*
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 Confirm that the solution provider has a current copy of the *Implementation Guide*.	*<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 Interview solution-provider personnel to confirm they have read a current copy of the *Implementation Guide* and are familiar with the contents and instructions therein.	*<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 Confirm the following via interviews with solution-provider personnel: • The solution provider receives periodic updates of the *Implementation Guide* from the software vendor. • The solution provider has distributed the Implementation Guide to any outsourced integrators/resellers they use for their P2PE solution.	*<Report Findings Here>*
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*.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 2 Requirements and Solution Provider Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
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 For the training materials provided by the software vendor for integrators/resellers, confirm the following via interviews with solution-provider personnel: • The solution provider has read and understands the training material. • The solution provider has distributed the training material to any outsourced integrators/resellers they use for their P2PE solution.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

Domain 3: Encryption Environment

Domain 3 applies to all POI device types identified in Table 1.1.

Table 3.1 – **Samples of POI Devices assessed for Domain 3 Testing Procedures** ***Note:*** *Every POI device type listed in Table 1.1 must be included in every Domain 3 sample set.*			
POI device type name/identifier (per Table 1.1)	**Sample Size** (Number of each device type assessed for Domain 3 Testing Procedures)	**Rationale** How sample size was determined to be appropriate and representative of the overall population	**Domain 3 Testing Procedures this sample was assessed against**
POI Sample Set #1 – Description (e.g., POIs awaiting deployment)			
POI Sample Set #2 – Description (e.g., POIs in storage)			
POI Sample Set #3 – Description (e.g., POIs …)			

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3A-1 Solution provider maintains inventory-control and monitoring procedures to accurately track POI devices in their possession, and provides related instructions to merchants.	
3A-1.1 Maintain inventory-control and monitoring procedures to identify and locate all POI devices, including where devices are: • Deployed • Awaiting deployment • Undergoing repair or otherwise not in use • In transit	
3A-1.1.a Examine documented inventory-control procedures to confirm the solution provider has defined methods to identify and locate all POI devices, including where devices are: • Deployed • Awaiting deployment • Undergoing repair or otherwise not in use • In transit	*<Report Findings Here>*
3A-1.1.b For a sample of devices, examine the documented device inventory and observe device locations to verify that the inventory-control and monitoring procedures identify and locate all POI devices.	*<Report Findings Here>*
3A-1.1.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to maintain inventory-control and monitoring procedures to identify and locate all devices, including where devices are: Deployed Awaiting deployment Undergoing repair or otherwise not in use In transit	
3A-1.1.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed procedures for merchants to maintain inventory-control and monitoring procedures to identify and locate all devices, including those where devices are: Deployed Awaiting deployment Undergoing repair or otherwise not in use In transit	*<Report Findings Here>*
3A-1.2 Perform POI device inventories at least annually to detect removal or substitution of devices.	
3A-1.2.a Examine documented procedures to verify device inventories are required to be performed at least annually to detect removal or substitution of devices.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3A-1.2.b Examine records of device inventories and interview personnel to verify that device inventories are performed at least annually.	*<Report Findings Here>*
3A-1.2.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to perform POI device inventories at least annually.	
3A-1.2.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes: Detailed procedures for merchants to perform device inventories to detect removal or substitution of devices Recommended frequency for performing device inventories, not to exceed annually	*<Report Findings Here>*
3A-1.3 Maintain a documented inventory of all POI devices to include at least the following: • Make, model of device • Location (site/facility, and/or identity of merchant) • Serial number • General description • Photograph of device that clearly shows device type and model (to assist with identification of different devices • Security seals, labels, hidden markings, etc. • Number and type of physical connections to device • Date of last inventory performed • Firmware version • Hardware version • Applications (including versions)	
3A-1.3.a Verify through observation that a documented inventory of all POI devices is maintained.	*<Report Findings Here>*
3A-1.3.b Verify the documented inventory includes at least the following: • Make, model of device • Location (site/facility, and/or identity of merchant) • Serial number • General description • Photograph of device that clearly shows device type and model (to assist with identification of different devices • Security seals, labels, hidden markings, etc. • Number and type of physical connections to device • Date of last inventory • Firmware version • Hardware version • Any applications (including versions)	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3A-1.3.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to maintain an inventory of all POI devices used for P2PE, to include at least those items described in 3A-1.3.	
3A-1.3.1.a Examine the *P2PE Instruction Manual (PIM)* to verify it includes procedures and guidance for merchants to maintain an inventory of POI devices.	*<Report Findings Here>*
3A-1.3.1.b Verify the instructions include maintaining at least the following details: Make, model of device Location (including site/facility, if applicable) Serial number General description Security seals, labels, hidden markings, etc. Number and type of physical connections to device Date of last inventory performed Firmware version Hardware version	*<Report Findings Here>*
3A-1.3.2 Secure the documented inventory of POI devices from unauthorized access.	
3A-1.3.2 Observe implemented controls and interview personnel to verify the documented inventory of devices is secured from unauthorized access.	*<Report Findings Here>*
3A-1.3.2.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to secure the documented inventory of POI devices from unauthorized access.	
3A-1.3.2.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes procedures and guidance for merchants to secure their documented inventory of devices from unauthorized access.	*<Report Findings Here>*
3A-1.4 Implement procedures for detecting and responding to variances in the annual inventory, including missing or substituted POI devices. Response procedures must include inclusion of any procedures defined by all applicable PCI payment brands, including timeframes for incident reporting, and providing a point of contact for merchants to report missing/substituted devices.	
3A-1.4.a Examine documented procedures to verify that procedures are defined for responding to variances in the annual inventory, including: • Procedures to detect missing or substituted devices • Procedures for responding to missing or substituted devices, including any procedures defined by all applicable PCI payment brands, including timeframes for incident reporting • A point of contact for reporting missing/substituted devices.	*<Report Findings Here>*
3A-1.4.b Interview personnel to verify that procedures for detecting and responding to variances in the annual inventory, including identification of missing or substituted devices, are implemented.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3A-1.4.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to detect and report variances in the annual inventory, including missing or substituted POI devices.	
3A-1.4.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes: Procedures for merchants to detect and report variances in the annual inventory, including missing or substituted device Point of contact for merchants to report missing or substituted devices	*<Report Findings Here>*
3A-2 Solution provider physically secures POI devices in their possession when not deployed or being used, and provides related instructions to merchants.	
3A-2.1 Physically secure the storage of POI devices awaiting deployment.	
3A-2.1.a Examine documented procedures to verify they include storing POI devices awaiting deployment in a physically secure location.	*<Report Findings Here>*
3A-2.1.b Inspect storage locations for POI devices awaiting deployment, to verify that the location is physically secure.	*<Report Findings Here>*
3A-2.1.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to physically secure the storage of POI devices awaiting deployment.	
3A-2.1.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes instructions for storing POI devices awaiting deployment in a physically secure location.	*<Report Findings Here>*
3A-2.2 Physically secure the storage of POI devices undergoing repair or otherwise not in use.	
3A-2.2.a Examine documented procedures to verify they include storing POI devices undergoing repair, or otherwise not in use, in a physically secure location.	*<Report Findings Here>*
3A-2.2.b Inspect storage locations for POI devices undergoing repair or otherwise not in use, to verify that the location is physically secure.	*<Report Findings Here>*
3A-2.2.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to physically secure the storage of POI devices undergoing repair or otherwise not in use	
3A-2.2.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes instructions for storing POI devices undergoing repair or otherwise not in use in a physically secure location.	*<Report Findings Here>*
3A-2.3 Physically secure the storage of POI devices awaiting transport between sites/locations.	
3A-2.3.a Examine documented procedures to verify they include storing POI devices awaiting transport between sites/locations in a physically secure location.	*<Report Findings Here>*
3A-2.3.b Inspect storage locations for decryption devices awaiting transport between sites/locations, to verify that the location is secure.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3A-2.3.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to physically secure the storage of POI devices awaiting transport between sites/locations.	
3A-2.3.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes instructions for storing POI devices awaiting transport between sites/locations in a physically secure location.	*<Report Findings Here>*
3A-2.4 Physically secure POI devices in transit, including: • Packing devices in tamper-evident packaging prior to transit. • Implementing procedures for determining whether device packaging has been tampered with. • Use of a defined secure transport method, such as bonded carrier or secure courier.	
3A-2.4.a Examine documented procedures for the transportation of POI devices and verify that procedures include the following: • Procedures for packing POI devices in tamper-evident packaging prior to transit • Procedures for determining whether device packaging has been tampered with • Procedures for using a defined secure transport method, such as bonded carrier or secure courier	*<Report Findings Here>*
3A-2.4.b For a sample of device shipments, examine records of device transportation and interview personnel to verify that the following procedures are implemented: • POI devices are packed in tamper-evident packaging prior to transit • Procedures are followed for determining whether device packaging has been tampered with • Use of a defined secure transport method, such as bonded carrier or secure courier	*<Report Findings Here>*
3A-2.4.1 Provide instructions to the merchant via the *P2PE Instruction Manual* for the merchant to physically secure POI devices in transit, to include at least those items described in 3A-2.4.	
3A-2.4.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed procedures for merchants to physically secure POI devices being transported, including: Procedures for packing the device using tamper-evident packaging prior to transit Procedures for inspecting device packaging to determine whether it has been tampered with, including specific details on how tamper-evidence may appear on the packaging used Defined secure transport method, such as bonded carrier or secure courier	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3A-2.4.2 Implement procedures to be followed upon determining that POI device packaging has been tampered with, including: Devices must not be deployed or used Procedures for returning device to authorized party for investigation Escalation procedures and contact details for reporting tamper-detection	
3A-2.4.2.a Examine documented procedures to verify they include procedures to be followed upon determining that device packaging has been tampered with, including: Devices must not be deployed or used Procedures for returning device to authorized party for investigation Contact details for reporting tamper-detection	*<Report Findings Here>*
3A-2.4.2.b Interview personnel to verify that, upon determining that device packaging has been tampered with, the following procedures are implemented: Devices are not deployed or used Procedures are followed for returning device to authorized party for investigation Reporting of tamper-detection to defined contact details	*<Report Findings Here>*
3A-2.4.3 Provide instructions via the *P2PE Instruction Manual* for the merchant to follow upon determining that POI device packaging has been tampered with, including: Devices must not be deployed or used Procedures for returning device to authorized party for investigation Contact details for reporting tamper-detection	
3A-2.4.3 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for merchant to follow upon determining that device packaging has been tampered with, including: Devices must not be deployed or used Procedures for returning device to authorized party for investigation Contact details for reporting tamper-detection	*<Report Findings Here>*
3A-2.5 Ensure POI devices are transported only between trusted sites/locations as follows: • A list of trusted sites (e.g., vendor / maintenance provider, etc.) is maintained. • Only devices received from trusted sites/locations are accepted for use. • Procedures are defined in the event that devices are received from untrusted or unknown locations, including: ○ Procedures (including contact details for authorized parties) for verifying location from which device was sent ○ Procedures to ensure devices are not used unless and until the source location is verified as trusted • Devices are sent only to trusted sites/locations.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3A-2.5.a Examine documented procedures to verify they include: • A list of trusted sites (e.g., vendor / maintenance provider, etc.) between which devices may be transported • Procedures to ensure that only devices received from trusted sites/locations are accepted for use • Procedures to be followed in the event that a device is received from an untrusted or unknown location, including: ○ Procedures (including contact details for authorized parties) for verifying location from which device was sent ○ Procedures to ensure devices are not used unless and until the source location is verified as trusted. • Procedures to ensure that devices are only sent to trusted sites/locations	*<Report Findings Here>*
3A-2.5.b For a sample of device shipments, examine records of device transportation and interview personnel to verify: • Only devices received from trusted sites/ locations are accepted for use. • Procedures are followed in the event that a device is received from an untrusted or unknown location, including: ○ Procedures (including contact details for authorized parties) for verifying location from which device was sent ○ Procedures to ensure devices are not used unless and until the source location is verified as trusted • Devices are only sent to trusted sites/locations	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3A-2.5.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to only transport POI devices between trusted sites/locations, as described in 3A-2.5.	
3A-2.5.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for transporting devices including: • A list of trusted sites (e.g., vendor / maintenance provider, etc.) from which devices may be accepted for use • Procedures to ensure that only devices received from trusted sites/locations are accepted for use • Procedures to be followed in the event that a device is received from an untrusted or unknown source location, including: ○ Procedures (including contact details for authorized parties) for verifying location from which device was sent ○ Procedures to ensure devices are not used unless and until the source location is verified as trusted • A list of trusted sites (e.g., vendor / maintenance provider, etc.) to which devices may be sent	*<Report Findings Here>*
3A-3 Solution provider has procedures to prevent and detect the unauthorized alteration or replacement of POI devices in their possession prior to and during deployment, and provides related instructions to merchants.	
3A-3.1 Implement procedures to prevent and detect unauthorized modification, substitution, or tampering of POI devices prior to use. Procedures must include the following:	
3A-3.1.1 Validate that serial numbers of received devices match sender records, and maintain records of serial-number verification. ***Note:*** *Examples of how serial numbers may be documented by the sender include but are not limited to: purchase order, shipping waybill, manufacturer's invoice, or similar document.*	
3A-3.1.1.a Examine documented procedures to verify they include: Procedures for comparing device serial numbers to the serial numbers documented by the sender Procedures for maintaining records of serial-number verifications	*<Report Findings Here>*
3A-3.1.1.b For a sample of received POIs, observe records of serial-number validations and interview personnel to verify: Device serial numbers for the received device were verified to match that documented by the sender. Records of serial-number verifications are maintained.	*<Report Findings Here>*
3A-3.1.2 Documentation used for validating device serial numbers must be received via a separate communication channel and must not have arrived with the device shipment.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3A-3.1.2.a Examine documented procedures to verify that documentation used for validating device serial numbers must be received via a separate communication channel and must not arrive with the device shipment	*<Report Findings Here>*
3A-3.1.2.b For a sample of received POIs, review delivery records and interview personnel to verify that documentation used to validate the device serial number was received via a separate communication channel than the device and was not received in the same shipment as the device.	*<Report Findings Here>*
3A-3.1.3 Perform pre-installation inspection procedures, including physical and functional tests and visual inspection, to confirm devices have not been tampered with or compromised.	
3A-3.1.3.a Examine documented procedures to verify that pre-installation inspection procedures are defined, including physical and functional tests and visual inspection, to confirm devices have not been tampered with or compromised.	*<Report Findings Here>*
3A-3.1.3.b Examine records of inspections, interview personnel performing device inspections and observe inspection process to confirm that POIs are subject to physical and functional tests as well as visual inspection prior to installation to confirm devices have not been tampered with or compromised.	*<Report Findings Here>*
3A-3.1.4 Maintain devices in original, tamper-evident packaging or store devices in a physically secured location, until ready for use.	
3A-3.1.4.a Examine documented procedures to verify they require devices be maintained in original, tamper-evident packaging or stored in a physically secured location, until ready for use.	*<Report Findings Here>*
3A-3.1.4.b Observe devices to verify they are maintained in original, tamper-evident packaging or stored in a physically secured location, until ready for use.	*<Report Findings Here>*
3A-3.1.5 Record device serial number in inventory-control system as soon as possible upon receipt and prior to installation	
3A-3.1.5.a Examine documented procedures to verify they require devices be entered into an inventory-control system as soon as possible upon receipt and prior to installation.	*<Report Findings Here>*
3A-3.1.5.b Review documented device inventories and interview responsible personnel to verity devices are entered into an inventory-control system as soon as possible after receipt of the device, and before installation.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3A-3.1.6 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures, including those items described in 3A-3.1.1 through 3A-3.1.5, to prevent and detect unauthorized alteration or replacement of POI devices prior to installation and use.	
3A-3.1.6 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for merchants to implement procedures for preventing and detecting unauthorized modification, substitution, or tampering of POI devices prior to installation and use, including: Procedures for matching device serial numbers to the serial numbers documented by the sender Procedures for maintaining records of serial-number verifications Defined method for transporting documents used for validating device serial numbers, via a separate communication channel and not with the device shipment Instructions for performing pre-installation inspection procedures, including physical and functional tests and visual inspection, to verify devices have not been tampered with or compromised Instructions for maintaining devices in original, tamper-evident packaging or in physically secure storage until ready for use Instructions for recording device serial numbers in merchant inventory-control system as soon as possible	*<Report Findings Here>*
3A-3.2 Implement procedures to control and document all physical access to devices prior to deployment. Procedures to include: • Identifying personnel authorized to access devices • Restricting access to authorized personnel • Maintaining a log of all access including personnel name, company, reason for access, time in and out. Retain access log for at least one year.	
3A-3.2.a Examine documented access procedures and verify they require controlling and documenting all physical access to devices, and include: • Identifying personnel authorized to access devices • Restricting access to authorized personnel • Maintaining a log of all access including personnel name, company, reason for access, time in and out • Retaining access logs for at least one year	*<Report Findings Here>*
3A-3.2.b Observe physical access controls to verify they include controlling and documenting all physical access to devices, and include: • Identifying personnel authorized to access devices • Restricting access to authorized personnel • Maintaining a log of all access including personnel name, company, reason for access, time in/out	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3A-3.2.c Examine access logs/records to verify it is retained for at least one year and contains, at a minimum, the following details: • Personnel name • Company • Reason for access • Time in and out	*<Report Findings Here>*
3A-3.2.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures to control and document all physical access to devices prior to deployment. Procedures to include those items described in 3A-3.2.	
3A-3.2.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for merchants to implement procedures for controlling and documenting all physical access to devices prior to deployment, including: Identifying personnel authorized to access devices Restricting access to authorized personnel Maintaining a log of all access including personnel name, company, reason for access, time in and out	*<Report Findings Here>*
3A-3.3 Implement a documented audit trail to demonstrate that devices are controlled, and are not left unprotected, at all times from receipt through to installation.	
3A-3.3.a Examine documented procedures to verify a documented audit trail must be maintained to demonstrate that devices are controlled, and not left unprotected, at all times from receipt through to installation.	*<Report Findings Here>*
3A-3.3.b Examine audit trail records to verify a documented audit trail is maintained and demonstrates that devices are controlled, and not left unprotected, at all times from receipt through to installation.	*<Report Findings Here>*
3A-3.3.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement an audit trail to demonstrate that a device is controlled, and not left unprotected, at all times from receipt through to installation	
3A-3.3.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for the merchant to maintain an audit trail to demonstrate that devices are controlled, and not left unprotected, at all times from receipt through to installation.	*<Report Findings Here>*
3A-4 Solution provider provides instructions to merchants to physically secure devices to prevent unauthorized access, modification, or substitution while devices are deployed for use. This includes both attended and unattended devices (for example, kiosks, "pay-at-the-pump," etc.).	
3A-4.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to select appropriate locations for deployed devices, for example: • Control public access to devices such that public access is limited to only parts of the device a person is expected to use to complete a transaction (for example, PIN pad and card reader). • Locate devices so they can be observed and/or monitored by authorized personnel (for example, during daily device checks performed by store/security staff). • Locate devices in an environment that deters compromise attempts (for example, through use of appropriate lighting, access paths, visible security measures, etc.)	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3A-4.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for the merchant to select appropriate locations for deployed devices, for example: • Controlling public access to devices such that public access is limited to only parts of the device a person is expected to use to complete a transaction (for example, PIN pad and card reader). • Locating devices so they can be observed and/or monitored by authorized personnel (for example, during daily store checks of the devices performed by store/security staff). • Locating devices in an environment that deters compromise attempts (for example, through lighting, access paths, visible security measures, etc.).	*<Report Findings Here>*
3A-4.2 Provide instructions via the *P2PE Instruction Manual* for the merchant to physically secure deployed devices to prevent unauthorized removal or substitution, including examples of how devices can be physically secured.	
3A-4.2 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for the merchant to physically secure deployed devices to prevent unauthorized removal or substitution, including specific examples of how devices can be physically secured.	*<Report Findings Here>*
3A-4.2.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures to prevent unauthorized removal or substitution of devices that cannot be physically secured (such as wireless or handheld devices). *For example, secure devices in a locked room when not in use, assign responsibility to specific individuals when in use, observe devices at all times, sign devices in/out, etc.*	
3A-4.2.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes instructions for the merchant to implement procedures to prevent unauthorized removal or substitution of devices that cannot be physically secured, such as wireless or handheld devices.	*<Report Findings Here>*
3A-5 Solution provider prevents unauthorized physical access to devices undergoing repair or maintenance while in their possession, and provides related instructions to merchants.	
3A-5.1 Implement procedures for identification and authorization of third-party personnel (including repair/maintenance personnel) prior to granting access. Procedures must include the following:	
3A-5.1.a Examine documented procedures to verify they include identification and authorization of third-party personnel prior to granting access.	*<Report Findings Here>*
3A-5.1.b Verify documented procedures include 3A-5.1.1 through 3A-5.1.5 below.	*<Report Findings Here>*
3A-5.1.1 Verify the identity and authorization of third-party personnel prior to granting access to devices.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3A-5.1.1 Interview responsible personnel and observe processes to confirm that the identity and authorization of third-party personnel is verified prior to granting access to devices.	*<Report Findings Here>*
3A-5.1.2 Unexpected personnel must be denied access until fully validated and authorized.	
3A-5.1.2 Interview responsible personnel and observe processes to verify that unexpected personnel are denied access until fully validated and authorized.	*<Report Findings Here>*
3A-5.1.3 Once authorized, third-party personnel must be escorted and monitored at all times.	
3A-5.1.3 Interview responsible personnel and observe processes to verify that, once authorized, third-party personnel are escorted and monitored at all times.	*<Report Findings Here>*
3A-5.1.4 A log of all third-party personnel access is maintained.	
3A-5.1.4 Examine access logs/records to verify that a log of all third-party personnel access is maintained in accordance with logging requirements defined in 3A-3.2.	*<Report Findings Here>*
3A-5.1.5 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures for identification and authorization of third-party personnel (including repair/maintenance personnel) prior to granting access. Procedures to include those items described in 3A-5.1.1 through 3A-5.1.4.	
3A-5.1.5 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for the merchant to implement procedures for identification and authorization of third-party personnel (including repair/maintenance personnel) prior to granting access, including: Procedures for verifying the identity and authorization of third-party personnel prior to granting access to devices Instructions that unexpected personnel must be denied access unless fully validated and authorized Escorting and monitoring authorized personnel at all times Maintaining a log of all third-party personnel access	*<Report Findings Here>*
3B-1 Solution provider securely maintains devices being returned, replaced, or disposed of, and provides related instructions to merchants.	
3B-1.1 Implement procedures to ensure that devices to be removed from service, retired, or returned for repair, are not intercepted and used in an unauthorized manner, as follows.	
3B-1.1.a Examine documented procedures to verify that procedures are defined for any devices to be removed from service, retired, or returned for repair.	*<Report Findings Here>*
3B-1.1.b Verify documented procedures include 3B-1.1.1 through 3B-1.1.5.	*<Report Findings Here>*
3B-1.1.1 Affected entities are notified before devices are returned.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-1.1.1 Interview responsible personnel and examine device-return records to verify that affected entities are notified before devices are returned.	*<Report Findings Here>*
3B-1.1.2 Devices are transported via trusted carrier service—for example, bonded carrier.	
3B-1.1.2 Interview responsible personnel and examine device-return records to verify that devices are transported via trusted carrier service—for example, bonded carrier.	*<Report Findings Here>*
3B-1.1.3 Devices are shipped in serialized, counterfeit-resistant, and tamper-evident packaging.	
3B-1.1.3 Interview responsible personnel and observe device-return processes and packaging to verify that devices are shipped in serialized, counterfeit-resistant, and tamper-evident packaging.	*<Report Findings Here>*
3B-1.1.4 Devices are tracked during the return process.	
3B-1.1.4 Interview responsible personnel and examine device-return records to verify that devices are tracked during the return process.	*<Report Findings Here>*
3B-1.1.5 Once received, devices remain in their packaging (as defined in 3B-1.1.3) until ready for repair or destruction.	
3B-1.1.5 Interview responsible personnel and examine device-return processes to verify that, once received, devices remain in their packaging (defined in 3B-1.1.3) until ready for repair or destruction.	*<Report Findings Here>*
3B-1.1.6 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures for securing devices being removed from service, retired, or returned for repair.	
3B-1.1.6 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed procedures for the merchant to secure devices being returned or replaced, including: Procedures and contact details for notifying affected entities—including the entity to which the device is being returned—before devices are returned Procedures for transporting devices via a trusted carrier service Procedures for packing and sending devices in serialized, counterfeit-resistant, and tamper-evident packaging Procedures to ensure the solution provider can track devices during the return process	*<Report Findings Here>*
3B-1.2 Implement procedures for secure disposal of devices, to include the following:	
3B-1.2 Examine documented procedures to verify procedures are defined for secure disposal of devices and include 3B-1.2.1 through 3B-1.2.2.	*<Report Findings Here>*
3B-1.2.1 Return devices to authorized parties for disposal.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-1.2.1 Interview responsible personnel and examine device-return processes to verify devices are returned only to authorized parties for disposal.	*<Report Findings Here>*
3B-1.2.2 Keys and data storage (including account data) must be rendered irrecoverable (for example, zeroized) prior to device disposal. If data cannot be rendered irrecoverable, the device must be physically destroyed to prevent the disclosure of any sensitive data or keys.	
3B-1.2.2 Interview personnel and observe processes for removing devices from service to verify that all key and data storage (including account data) is rendered irrecoverable (for example, zeroized) prior to disposal, or that devices are physically destroyed to prevent the disclosure of any sensitive data or keys.	*<Report Findings Here>*
3B-1.2.3 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures for the secure disposal of devices.	
3B-1.2.3 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for the merchant to implement procedures for the secure disposal of devices, including: Returning devices only to authorized parties for destruction (including a list of authorized parties) Procedures to render sensitive data irrecoverable, prior to device being shipped for disposal.	*<Report Findings Here>*
3B-2 Solution provider configures devices to fail closed if encryption mechanism fails, until either the P2PE encryption is restored or merchant opts out of using solution.	
3B-2.1 Upon failure of the encryption mechanism, the device must immediately fail closed and/or be immediately removed, shut down, or taken offline until the P2PE encryption is restored. ***Note:*** *Domain 5 requires that solution providers actively monitor traffic that is received into the decryption environment to confirm that the POI equipment in the merchant's encryption environment is not outputting clear-text CHD through some error or misconfiguration. Refer to 5D-2.*	
3B-2.1.a Review documented procedures and interview responsible personnel to verify that upon failure of the encryption mechanism, POI devices are configured to immediately fail closed, and/or be immediately removed, shut down, or taken offline.	*<Report Findings Here>*
3B-2.1.b Observe POI device configurations to verify that POI devices are configured to, upon failure of the encryption mechanism, immediately fail closed, and/or be immediately shut down or taken offline.	*<Report Findings Here>*
3B-2.1.c Observe devices during a simulated encryption failure to verify that devices immediately fail closed and/or are immediately removed/shut down/taken offline upon failure of the encryption mechanism.	*<Report Findings Here>*
3B-2.1.1 The device cannot be re-enabled until it is confirmed that either: The issue has been resolved and P2PE encryption functionality is restored and re-enabled, or The merchant has formally opted out from using the P2PE solution according to the solution provider's opt-out procedures (as defined in Requirement 3B-2.2), and has accepted responsibility for using alternative controls and/or processing method.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-2.1.1.a Examine documented procedures to verify the POI devices must not be re-enabled until it is confirmed that either: The issue has been resolved and P2PE encryption functionality is restored and re-enabled, or The merchant has formally opted out from using the P2PE solution according to the solution provider's opt-out procedures (as defined in Requirement 3B-2.2), and has accepted responsibility for using an alternative controls and/or processing method.	*<Report Findings Here>*
3B-2.1.1.b Verify the documented procedures include verifying that encryption functionality is restored before devices are re-enabled.	*<Report Findings Here>*
3B-2.1.1.c Interview responsible personnel and observe implemented processes to verify that: POI devices are not re-enabled until it is confirmed that either: The issue has been resolved and P2PE encryption functionality is restored and re-enabled, or The merchant has formally opted out from using the P2PE solution, according to the solution provider's opt-out procedures (as defined in Requirement 3B-2.2), and has accepted responsibility for using an alternative processing method. Encryption functionality is verified as being restored before devices are re-enabled.	*<Report Findings Here>*
3B-2.1.1.d Observe device configurations to verify devices are configured to remain closed until re-enabled by authorized personnel.	*<Report Findings Here>*
3B-2.1.2 The solution provider must maintain a record of all encryption failures, to include the following: Identification of affected device(s), including make, model, and serial number Identification of affected merchant, including specific sites/locations if applicable Date/time of encryption failure Date/time and duration of device downtime Date/time that encryption functionality was verified as being restored Details of whether any account data was transmitted from the P2PE POI device during the time that encryption was disabled	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-2.1.2.a Examine documented procedures to verify they require a record of all encryption failures to be maintained, including the following details: • Identification of affected device (s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicable • Date/time of encryption failure • Date/time and duration of device downtime • Date/time that encryption functionality was verified as being restored • Details of whether any account data was transmitted from the P2PE POI device during the time that encryption was disabled	*<Report Findings Here>*
3B-2.1.2.b Interview responsible personnel and observe implemented processes to verify that a record of all encryption failures is maintained, including the following details: • Identification of affected device (s), including make, model, and serial number • Identification of affected merchant, including specific sites/locations if applicableDate/time of encryption failure • Date/time and duration of device downtime • Date/time that encryption functionality was verified as being restored • Details of whether any account data was transmitted from the P2PE POI device during the time that encryption was disabled	*<Report Findings Here>*
3B-2.1.3 Provide instructions via the *P2PE Instruction Manual* for the merchant to follow in the event of a device encryption failure.	
3B-2.1.3 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed instructions for the merchant to follow in the event of a device encryption failure. Verify the detailed instructions include ensuring that devices are not re-enabled for use until merchant has confirmed with solution provider that either: The issue has been resolved and P2PE-encryption functionality is restored and re-enabled, or The merchant has formally opted out from using the P2PE solution according to the solution provider's opt-out procedures (as defined in Requirement 3B-2.2), and has accepted responsibility for using alternative controls and/or processing method.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-2.2 The solution provider must document and implement an opt-out process for merchants to follow in the event that, upon device encryption failure, the merchant chooses to opt out of the P2PE solution and process transactions without P2PE protection. The process must include the following:	
3B-2.2.a Examine documented procedures to verify the solution provider has a documented opt-out process for merchants to follow in the event that, upon device encryption failure, the merchant chooses to opt out of the P2PE solution and process transactions without P2PE protection.	*<Report Findings Here>*
3B-2.2.b Verify documented opt-out procedures include 3B-2.2.1 through 3B-2.2.4	*<Report Findings Here>*
3B-2.2.1 Defined method of communication for merchants to advise the solution provider that they wish to opt out of the P2PE solution.	
3B-2.2.1 Interview responsible personnel and observe processes to verify the defined method of communication is in place for merchants to advise the solution provider that they wish to opt out of the P2PE solution.	*<Report Findings Here>*
3B-2.2.2 Upon receipt of a merchant request to opt out of the P2PE solution, the solution provider must formally communicate to the merchant the procedures to be followed, and advise the merchant of the following: The security impact to the merchant's account data and potential risks associated with processing transactions without P2PE protection. The merchant is responsible for implementing alternative controls to protect account data in lieu of the P2PE solution (such as the applicable PCI DSS requirements for secure data transmission, network security, etc.). The merchant is no longer eligible for the PCI DSS scope reduction which was afforded by the P2PE solution. The merchant is obligated to advise their acquirer that they are no longer using the P2PE solution. Processing transactions without P2PE protection may impact the merchant's PCI DSS compliance validation, and the merchant should confirm with their acquirer or payment brand, as applicable, for all PCI payment brands affected. If the merchant wishes to opt out of the P2PE solution, the merchant must provide formal acknowledgment and acceptance of the above and formally request that transactions be accepted without P2PE encryption. A defined method of communication for the merchant to provide their acknowledgement and acceptance of the above.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-2.2.2 Interview responsible personnel and observe implemented processes and communications to verify that upon receipt of a merchant request to opt out of the P2PE solution, the solution provider formally communicates to the merchant the procedures to be followed, and advises the merchant of the following: The security impact to the merchant's account data and potential risks associated with processing transactions without P2PE protection. The merchant is responsible for implementing alternative controls to protect account data in lieu of the P2PE solution (such as the applicable PCI DSS requirements for secure data transmission, network security, etc.) The merchant is no longer eligible for the PCI DSS scope reduction which was afforded by the P2PE solution. The merchant is obligated to advise their acquirer that they are no longer using the P2PE solution. Processing transactions without P2PE protection may impact the merchant's PCI DSS compliance validation and the merchant should confirm with their acquirer or payment brand, as applicable, for all PCI payment brands affected. If the merchant wishes to opt out of the P2PE solution, the merchant must provide formal acknowledgment and acceptance of the above and formally request that transactions be accepted without P2PE encryption. A defined method of communication for the merchant to provide their acknowledgement and acceptance of the above.	*<Report Findings Here>*
3B-2.2.3 The process for merchants to acknowledge their acceptance of the opt-out conditions must include a mechanism for the solution provider to verify the authenticity of the acknowledgment, including: Verification that the acknowledgement originated from the merchant using the affected devices Verification that the acknowledgement was approved by merchant personnel authorized to make such an acknowledgement	
3B-2.2.3 Observe implemented processes and interview responsible personnel to confirm that the authenticity of the acknowledgment is verified, including: Verification that the acknowledgement originated from the merchant using the affected devices Verification that the acknowledgement was approved by merchant personnel authorized to make such an acknowledgement	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-2.2.4 The solution provider must maintain a record of all opt-out requests received, including the following: Identification of merchant submitting request Date initial request received Result of request (that is, the merchant chose to either accept the conditions and opt out of the solution, or chose to continue with the solution using P2PE devices) If merchant chose to accept the conditions and opt out of the solution: ○ Date formal acknowledgement received ○ Identification of device(s) in use by the merchant that are no longer covered by the P2PE solution	
3B-2.2.4 Observe implemented processes and interview responsible personnel to verify a record of all received opt-out requests is maintained and includes: Identification of merchant submitting request Date initial request received Result of request If merchant chose to accept the conditions and opt out of the solution: ○ Date formal acknowledgement received ○ Identification of device(s) in use by the merchant that are no longer covered by the P2PE solution	*<Report Findings Here>*
3B-2.3 Provide instructions via the *P2PE Instruction Manual*, including details of the opt-out process and instructions for the merchant to follow in the event that, upon device encryption failure, the merchant chooses to opt out of the P2PE solution and process transactions without P2PE protection.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-2.3 Examine the *P2PE Instruction Manual (PIM)* to verify it clearly describes the opt-out process and provides detailed instructions, including: • Procedures for the merchant to follow in the event that, upon device encryption failure, the merchant chooses to opt out of the P2PE solution and process transactions without P2PE protection. • The method of communication for merchants to advise the solution provider that they wish to opt out of the P2PE solution. • That if they choose to opt out, the merchant must formally acknowledge that they accept responsibility for the following: ○ The security impact to the merchant's account data and potential risks associated with processing transactions without P2PE protection. ○ Responsibility for implementing alternative controls to protect account data in lieu of the P2PE solution. ○ That the merchant is no longer eligible for the PCI DSS scope reduction afforded by the P2PE solution. ○ Advising their acquirer that they are no longer using the P2PE solution. ○ That processing transactions without P2PE protection may impact the merchant's PCI DSS compliance validation and the merchant should confirm with their acquirer or payment brand, as applicable, for all PCI payment brands affected. ○ Formal request that transactions be accepted without P2PE encryption. • The method of communication that will be used for the merchant to provide their formal acknowledgement and acceptance of the above.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-3 Solution provider restricts access to devices to authorized personnel.	
3B-3.1 Solution provider ensures merchant has no administrative access to the device and cannot change anything on the device that could impact the security settings of the device. Merchant access, if needed, must meet the following: • Be read-only. • Only view transaction-related data. • Cannot view or access encryption keys. • Cannot view or access full PAN. • Cannot view or access SAD. • Cannot view or access device configuration settings which could impact the security controls of the device, or allow access to encryption keys or clear-text PAN and/or SAD. • Cannot enable device interfaces or data-capture mechanisms that have been disabled by the solution provider.	
3B-3.1.a Examine documented device configuration procedures and account privilege assignments to verify that merchant accounts are defined to meet the following access requirements: • No administrative access to the device is allowed. • Cannot change anything on the device that could impact the security settings of the device. • Be read-only. • Only view transaction-related data. • Cannot view or access encryption keys. • Cannot view or access full PAN. • Cannot view or access SAD. • Cannot view or access device configuration settings which could impact the security controls of the device, or allow access to encryption keys or clear-text PAN and/or SAD. • Cannot enable device interfaces or data-capture mechanisms that have been disabled by the solution provider.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-3.1.b For a sample of all POI devices used in the solution, logon to the device using an authorized test merchant account. Verify that merchant-account access meets the following: • Be read-only. • Only view transaction-related data. • Cannot view or access encryption keys. • Cannot view or access full PAN. • Cannot view or access SAD. • Cannot view or access device configuration settings which could impact the security controls of the device, or allow access to encryption keys or clear-text PAN and/or SAD. • Cannot enable device interfaces or data-capture mechanisms that have been disabled by the solution provider.	*<Report Findings Here>*
3B-3.1.c Observe a sample of device configurations and interview responsible personnel to verify that the defined merchant-access requirements are configured for all devices used in the solution.	*<Report Findings Here>*
3B-3.2 All solution-provider personnel with access to POI devices are documented in a formal list and authorized by management. The list of authorized personnel is reviewed at least annually.	
3B-3.2.a Examine documented authorizations to verify: • All personnel with access to devices are documented in a formal list. • All personnel with access to devices are authorized by management. • The list of authorized personnel is reviewed at least annually.	*<Report Findings Here>*
3B-3.2.b For a sample of all POI devices used in the solution, examine account-access configurations to verify that only personnel documented and authorized in the formal list have access to devices.	*<Report Findings Here>*
3B-3.3 Access and permissions on devices are granted based on least privilege and need to know.	
3B-3.3.a Examine documented access-control policies and procedures to verify that access and permissions must be assigned according to least privilege and need to know.	*<Report Findings Here>*
3B-3.3.b For a sample of all POI devices and personnel, observe configured accounts and permissions, and interview responsible personnel to verify that the level of access and permission granted are according to least privilege and need to know.	*<Report Findings Here>*
3B-4 Solution provider provides features for secure remote access to devices deployed at merchant locations.	
3B-4.1 Solution provider's authorized personnel use two-factor or cryptographic authentication for all remote access to merchant POIs over a public network (Internet). ***Note:*** *If cryptographic authentication is used, the update or file must be cryptographically signed under dual control.*	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-4.1.a Examine documented procedures to verify that either two-factor or cryptographic authentication must be used for all remote access to POI devices.	*<Report Findings Here>*
3B-4.1.b Observe remote-access mechanisms and controls to verify that either two-factor or cryptographic authentication is configured for all remote access to POI devices.	*<Report Findings Here>*
3B-4.1.c Interview personnel and observe authorized remote connection to verify that either two-factor or cryptographic authentication is used for all remote access to POI devices.	*<Report Findings Here>*
3B-4.2 POIs must be configured to ensure that remote access is only permitted from the solution provider's authorized systems and only from the solution provider's secure decryption environment/network.	
3B-4.2.a Examine documented device-configuration procedures and interview personnel to verify that devices must be configured to permit remote access only from the solution provider's authorized systems, and only from the solution provider's secure decryption environment/network.	*<Report Findings Here>*
3B-4.2.b For all devices used in the solution, observe a sample of device configurations to verify that remote access is permitted only from the solution provider's authorized systems, and only from the solution provider's secure decryption environment/network.	*<Report Findings Here>*
3B-4.3 Merchants do not have remote access to the merchant POIs.	
3B-4.3.a Examine documented POI-configuration procedures and interview personnel to verify that devices must be configured to ensure merchants do not have remote access to the POIs.	*<Report Findings Here>*
3B-4.3.b For all devices used in the solution, observe a sample of device configurations to verify that merchants do not have remote access to the POIs.	*<Report Findings Here>*
3B-4.4 Solution provider implements secure identification and authentication procedures for access to devices deployed at merchant locations, including: ***Note:*** *This applies to non-console and console access.*	
3B-4.4.a Examine documented identification and authentication procedures to verify secure identification and authentication procedures are defined for remote access to devices deployed at merchant locations.	*<Report Findings Here>*
3B-4.4.b Verify documented procedures are defined for 3B-4.4.1 through 3B-4.4.3	*<Report Findings Here>*
3B-4.4.1 Authentication credentials for solution-provider personnel that are unique for each merchant site	
3B-4.4.1 Examine device configurations and authentication mechanisms to verify that solution-provider personnel have unique authentication credentials for each merchant site.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-4.4.2 Tracing all logical access to devices by solution-provider personnel to an individual user.	
3B-4.4.2.a Examine device configurations and authentication mechanisms to verify that all logical access to devices can be traced to an individual user.	*<Report Findings Here>*
3B-4.4.2.b Observe authorized logical accesses and examine access records/logs to verify that all logical access is traced to an individual user.	*<Report Findings Here>*
3B-4.4.3 Maintaining audit logs of all logical access to devices, and retaining access logs for at least one year.	
3B-4.4.3.a Observe authorized logical accesses and examine access records/logs to verify that an audit log of all logical access to devices is maintained.	*<Report Findings Here>*
3B-4.4.3.b Examine access records/logs to verify that access logs are retained for at least one year.	*<Report Findings Here>*
3B-5 The solution provider protects POI devices from known vulnerabilities and implements procedures for secure updates to devices.	
3B-5.1 Implement secure update processes for all firmware and software updates, including: • Integrity check of update • Authentication of origin of the update	
3B-5.1.a Examine documented procedures to verify secure update processes are defined for all firmware and software updates, and include: • Integrity checks of update • Authentication of origin of the update	*<Report Findings Here>*
3B-5.1.b Observe a sample of firmware and software updates, and interview personnel to verify: • The integrity of the update is checked • The origin of the update is authenticated	*<Report Findings Here>*
3B-5.2 Maintain an up-to-date inventory of POI system builds and conduct vulnerability assessments against all builds at least annually and upon any changes to the build.	
3B-5.2.a Examine documented procedures to verify they include: • Procedures for maintaining an up-to-date inventory of POI system builds • Procedures for conducting vulnerability assessments against all builds at least annually and upon any changes to the build	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-5.2.b Review documented inventory of devices (as required in 3A-1.3), and examine the inventory of system builds to verify: • The inventory includes all POI system builds. • The inventory of POI system builds is up-to-date.	*<Report Findings Here>*
3B-5.2.c Observe results of vulnerability assessments and interview responsible personnel to verify vulnerability assessments are performed against all POI builds: • At least annually and • Upon any changes to the build	*<Report Findings Here>*
3B-5.3 Develop and deploy patches and other device updates in a timely manner.	
3B-5.3.a Examine documented procedures to verify they include defined procedures for patches and other device updates to be developed and deployed in a timely manner.	*<Report Findings Here>*
3B-5.3.b Examine patch-deployment records and device logs, and interview responsible personnel to verify that patches and other device updates are developed and deployed in a timely manner.	*<Report Findings Here>*
3B-5.4 Deliver updates in a secure manner with a known chain-of-trust.	
3B-5.4.a Examine documented procedures for device updates to verify they include delivering updates in a secure manner with a known chain-of-trust.	*<Report Findings Here>*
3B-5.4.b Observe processes for delivering updates and interview responsible personnel to verify that updates are delivered in a secure manner with a known chain-of-trust.	*<Report Findings Here>*
3B-5.5 Maintain the integrity of patch and update code during delivery and deployment.	
3B-5.5.a Examine documented procedures for device updates to verify they define controls to maintain the integrity of all patch and update code during delivery and deployment.	*<Report Findings Here>*
3B-5.5.b Observe processes for delivering updates and interview responsible personnel to verify that the integrity of patch and update code is maintained during delivery and deployment.	*<Report Findings Here>*
3B-5.5.c Observe authorized personnel attempt to run the update process with arbitrary code to verify that the system will not allow the update to occur.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-6 Secure account data when troubleshooting	
3B-6.1 Securely delete any PAN or SAD used for debugging or troubleshooting purposes. These data sources must be collected in limited amounts and collected only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use.	
3B-6.1.a Examine the solution provider's procedures for troubleshooting customer problems and verify the procedures include: • PAN and/or SAD is never output to merchant environment • Collection of PAN and/or SAD only when needed to solve a specific problem • Storage of such data in a specific, known location with limited access • Collection of only a limited amount of data needed to solve a specific problem • Encryption of account data while stored • Secure deletion of such data immediately after use	*<Report Findings Here>*
3B-6.1.b For a sample of recent troubleshooting requests, observe data collection and storage locations, and interview responsible personnel to verify the procedures identified at 3B-6.1.a were followed.	*<Report Findings Here>*
3B-6.2 Provide instructions via the *P2PE Instruction Manual* for the merchant to follow secure troubleshooting procedures.	
3B-6.2 Examine the *P2PE Instruction Manual (PIM)* to verify it includes information for the merchant regarding the solution provider's troubleshooting processes, including that the solution provider ensures the following: • PAN and/or SAD is never output to the merchant environment • Collection of PAN and/or SAD only when needed to solve a specific problem. • Storage of such data only in specific, known locations with limited access. • Collection of only a limited amount of data needed to solve a specific problem. • Encryption of account data while stored • Secure deletion of such data immediately after use	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-7 The P2PE solution provides auditable logs of any changes to critical functions of the POI device(s).	
3B-7.1 Ensure that any changes to the critical functions of the POI are logged—either on the device or within the remote-management systems of the P2PE solution provider. Critical functions include application and firmware updates as well as changes to security-sensitive configuration options, such as whitelists or debug modes.	
3B-7.1.a Examine device and/or system configurations to verify that any changes to the critical functions of the POI are logged, including: • Changes to the applications within the device • Changes to the firmware within the device • Changes to any security-sensitive configuration options within the device (including whitelists and debug modes)	*<Report Findings Here>*
3B-7.1.b Observe authorized personnel perform authorized changes on POI devices, as follows, and examine log files to verify that all such activities result in a correlating log file: • Changes to the applications within the device • Changes to the firmware within the device • Changes to any security-sensitive configuration options within the device (including whitelists and debug modes)	*<Report Findings Here>*
3B-8 Solution provider implements tamper-detection mechanisms for devices in their possession, and provides related instructions to merchants.	
3B-8.1 Perform periodic physical inspections of devices in solution provider's possession to detect tampering or modification of devices. ***Note:*** *Frequency of inspection should be appropriate for device location and usage. For example, it may be suitable to inspect POIs in secure storage at least quarterly.*	
3B-8.1.a Examine documented procedures to verify they define: • Procedures for performing periodic inspections of devices to detect signs of tampering or modification, for all POI devices in the solution provider's possession • The frequency of inspections	*<Report Findings Here>*
3B-8.1.b Observe inspection processes to verify that inspections detect tampering or modification of POI devices.	*<Report Findings Here>*
3B-8.1.c Examine inspection records and interview personnel to verify that inspections are periodically performed according to the defined frequency for all POI devices in the solution provider's possession.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-8.1.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to perform periodic physical inspections of devices to detect tampering or modification of devices. Detailed procedures for performing periodic physical inspections to include: • Description of tamper-detection mechanisms • Guidance for physical inspections, including photographs or drawings of the device illustrating what the merchant is to inspect, for example: ○ Missing or altered seals or screws, extraneous wiring, holes in the device, or the addition of labels or other covering material that could be used to mask damage from device tampering. ○ Instructions for weighing POI devices on receipt and then periodically for comparison with vendor specifications to identify potential insertion of tapping mechanisms within devices • Recommendations for frequency of inspections ***Note:*** *Frequency of inspection should be appropriate for device location and usage. For example, it may be suitable for merchants to inspect POIs in secure storage at least quarterly, and to inspect POIs in use at least weekly. If POIs cannot easily be inspected—for example, due to remote or inaccessible locations—alternative controls should be implemented to mitigate the risk of less-frequent inspections.*	
3B-8.1.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes detailed procedures for merchants to perform periodic physical inspections of devices to detect tampering or modification. Verify instructions include: • Description of tamper-detection mechanisms • Guidance for physical inspections, including photographs or drawings of the device illustrating what the merchant is to inspect, for example: ○ Missing or altered seals or screws, extraneous wiring, holes in the device, or the addition of labels or other covering material that could be used to mask damage from device tampering. ○ Instructions for weighing POI devices on receipt and then periodically for comparison with vendor specifications to identify potential insertion of tapping mechanisms within devices • Recommendations for frequency of inspections	*<Report Findings Here>*
3B-8.2 Implement tamper-detection mechanisms and/or processes for devices deployed in remote or unattended locations—for example, use cameras or other physical mechanisms to alert personnel to physical breach.	
3B-8.2.a Examine documented procedures to verify tamper-detection mechanisms and/or processes are defined for devices deployed in remote or unattended locations.	*<Report Findings Here>*
3B-8.2.b Observe tamper-detection mechanisms and/or processes in use to verify detection mechanisms and/or processes are implemented for devices deployed in remote or unattended locations.	*<Report Findings Here>*
3B-8.2.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement tamper-detection mechanisms and/or processes for devices deployed in remote or unattended locations—for example, the use of cameras or other physical mechanisms to alert personnel to physical breach.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-8.2.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes instructions for implementing tamper-detection mechanisms and/or processes for devices deployed in remote or unattended locations.	*<Report Findings Here>*
3B-8.3 Implement procedures for responding to tampered devices.	
3B-8.3.a Examine documented procedures to verify procedures are defined for responding to tampered devices.	*<Report Findings Here>*
3B-8.3.b Observe response processes and interview response personnel to verify procedures for responding to tampered devices are implemented.	*<Report Findings Here>*
3B-8.3.1 Provide instructions via the *P2PE Instruction Manual* for the merchant to implement procedures for responding to tampered devices.	
3B-8.3.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes response procedures and contact details for merchants to report and respond to tampered devices.	*<Report Findings Here>*
3B-9 Solution provider implements mechanisms to monitor and respond to suspicious activity on POI devices deployed at merchant locations.	
3B-9.1 Implement mechanisms to provide immediate notification of suspicious activity, including but not limited to: • Physical device breach • Logical alterations to device (configuration, access controls) • Disconnect/reconnect of devices (notification for known devices, but an alert if device is not recognized) • Failure of any device security control	
3B-9.1.a Examine documented procedures to verify mechanisms are defined to provide immediate notification of potential security breaches, including but not limited to: • Physical device breach • Logical alterations to device (configuration, access controls) • Disconnect/reconnect of devices (notification for known devices, but an alert if device is not recognized) • Failure of any device security control	*<Report Findings Here>*
3B-9.1.b Observe notification mechanisms and interview response personnel to verify the mechanisms provide immediate notification of suspicious activity, including but not limited to: • Physical device breach • Logical alterations to device (configuration, access controls) • Disconnect/reconnect of devices (notification for known devices, but an alert if device is not recognized) • Failure of any device security control	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3B-9.1.1 Provide instructions and contact details via the *P2PE Instruction Manual* for the merchant to notify the solution provider of suspicious activity.	
3B-9.1.1 Examine the *P2PE Instruction Manual (PIM)* to verify it includes instructions and contact details for the merchant to notify the solution provider of suspicious activity.	*<Report Findings Here>*
3B-9.2 Prepare incident-response procedures to respond to detection of potential security breaches, including but not limited to: • Physical device breach • Logical alterations to device (configuration, access controls) • Connection of unrecognized device • Failure of any device security control	
3B-9.2.a Examine documented incident-response procedures and verify that procedures are defined for responding to: • Physical device breach • Logical alterations to device (configuration, access controls) • Connection of unrecognized device • Failure of any device security control	*<Report Findings Here>*
3B-9.2.b Observe incident-response processes and interview response personnel to verify procedures are implemented for responding to: • Physical device breach • Logical alterations to device (configuration, access controls) • Connection of unrecognized device • Failure of any device security control	*<Report Findings Here>*
3C-1 Solution provider develops, maintains, and disseminates a *P2PE Instruction Manual (PIM)* to merchants	
3C-1.1 Develop and maintain *P2PE Instruction Manual (PIM)* and distribute PIM to merchants. Ensure PIM is available to merchants upon request. PIM must address the following:	
3C-1.1.a Examine documented procedures to verify mechanisms are defined to distribute the PIM to all merchants using the P2PE solution, and to provide PIM to merchants upon request.	*<Report Findings Here>*
3C-1.1.b Interview responsible personnel and observe processes to verify PIM is distributed to all merchants using the P2PE solution and PIM is provided to merchants upon request.	*<Report Findings Here>*
3C-1.1.1 All requirements in this document wherever the *P2PE Instruction Manual (PIM)* is referenced.	
3C-1.1.1 Examine the *P2PE Instruction Manual (PIM)* to verify it covers all related instructions, guidance and requirements in this document (summarized in Domain 3 PIM Annex).	*<Report Findings Here>*
3C-1.1.2 Specific instructions for installing and connecting POI devices to maintain the integrity of P2PE solution, including any permitted connections to other devices.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3C-1.1.2 Examine the *P2PE Instruction Manual (PIM)* to verify it includes specific instructions for installing and connecting POI devices to maintain the integrity of P2PE solution, including any permitted connections to other devices.	*<Report Findings Here>*
3C-1.1.3 Specific details of all PCI-approved POI components used in the P2PE solution.	
3C-1.1.3 Examine the *P2PE Instruction Manual (PIM)* to verify it includes details of all PCI-approved POI components used in the P2PE solution.	*<Report Findings Here>*
3C-1.1.4 If the P2PE solution includes or allows for a POI component that is not PCI-approved (for example, the P2PE solution provides a PCI-approved SCR which may be attached to a non PCI-approved component), the PIM includes detailed instructions for connecting the PCI-approved component to other devices and/or components in order to ensure the integrity of the P2PE solution is maintained.	
3C-1.1.4 If the P2PE solution includes or allows for a POI component that is not PCI-approved (for example, the P2PE solution provides a PCI-approved SCR which may be attached to a non PCI-approved component), verify the PIM includes detailed instructions for connecting the PCI-approved component to other devices and/or components in order to ensure the integrity of the P2PE solution is maintained.	*<Report Findings Here>*
3C-1.1.5 Specific guidance that if a PCI-approved POI component is connected to another device or data-capture mechanism (for example, if a PCI-approved SCR was connected to a non PCI-approved keypad), the non-PCI-approved capture mechanism is not secured by the P2PE solution, and the use of any such mechanisms to collect PCI payment-card data would negate any PCI DSS scope reduction which might otherwise have been provided by the P2PE solution's device. ***Note**: P2PE Requirement 1A-1.1 allows only PCI-approved POI devices to be used for accepting and processing P2PE transactions.*	
3C-1.1.5 Examine the *P2PE Instruction Manual (PIM)* to verify it includes specific guidance that if a PCI-approved POI component is connected to another device or data-capture mechanism, the non-PCI-approved capture mechanism is not secured by the P2PE solution, and the use of any such mechanisms to collect PCI payment-card data would negate any PCI DSS scope reduction which might otherwise have been provided by the P2PE solution's device.	*<Report Findings Here>*
3C-1.1.6 Provides specific information that changing or attempting to change device configurations or settings would negate the solution's ability to provide PCI DSS scope reduction. Examples include, but are not limited to: Attempting to enable any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device Attempting to alter security configurations or authentication controls Physically opening the device Attempting to install applications onto the device	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 3 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
3C-1.1.6 Examine the *P2PE Instruction Manual (PIM)* to verify it includes specific information that changing or attempting to change device configurations or settings would negate the solution's ability to provide PCI DSS scope reduction. Examples include, but are not limited to: Attempting to enable any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device Attempting to alter security configurations or authentication controls Physically opening the device Attempting to install applications onto the device	*<Report Findings Here>*
3C-1.2 Review *P2PE Instruction Manual (PIM)* at least annually and upon changes to the solution or the PCI P2PE requirements. Update PIM as needed to keep the documentation current with: • Any changes to the P2PE solution, and • Any changes to the requirements in this document.	
3C-1.2.a Examine documented procedures to verify they include: • PIM must be reviewed at least annually and upon changes to the solution or changes to the PCI P2PE requirements • PIM must be updated as needed to keep the document current with: • Any changes to the P2PE solution, and Any changes to the PCI P2PE requirements.	*<Report Findings Here>*
3C-1.2.b Observe processes for reviewing and updating the PIM, and interview responsible personnel to verify: • PIM is reviewed at least annually and upon changes to the solution or changes to the PCI P2PE requirements • PIM is updated as needed to keep the document current with: o Any changes to the P2PE solution, and o Any changes to the PCI P2PE requirements.	*<Report Findings Here>*
3C-1.2.1 Communicate PIM updates to affected merchants, and provide merchants with updated PIM as needed.	
3C-1.2.1.a Examine documented procedures to verify they include communicating PIM updates to affected merchants and providing an updated PIM as needed.	*<Report Findings Here>*
3C-1.2.1.b Observe processes for reviewing and updating the PIM, and interview responsible personnel to verify PIM updates are communicated to affected merchants and an updated PIM is provided to merchants as needed.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

Domain 4: Segmentation between Encryption and Decryption Environments

Domain 4 is Not Applicable for P2PE Standard v1.1 – Hardware/Hardware solutions

Copyright 2012 PCI Security Standards Council LLC

Domain 5: Decryption Environment and Device Management

Table 5.1 – List of all HSMs used in P2PE solution decryption environment

(All Domain 2 Requirements apply.)

PCI PTS-approved HSMs								
HSM device name/ identifier	HSM manufacturer	HSM model name and number	Device location	**PTS** approval number	**PTS** approval class	Approved HSM Hardware version #	Approved HSM Firmware version #	Applications (include version number) resident on the HSM which were included in the PTS assessment

FIPS-approved HSMs								
HSM device name/ identifier	HSM manufacturer	HSM model name and number	Device location	**FIPS 140-2** listing number	**FIPS 140-2** certification level	Approved HSM Hardware version #		Approved HSM Firmware version #

Copyright 2012 PCI Security Standards Council LLC

Table 5.2 – **Samples of HSMs assessed for Domain 5 Testing Procedures**

Note: *Sampling of HSMs is only permitted for specific requirements.*
Every HSM Hardware # and Firmware # listed in Table 5.1 must be included in every sample set in Table 5.2.

HSM device type name/identifier (per Table 1.1)	**Sample Size** (Number of each device type assessed for Domain 5 Testing Procedures)	**Rationale** How sample size was determined to be appropriate and representative of the overall population	**Domain 5 Testing Procedures this sample was assessed against**
HSM Sample Set #1 – Description (e.g., HSMs in use)			
POI Sample Set #2 – Description (e.g., HSMs being decommissioned)			
POI Sample Set #3 – Description (e.g., POIs …)			

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 5 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
5A-1 Use approved decryption devices	
5A-1.1 Ensure that all hardware security modules (HSMs) are either: • FIPS140-2 Level 3 or higher certified, or • A PCI-approved HSM.	
5A-1.1.a For all HSMs used in the solution, examine approval documentation (e.g., FIPS certification or PTS approval) and review the list of approved devices to verify that all HSMs used in the solution are either: • Listed on the NIST Cryptographic Module Validation Program (CMVP) list, with a valid listing number, and approved to FIPS 140-2 Level 3, or higher. Refer to http://csrc.nist.gov. • Listed on the PCI SSC website, with a valid SSC listing number, as Approved PCI PTS Devices under the approval class "HSM." Refer to https://www.pcisecuritystandards.org.	*<Report Findings Here>*
5A-1.1.b Examine documented procedures and interview personnel to verify that all decryption operations are performed only by the FIPS-approved and/or PTS-approved HSMs identified in 5A-1.1.a.	*<Report Findings Here>*
5A-1.1.1 The approval listing must match the deployed devices in the following characteristics: Model name and number Hardware version number Firmware version number For PCI-approved HSMs, any applications, including application version number, resident within the device which were included in the PTS assessment	
5A-1.1.1.a For all PCI-approved HSMs used in the solution, examine HSM devices and review the PCI SSC list of Approved PCI PTS Devices to verify that all of the following device characteristics match the PCI PTS listing for each HSM: Model name/number Hardware version number Firmware version number Any applications, including application version number, resident within the device which were included in the PTS assessment	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 5 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
5A-1.1.1.b For all FIPS-approved HSMs used in the solution, examine HSM devices and review the NIST Cryptographic Module Validation Program (CMVP) list to verify that all of the following device characteristics match the FIPS140-2 Level 3 (or higher) approval listing for each HSM: Model name/number Hardware version number Firmware version number	*<Report Findings Here>*
5A-1.1.2 If FIPS-approved HSMs are used, the FIPS approval must cover all functions used for the P2PE solution, including all cryptographic algorithms, data-protection mechanisms, and key-management processes.	
5A-1.1.2 Examine FIPS approval documentation and HSM operational procedures to verify that the FIPS approval covers all HSM components and functions used for the P2PE solution, including all cryptographic algorithms, data-protection mechanisms, and key-management processes.	*<Report Findings Here>*
5A-1.1.3 If FIPS-approved HSMs are used, the HSM must be configured to operate in the FIPS-approved mode for all operations (including algorithms, data protection, key management, etc.), according to the FIPS140-2 Level 3 (or higher) certification.	
5A-1.1.3.a Examine documented HSM operational procedures to verify they require HSMs to be configured to operate in the FIPS-approved mode for all P2PE operations (including algorithms, data protection, key management, etc.), according to the FIPS140-2 Level 3 (or higher) certification.	*<Report Findings Here>*
5A-1.1.3.b Examine HSM configurations for all P2PE solution functions to verify that HSMs are configured to operate in the FIPS-approved mode for all operations (including algorithms, data protection, key management, etc.), according to the FIPS140-2 Level 3 (or higher) certification.	*<Report Findings Here>*
5A-1.2 Decryption devices (HSMs) must be deployed according to the security policy to which they have been approved. ***Note:*** *Both FIPS140-2 and PCI HSM require that the decryption-device manufacturer makes available a security policy document to end users, which provides information on how the device must be installed, maintained, and configured to meet the compliance requirements under which it was approved.*	
5A-1.2 Examine the security policies for decryption devices and observe device implementations to verify HSMs are deployed in accordance with the security policy to which they have been approved.	*<Report Findings Here>*
5B-1 Maintain inventory-control and monitoring procedures for decryption devices.	

Copyright 2012 PCI Security Standards Council LLC

5B-1.1 Maintain inventory-control and monitoring procedures to accurately track devices from receipt until decommissioning, including where devices are: • Deployed • Awaiting deployment • Undergoing repair or otherwise not in use • In transit The inventory-control and monitoring procedures must provide for the following:	
5B-1.1.a Examine documented inventory-control procedures to confirm that they define methods for tracking device locations from receipt of the device until device decommissioning, including where devices are: • Deployed • Awaiting deployment • Undergoing repair or otherwise not in use • In transit	*<Report Findings Here>*
5B-1.1.b Verify documented procedures include 5B-1.1.1 through 5B-1.1.3 below.	*<Report Findings Here>*
5B-1.1.c Examine the documented device inventory and observe device locations to verify that the inventory-control and monitoring procedures accurately track device locations.	*<Report Findings Here>*
5B-1.1.1 Record device serial number in inventory-control system as soon as possible upon receipt and prior to installation.	
5B-1.1.1 Review documented device inventories and interview personnel to verify that devices are entered into the inventory-control system as soon as possible upon receipt of the device, and prior to installation.	*<Report Findings Here>*
5B-1.1.2 Devices are protected against unauthorized substitution or modification until all applicable keys have been loaded.	
5B-1.1.2 Observe implemented controls and interview personnel to verify that devices are protected against unauthorized substitution or modification until all applicable keys have been loaded.	*<Report Findings Here>*
5B-1.1.3 Control and monitoring procedures must provide for detection of lost or stolen equipment and notification to authorized personnel	
5B-1.1.3 Observe implemented controls and interview personnel to verify that procedures are implemented to detect lost or stolen devices and notify authorized personnel.	*<Report Findings Here>*
5B-1.2 Perform device inventories at least annually to detect removal or substitution of devices.	

Copyright 2012 PCI Security Standards Council LLC

5B-1.2.a Examine documented procedures to verify device inventories are required to be performed at least annually to detect removal or substitution of devices.	*<Report Findings Here>*
5B-1.2.b Examine records of device inventories and interview personnel to verify that device inventories are performed at least annually.	*<Report Findings Here>*
5B-1.3 Maintain a documented inventory of all devices to include at least the following: • Make, model, and hardware version of device • Location (including site/facility, if applicable) • Serial number • General description • Security seals, labels, hidden markings, etc. • Number and type of physical connections to device • Date of last inventory performed • Firmware version • Hardware version • Applications (including versions)	
5B-1.3.a Verify through observation that a documented inventory of all devices is maintained.	*<Report Findings Here>*
5B-1.3.b Verify the documented inventory includes at least the following: • Make, model, and hardware version of device • Location (including site/facility, if applicable) • Serial number • General description • Security seals, labels, hidden markings, etc. • Number and type of physical connections to device • Date of last inventory performed • Hardware version • Firmware version • Applications and versions	*<Report Findings Here>*
5B-1.3.1 Secure the documented inventory of devices from unauthorized access.	
5B-1.3.1 Observe implemented controls and interview personnel to verify the documented inventory of devices is secured from unauthorized access.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

5B-1.4 Implement procedures for detecting and responding to variances in the annual inventory, including identification of missing or substituted devices.	
5B-1.4.a Examine documented procedures to verify procedures are defined for detecting and responding to variances in the annual inventory, including identification of missing or substituted devices.	*<Report Findings Here>*
5B-1.4.b Interview personnel to verify procedures for detecting and responding to variances in the annual inventory, including identification of missing or substituted devices, are implemented.	*<Report Findings Here>*
5B-2 Physically secure decryption devices when not in use.	
5B-2.1 Physically secure the storage of devices awaiting deployment.	
5B-2.1.a Examine documented procedures to verify they include storing decryption devices awaiting deployment in a physically secure location.	*<Report Findings Here>*
5B-2.1.b Inspect storage locations for decryption devices awaiting deployment, to verify that the location is physically secure.	*<Report Findings Here>*
5B-2.2 Physically secure the storage of devices undergoing repair or otherwise not in use.	
5B-2.2.a Examine documented procedures to verify they include storing decryption devices undergoing repair or otherwise not in use in a physically secure location.	*<Report Findings Here>*
5B-2.2.b Inspect storage locations for decryption devices undergoing repair or otherwise not in use to verify that the location is physically secure.	*<Report Findings Here>*
5B-2.3 Physically secure the storage of devices awaiting transport between sites/locations.	
5B-2.3.a Examine documented procedures to verify they include storing decryption devices awaiting transport between sites/locations in a physically secure location.	*<Report Findings Here>*
5B-2.3.b Inspect storage locations for decryption devices awaiting transport between sites/locations to verify that the location is secure.	*<Report Findings Here>*
5B-2.4 Physically secure devices in transit, including: • Packing devices in tamper-evident packaging prior to transit • Implementing procedures for determining whether device packaging has been tampered with • Use of a defined, secure transport method, such as bonded carrier or secure courier	

Copyright 2012 PCI Security Standards Council LLC

5B-2.4.a Examine documented procedures for the transportation of decryption devices to verify they include: • Procedures for packing decryption devices in tamper-evident packaging prior to transit • Procedures for determining whether device packaging has been tampered with • Procedures for using a defined, secure transport method, such as bonded carrier or secure courier	*<Report Findings Here>*
5B-2.4.b For a sample of device shipments, examine records of device transportation and interview personnel to verify that the following procedures are implemented: • Decryption devices are packed in tamper-evident packaging prior to transit. • Procedures are followed for determining if device packaging has been tampered with. • Use of a defined secure transport method, such as bonded carrier or secure courier.	*<Report Findings Here>*
5B-2.4.1 Implement procedures to be followed upon determining that device packaging has been tampered with, including: Devices must not be deployed or used Procedures for returning device to authorized party for investigation Escalation procedures and contact details for reporting tamper-detection	
5B-2.4.1.a Examine documented procedures to verify they include procedures to be followed upon determining that device packaging has been tampered with, including: Devices must not be deployed or used Procedures for returning device to authorized party for investigation Contact details for reporting tamper-detection	*<Report Findings Here>*
5B-2.4.1.b Interview response personnel to verify that, upon determining that device packaging has been tampered with, the following procedures are implemented: Devices are not deployed or used. Procedures are followed for returning device to authorized party for investigation. Reporting of tamper-detection to defined contact details.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

5B-2.5 Ensure devices are only transported between trusted sites/locations, as follows: • A list of trusted sites (e.g., vendor / maintenance provider, etc.) is maintained. • Only devices received from trusted sites/locations are accepted for use. • Procedures are defined in the event that devices are received from untrusted or unknown locations, including: ○ Procedures (including contact details for authorized parties) for verifying location from which device was sent ○ Procedures to ensure devices are not used unless and until the source location is verified as trusted ○ Devices are sent only to trusted sites/locations.	
5B-2.5.a Examine documented procedures to verify they include: • A list of trusted sites (e.g., vendor / maintenance provider, etc.) between which devices may be transported • Procedures to ensure that only devices received from trusted sites/locations are accepted for use • Procedures to be followed in the event that a device is received from an untrusted or unknown location, including: ○ Procedures (including contact details for authorized parties) for verifying location from which device was sent ○ Procedures to ensure devices are not used unless and until the source location is verified as trusted • Procedures to ensure that devices are only sent to trusted sites/locations	*<Report Findings Here>*
5B-2.5.b For a sample of device shipments, examine records of device transportation and interview personnel to verify: • Only devices received from trusted sites/locations are accepted for use. • Procedures are followed in the event that a device is received from an untrusted or unknown location, including: ○ Procedures (including contact details for authorized parties) for verifying location from which device was sent ○ Procedures to ensure devices are not used unless and until the source location is verified as trusted • Devices are only sent to trusted sites/locations	*<Report Findings Here>*
5B-3 Prevent and detect the unauthorized alteration or replacement of devices prior to and during deployment.	
5B-3.1 Ensure devices are placed into service only if there is assurance that the equipment has not been subject to unauthorized modification, substitution, or tampering prior to being put into use. ***Note:*** *This requirement applies to HSMs and other SCDs used for decryption and/or key storage and/or other key-management functions and/or signing of whitelists within the decryption environment.*	

Copyright 2012 PCI Security Standards Council LLC

5B-3.1a Review documented procedures to confirm that processes are defined to provide assurance that devices have not been substituted or subjected to unauthorized modifications or tampering prior to being put into use.	*<Report Findings Here>*
5B-3.1b Observe processes and interview personnel to verify that processes are followed to provide assurance that devices have not been substituted or subjected to unauthorized modifications or tampering prior to being put into use.	*<Report Findings Here>*
5B-3.1.1 Implement controls to protect devices from unauthorized access up to deployment. Controls must include the following:	
5B-3.1.1.a Review documented procedures to verify they include protecting devices from unauthorized access up to deployment.	*<Report Findings Here>*
5B-3.1.1.b Verify documented procedures include 5B-3.1.1.1 through 5B-3.1.1.3 below.	*<Report Findings Here>*
5B-3.1.1.c Verify procedures are implemented as follows:	*<Report Findings Here>*
5B-3.1.1.1 Ensure access to all devices is documented, defined, logged, and controlled.	
5B-3.1.1.1.a Examine access-control documentation and device configurations to verify that access to all devices is defined and documented.	*<Report Findings Here>*
5B-3.1.1.1.b For a sample of devices, observe authorized personnel accessing devices and examine access logs to verify that access to all devices is logged.	*<Report Findings Here>*
5B-3.1.1.1.c Examine implemented access controls to verify that unauthorized individuals cannot access, modify, or substitute any device.	*<Report Findings Here>*
5B-3.1.1.2 Devices do not use default keys (such as keys that are pre-installed for testing purposes), passwords, or data.	
5B-3.1.1.2 Examine vendor documentation or other information sources to identify default keys (such as keys that are pre-installed for testing purposes), passwords, or data. Observe implemented processes and interview personnel to verify that default keys, passwords, or data are not used.	*<Report Findings Here>*
5B-3.1.1.3 All personnel with access to devices are documented in a formal list and authorized by management. The list of authorized personnel is reviewed at least annually.	

Copyright 2012 PCI Security Standards Council LLC

5B-3.1.1.3.a Examine documented authorizations to verify: • All personnel with access to devices are documented in a formal list. • All personnel with access to devices are authorized by management. • The list of authorized personnel is reviewed at least annually.	*<Report Findings Here>*
5B-3.1.1.3.b For a sample of devices, examine account-access configurations to verify that only personnel documented and authorized in the formal list have access to devices.	*<Report Findings Here>*
5B-3.1.2 Implement a documented "chain-of-custody" to ensure that all devices are controlled from receipt through to installation and use. The chain-of-custody must include records to identify responsible personnel for each interaction with the devices.	
5B-3.1.2.a Examine documented processes to verify that the chain of custody is required for devices from receipt to installation and use.	*<Report Findings Here>*
5B-3.1.2.b For a sample of devices, review documented records and interview responsible personnel to verify the chain of custody is maintained from receipt to installation and use.	*<Report Findings Here>*
5B-3.1.2.c Verify the chain of custody records identify responsible personnel for each interaction with the device	*<Report Findings Here>*
5B-3.1.3 Implement controls, including the following, to ensure that all received devices are from a legitimate source:	
5B-3.1.3.a Examine documented purchasing, receipt, and deployment procedures to confirm that they include verifying all received hardware components are from a legitimate source.	*<Report Findings Here>*
5B-3.1.3.b Confirm that the documented procedures include 5B-3.1.3.1 through 5B-3.1.3.2 below.	*<Report Findings Here>*
5B-3.1.3.1 Device serial numbers must be compared to the serial numbers documented by the sender to ensure device substitution has not occurred. A record of device serial-number verification must be maintained. ***Note:*** *Examples of how serial numbers may be documented by the sender include but are not limited to: purchase order, shipping waybill, manufacturer's invoice, or similar document*	
5B-3.1.3.1.a Interview responsible personnel to verify that device serial numbers are compared to the serial number documented by the sender.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

5B-3.1.3.1.b For a sample of received devices, review sender documentation (for example, the purchase order, shipping waybill, manufacturer's invoice, or similar documentation) used to verify device serial numbers. Examine the record of serial-number validations to confirm the serial numbers for the received device were verified to match that documented by the sender.	*<Report Findings Here>*
5B-3.1.3.2 Documentation used for this process must be received via a separate communication channel and must not have arrived with the shipment.	
5B-3.1.3.2 For a sample of received devices, review delivery records and interview responsible personnel to verify that documentation used to validate the device serial number was received via a separate communication channel than the device and was not received in the same shipment as the device.	*<Report Findings Here>*
5B-3.1.4 Implement physical protection of devices from the manufacturer's facility up to the point of key-insertion or inspection, through one or more of the following. Transportation using a trusted courier service (for example, via bonded carrier). The devices are then securely stored until key-insertion occurs. Use of physically secure and trackable packaging (for example, pre-serialized, counterfeit-resistant, tamper-evident packaging). The devices are then stored is such packaging, or in secure storage, until key-insertion occurs. A secret, device-unique "transport-protection token" is loaded into the secure storage area of each device at the manufacturer's facility. Before key-insertion, the SCD used for key-insertion verifies the presence of the correct "transport-protection token" before overwriting this value with the initial key.	
5B-3.1.4.a Examine documented procedures to confirm that they require physical protection of devices from the manufacturer's facility up to the point of key-insertion or inspection, through one or more of the defined methods.	*<Report Findings Here>*
5B-3.1.4.b Interview responsible personnel to verify that one or more of the defined methods are in place to provide physical device protection for devices, from the manufacturer's facility up to the point of key-insertion.	*<Report Findings Here>*
5B-3.1.5 Inspect and test all SCDs prior to installation to verify devices have not been tampered with or compromised. Processes must include:	
5B-3.1.5.a Examine documented procedures to verify they require inspection and testing of devices prior to installation to verify integrity of device.	*<Report Findings Here>*
5B-3.1.5.b Verify documented procedures include 5B-3.1.5.1 through 5B-3.1.5.4, below.	*<Report Findings Here>*
5B-3.1.5.1 Running self-tests to ensure the correct operation of the device	
5B-3.1.5.1 Examine records of device inspections and tests, and observe tests in progress to verify that self-tests are run on devices to ensure the correct operation of the device.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

5B-3.1.5.2 Installing (or re-installing) devices only after confirming that the device has not been tampered with or compromised	
5B-3.1.5.2 Observe inspection processes and interview responsible personnel to verify that devices are installed, or reinstalled, only after confirming that the device has not been tampered with or compromised.	*<Report Findings Here>*
5B-3.1.5.3 Physical and/or functional tests and visual inspection to confirm that physical and logical controls and anti-tamper mechanisms are not modified or removed	
5B-3.1.5.3 Observe inspection processes and interview responsible personnel to confirm processes include physical and/or functional tests and visual inspection to verify that physical and logical controls and anti-tamper mechanisms are not modified or removed.	*<Report Findings Here>*
5B-3.1.5.4 Maintaining records of the tests and inspections, and retaining records for at least one year	
5B-3.1.5.4.a Examine records of inspections and interview responsible personnel to verify records of the tests and inspections are maintained.	*<Report Findings Here>*
5B-3.1.5.4.b Examine records of inspections to verify records are retained for at least one year.	*<Report Findings Here>*
5B-3.1.6 Maintain device in original, tamper-evident packaging until ready for installation.	
5B-3.1.6.a Examine documented procedures to verify they require devices be maintained in original, tamper-evident packaging until ready for installation.	*<Report Findings Here>*
5B-3.1.6.b Observe a sample of received devices to verify they are maintained in original, tamper-evident packaging until ready for installation.	*<Report Findings Here>*
5B-4 Physically secure decryption devices to prevent unauthorized access, modification, or substitution of deployed devices.	
5B-4.1 Physically secure deployed devices to prevent unauthorized removal or substitution.	
5B-4.1.a Examine physical security policy and procedures to verify devices must be physically secured to prevent unauthorized removal or substitution.	*<Report Findings Here>*
5B-4.1.b Inspect the secure location in which the decryption devices are deployed and verify that these devices are physically secured to prevent unauthorized removal or substitution.	*<Report Findings Here>*
5B-4.2 Implement dual-control mechanisms to help prevent substitution of devices, both in service and spare or backup devices.	
5B-4.2.a Examine documented procedures to verify that dual-control mechanisms are defined to prevent substitution of devices, both in-service and spare or backup devices.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

5B-4.2.b Examine dual-control mechanisms in use, for both in-service and spare or backup devices, to verify that the mechanisms prevent substitution of devices.	*<Report Findings Here>*
5B-5 Prevent unauthorized physical access to decryption devices in use.	
5B-5.1 Restrict physical access to decryption devices to minimum required personnel.	
5B-5.1.a Examine documented access privileges and procedures to verify that physical access to devices is restricted to minimum required personnel.	*<Report Findings Here>*
5B-5.1.b Observe access controls and processes and interview personnel to verify that physical access to devices is restricted to the minimum required personnel.	*<Report Findings Here>*
5B-5.2 Implement procedures to control and document all physical access to decryption devices in use. Procedures to include: • Identifying personnel authorized to access devices; • Restricting access to authorized personnel; • Maintaining a log of all access including personnel name, company, reason for access, time in and out. Retain access log for at least one year.	
5B-5.2.a Examine documented access procedures and verify they require controlling and documenting all physical access to devices, and include: • Identifying personnel authorized to access devices • Restricting access to authorized personnel • Maintaining a log of all access including personnel name, company, reason for access, time in and out • Retaining access logs for at least one year	*<Report Findings Here>*
5B-5.2.b Observe physical access controls to verify they include controlling and documenting all physical access to devices, and include: • Identifying personnel authorized to access devices • Restricting access to authorized personnel • Maintaining a log of all access including personnel name, company, reason for access, time in and out	*<Report Findings Here>*
5B-5.2.c Examine the access logs/records to verify it is retained for at least one year and contains, at a minimum, the following details: • Personnel name • Company • Reason for access • Time in and out	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

5B-5.3 Implement procedures for identification and authorization of third-party personnel (including repair /maintenance personnel) prior to granting access. Procedures must include the following:	
5B-5.3.a Examine documented procedures to verify they include identification and authorization of third-party personnel prior to granting access.	*<Report Findings Here>*
5B-5.3.b Verify documented procedures include 5B-5.3.1 through 5B-5.3.4 below.	*<Report Findings Here>*
5B-5.3.1 Procedures to verify the identity and authorization of third-party personnel prior to granting access to devices.	
5B-5.3.1 Interview personnel and observe processes to confirm that the identity and authorization of third-party personnel is verified prior to granting access to devices.	*<Report Findings Here>*
5B-5.3.2 Unexpected personnel must be denied access unless fully validated and authorized.	
5B-5.3.2 Interview responsible personnel and observe processes to verify that unexpected personnel are denied access until fully validated and authorized.	*<Report Findings Here>*
5B-5.3.3 Once authorized, third-party personnel must be escorted and monitored at all times.	
5B-5.3.3 Interview responsible personnel and observe processes to verify that, once authorized, third-party personnel are escorted and monitored at all times.	*<Report Findings Here>*
5B-5.3.4 A log of all third-party personnel access is maintained in accordance with 5B-5.2.	
5B-5.3.4 Examine access logs/records to verify that a log of all third-party personnel access is maintained in accordance with logging requirements defined in 5B-5.2.	*<Report Findings Here>*
5B-6 Maintain secure updates for decryption devices	
5B-6.1 Implement secure update processes for all firmware and software updates, to include: • Integrity check of update • Authentication of origin of the update	
5B-6.1.a Examine documented procedures to verify secure update processes are defined for all firmware and software updates, and include: • Integrity checks of update • Authentication of origin of the update	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

5B-6.1b Observe a sample of firmware and software updates, and interview personnel to verify: • The integrity of the update is checked • The origin of the update is authenticated	*<Report Findings Here>*
5C-1 Securely maintain devices.	
5C-1.1 Document operational security procedures for physical security controls and operational activities throughout device lifecycle, including but not limited to: • Installation procedures • Maintenance and repair procedures • Production procedures • Replacement procedures • Destruction procedures	
5C-1.1 Verify operational security procedures are documented for physical security controls and operational activities throughout device lifecycle, including but not limited to. • Installation procedures • Maintenance and repair procedures • Production procedures • Replacement procedures • Destruction procedures	*<Report Findings Here>*
5C-1.2 Procedures must be in place and implemented to protect decryption devices and ensure the destruction of any cryptographic keys or key material within such devices when removed from service, retired at the end of the deployment lifecycle, or returned for repair.	
5C-1.2.1 Procedures are in place to ensure that any devices to be removed from service, retired, or returned for repair are not intercepted or used in an unauthorized manner, as follows:	
5C-1.2.1.a Examine documented procedures to verify that procedures are defined for any devices to be removed from service, retired, or returned for repair.	*<Report Findings Here>*
5C-1.2.1.b Verify documented procedures include 5B-1.2.1.1 through 5B-1.2.1.5 below.	*<Report Findings Here>*
5C-1.2.1.1 Affected entities are notified before devices are returned.	
5C-1.2.1.1 Interview responsible personnel and examine device-return records to verify that affected entities are notified before devices are returned.	*<Report Findings Here>*
5C-1.2.1.2 Devices are transported via trusted carrier service—for example, bonded carrier.	

Copyright 2012 PCI Security Standards Council LLC

5C-1.2.1.2 Interview responsible personnel and examine device-return records to verify that devices are transported via trusted carrier service—for example, bonded carrier.	*<Report Findings Here>*
5C-1.2.1.3 Devices are shipped in serialized, counterfeit-resistant, and tamper-evident packaging.	
5C-1.2.1.3 Interview responsible personnel and observe device-return processes and packaging to verify that devices are shipped in serialized, counterfeit-resistant, and tamper-evident packaging.	*<Report Findings Here>*
5C-1.2.1.4 Devices are tracked during the return process.	
5C-1.2.1.4 Interview responsible personnel and examine device-return records to verify that devices are tracked during the return process.	*<Report Findings Here>*
5C-1.2.1.5 Once received, devices remain in their packaging (as defined in 5C-1.2.1.3) until ready for repair or destruction.	
5C-1.2.1.5 Interview responsible personnel and observe device-return processes to verify that once received, devices remain in their packaging (defined in 5C-1.2.1.3) until ready for destruction.	*<Report Findings Here>*
5C-1.2.2 When decryption devices are removed from service permanently or for repair, all keys and key material, and all account data stored within the device must be rendered irrecoverable. Processes must include the following:	
5C-1.2.2 Verify that documented procedures for removing devices from service include the following: Procedures require that all keys and key material, and all account data stored within the device be securely destroyed. Procedures cover all devices removed from service permanently or for repair. Procedures include 5C-1.2.2.1 through 5C-1.2.2.4 below.	*<Report Findings Here>*
5C-1.2.2.1 Dual control is implemented for all critical decommissioning processes.	
5C-1.2.2.1 Interview personnel and observe processes for removing devices from service to verify dual control is implemented for all critical decommissioning processes.	*<Report Findings Here>*
5C-1.2.2.2 Key and data storage (including account data) are rendered irrecoverable (for example, zeroized). If data cannot be rendered irrecoverable, the device must be physically destroyed to prevent the disclosure of any sensitive data or keys.	

Copyright 2012 PCI Security Standards Council LLC

5C-1.2.2.2 Interview personnel and observe processes for removing devices from service to verify that all key and data storage (including account data) is rendered irrecoverable (for example, zeroized), or that devices are physically destroyed to prevent the disclosure of any sensitive data or keys.	*<Report Findings Here>*
5C-1.2.2.3 Devices being decommissioned are tested and inspected to ensure keys and account data have been rendered irrecoverable.	
5C-1.2.2.3 Interview personnel and observe processes for removing devices from service to verify that tests and inspections of decryption devices are performed to confirm that keys and account data have been rendered irrecoverable.	*<Report Findings Here>*
5C-1.2.2.4 Records of the tests and inspections are maintained for at least one year.	
5C-1.2.2.4 Interview personnel and examine records to verify that records of the tests and inspections (as required in 5C-1.2.2.3) are maintained for at least one year.	*<Report Findings Here>*
5C-1.2.3 Document and log the removal process for the repair or decommissioning of decryption devices.	
5C-1.2.3 For a sample of decryption devices removed for repair or decommissioning, examine records of device removal to verify that the process is documented and logged.	*<Report Findings Here>*
5C-1.2.4 Implement procedures for secure disposal of decryption devices, including return of devices to an authorized party for destruction.	
5C-1.2.4.a Examine documented procedures to verify they include the secure disposal of decryption devices, including return of devices to an authorized party for destruction.	*<Report Findings Here>*
5C-1.2.4.b For a sample of decryption devices removed for disposal, examine records of device removal to verify that devices are returned to an authorized party for destruction.	*<Report Findings Here>*
5C-2 Implement administration procedures for logically securing decryption equipment.	
5C-2.1 Implement procedures to provide secure administration of decryption devices including but not limited to: • Management of user interface • Password/smart card management • Console and non-console administration • Access to physical keys • Use of HSM commands	

Copyright 2012 PCI Security Standards Council LLC

5C-2.1.a Examine documented procedures to verify secure administration procedures are defined for decryption devices including: • Management of user interface • Password/smart card management • Console/remote administration • Access to physical keys • Use of HSM commands	*<Report Findings Here>*
5C-2.1.b Observe authorized personnel performing device-administration operations to verify secure administration procedures are implemented for the following: • Management of user interface • Password/smart card management • Console/remote administration • Access to physical keys • Use of HSM commands	*<Report Findings Here>*
5C-2.2 Implement a process/mechanism to protect the HSM's Application Program Interfaces (APIs) from misuse. *For example, require authentication between the API and the HSM and secure all authentication credentials from unauthorized access. Where an HSM is unable to authenticate access to the API, the process should limit the exposure of the HSM to a host via connection by a dedicated physical link that authorizes access on behalf of the HSM over the trusted channel (for example, high speed serial or dedicated Ethernet).*	
5C-2.2.a Examine documented procedures and processes to verify that a process/mechanism is defined to protect the HSM's Application Program Interfaces (APIs) from misuse.	*<Report Findings Here>*
5C-2.2.b Interview responsible personnel and observe HSM system configurations and processes to verify that the defined process/mechanism is implemented and protects the HSM's Application Program Interfaces (APIs) from misuse.	*<Report Findings Here>*
5C-3 Restrict logical access to decryption devices to authorized personnel.	
5C-3.1 Logical access controls must be implemented to ensure only authorized personnel have access to decryption devices.	
5C-3.1.a Examine documentation to verify that a list of personnel authorized to access decryption devices is defined.	*<Report Findings Here>*
5C-3.1.b For a sample of decryption devices, observe access controls and privilege assignments on decryption devices to verify only authorized personnel (as defined in 5B-3.1.a) have access to the device.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

5C-3.2 Access and permissions must be granted based on least privilege and need to know.	
5C-3.2.a Examine documented access-control policies and procedures to verify that access and permissions must be assigned according to least privilege and need to know.	*<Report Findings Here>*
5C-3.2.b For a sample of decryption devices and personnel, observe configured accounts and permissions, and interview responsible personnel to verify that the level of access and permission granted are according to least privilege and need to know.	*<Report Findings Here>*
5C-4 Provide a mechanism for POI device authentication.	
5C-4.1 POI devices are authenticated upon connection to the decryption environment and upon request by the solution provider. ***Note:*** *This authentication can occur via use of cryptographic keys or certificates, uniquely associated with each POI device and decryption system.*	
5C-4.1.a Examine documented policies and procedures to verify they require POI devices be authenticated upon connection to the decryption environment and upon request by the solution provider.	*<Report Findings Here>*
5C-4.1.b Verify documented procedures are defined for the following: • Procedures and/or mechanisms for authenticating POI devices upon connection to the decryption environment • Procedures and/or mechanisms for authenticating POI devices upon request by the solution provider	*<Report Findings Here>*
5C-4.1.c Interview responsible personnel and observe a sample of device authentications to verify the following: • POI devices are authenticated upon connection to the decryption environment. • POI devices are authenticated upon request by the solution provider.	*<Report Findings Here>*
5C-5 Implement tamper-detection mechanisms.	
5C-5.1 Perform periodic physical inspections of decryption devices at least monthly to detect tampering or modification of devices. Inspections to include: • The device itself • Cabling/connection points • Physically connected devices	

Copyright 2012 PCI Security Standards Council LLC

5C-5.1.a Examine documented procedure to verify that periodic inspection of devices is required at least monthly to detect signs of tampering or modification, and that inspection procedures include: • The device itself • Cabling/connection points • Physically connected devices	*<Report Findings Here>*
5C-5.1.b Interview personnel performing inspections and observe inspection processes to verify that inspections include: • The device itself • Cabling/connection points • Physically connected devices	*<Report Findings Here>*
5C-5.1.c Interview personnel performing inspections and review supporting documentation to verify that physical inspections are performed at least monthly.	*<Report Findings Here>*
5C-6 Documented procedures exist and are demonstrably in use to ensure the security and integrity of decryption devices placed into service, initialized, deployed, used, and decommissioned.	
5C-6.1 All affected parties are aware of required processes and provided suitable guidance on the secure procedures for decryption devices placed into service, initialized, deployed, used, and decommissioned.	
5C-6.1 Examine documented procedures and processes and interview responsible personnel to verify that all affected parties are aware of required processes and are provided suitable guidance on procedures for devices placed into service, initialized, deployed, used, and decommissioned	*<Report Findings Here>*
5C-6.2 Procedures that govern access to decryption devices (HSMs) must be documented, implemented, and known to data-center personnel and any others involved with the physical security of such devices. HSM protections must include at least the following:	
5C-6.2.a Examine documented procedures to verify that procedures are defined to govern access to all HSMs, and include Requirements 5C-6.2.1– 5C-6.2.4 below.	*<Report Findings Here>*
5C-6.2.b Interview data-center personnel and others responsible for the physical security of the devices to verify that the documented procedures are known.	*<Report Findings Here>*
5C-6.2.1 Any physical keys needed to activate the HSM are stored securely.	

Copyright 2012 PCI Security Standards Council LLC

5C-6.2.1 Interview responsible personnel and observe key-storage locations and security controls to verify that any physical keys needed to activate the HSM are stored securely.	*<Report Findings Here>*
5C-6.2.2 If multiple physical keys are needed to activate the HSM: They are assigned to separate designated custodians; and Copies of individual keys are separated and stored such that two authorized individuals are required to gain access to these keys.	
5C-6.2.2 If multiple physical keys are needed to activate the HSM, interview responsible personnel and observe key operations to verify that: Keys are assigned to separate designated custodians; and Copies of individual keys are separated and stored such that two authorized individuals are required to gain access to these keys.	*<Report Findings Here>*
5C-6.2.3 Anti-tamper sensors are enabled as required by the security policy of the HSM.	
5C-6.2.3 Examine HSM security policy and HSM anti-tamper controls to verify that anti-tamper sensors are enabled as required by the security policy of the HSM.	*<Report Findings Here>*
5C-6.2.4 When HSMs are connected to online systems, they are not enabled in a sensitive state. ***Note:*** *A "sensitive state" allows an HSM to perform privileged or sensitive functions that are not available during routine HSM operations. Examples of sensitive functions include but are not limited to: loading of key components, outputting clear-text key components, and altering HSM configuration.*	
5C-6.2.4 Examine HSM configurations and observe processes to verify that HSMs are not enabled in a sensitive state when connected to online systems	*<Report Findings Here>*
5D-1 Perform logging and monitor decryption environment for suspicious activity.	
5D-1.1 Ensure that changes to the critical functions of the decryption devices are logged. ***Note:*** *Critical functions include but are not limited to application and firmware updates, as well as changes to security-sensitive configurations.*	
5D-1.1 Examine system configurations and correlating log files to verify that any changes to the critical functions of decryption devices are logged, including: • Changes to the applications • Changes to the firmware • Changes to any security-sensitive configurations	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

5D-1.2 Implement mechanisms to provide immediate notification of potential security breaches, including but not limited to: • Physical breach • Logical alterations (configuration, access controls) • Disconnect/reconnect of devices • Failure of any device security control • Misuse of the HSM API	
5D-1.2.a Examine documented procedures to verify mechanisms are defined to provide immediate notification of potential security breaches, including: • Physical breach • Logical alterations (configuration, access controls) • Disconnect/reconnect of devices • Failure of any device security control • Misuse of the HSM API	*<Report Findings Here>*
5D-1.2.b Interview personnel and observe implemented mechanisms to verify they provide immediate notification of potential security breaches in the following instances: • Physical breach • Logical alterations (configuration, access controls) • Disconnect/reconnect of devices • Failure of any device security control • Misuse of the HSM API	*<Report Findings Here>*
5D-2 Detect encryption failures.	
5D-2.1 Implement controls to detect encryption failures and provide immediate notification. Controls must include at least the following: ***Note:*** *Although Domain 5 is concerned with the decryption environment, not the encryption environment, it is the duty of the solution provider to actively monitor traffic received into the decryption environment to confirm that the POI equipment in the merchant environment is not outputting clear-text CHD through some error or misconfiguration.*	
5D-2.1 Examine documented procedures to verify controls are defined for the following: • Procedures are defined to detect encryption failures, and include 5D-2.1.1 through 5D-2.1.4 below. • Procedures include immediate notification upon detection of an encryption failure, for each 5D-2.1.1 through 5D-2.1.4 below.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

5D-2.1.1 Checking for incoming clear-text account data.	
5D-2.1.1.a Observe implemented processes to verify controls are in place to check for incoming clear-text account data.	*<Report Findings Here>*
5D-2.1.1.b Observe implemented controls and notification mechanisms, and interview personnel to verify that personnel are immediately notified upon detection of incoming clear-text account data.	*<Report Findings Here>*
5D-2.1.2 Reviewing any decryption errors reported by the HSM, which may be caused by inputting clear-text data when only encrypted data is expected.	
5D-2.1.2.a Observe implemented processes to verify controls are in place to review any decryption errors reported by the HSM, which may be caused by inputting clear-text data when only encrypted data is expected.	*<Report Findings Here>*
5D-2.1.2.b Observe implemented controls and notification mechanisms and interview personnel to verify that personnel are immediately notified upon detection of decryption errors reported by the HSM caused by inputting clear-text data when only encrypted data is expected.	*<Report Findings Here>*
5D-2.1.3 Reviewing any unexpected transaction data received. *For example, transaction data received without an expected authentication data block (such as a MAC or signature).*	
5D-2.1.3.a Observe implemented processes to verify controls are in place to review any unexpected transaction data received.	*<Report Findings Here>*
5D-2.1.3.b Observe implemented controls and notification mechanisms and interview personnel to verify that personnel are immediately notified upon detection of encryption failures in any unexpected transaction data received.	*<Report Findings Here>*
5D-2.1.4 Reviewing data sent by any POI devices that are causing an unusually high rate of transaction authorization rejections.	
5D-2.1.4.a Observe implemented processes to verify controls are in place to review data sent by any POI devices that are causing an unusually high rate of transaction authorization rejections.	*<Report Findings Here>*
5D-2.1.4.b Observe implemented controls and notification mechanisms and interview personnel to verify that personnel are immediately notified upon detection of encryption failures from POI devices that are causing an unusually high rate of transaction authorization rejections.	*<Report Findings Here>*
5D-2.2 Identify source of encryption failure (device, function).	

Copyright 2012 PCI Security Standards Council LLC

5D-2.2.a Examine documented procedures to verify they include procedures for identifying the source of encryption failures.	*<Report Findings Here>*
5D-2.2.b Observe implemented controls and interview personnel to verify that the source of any encryption failures is identified (device, function).	*<Report Findings Here>*
5D-3 Implement incident-response procedures.	
5D-3.1 Implement procedures for responding to security incidents, including the following:	
5D-3.1.1 Implement procedures for responding to tampered devices.	
5D-3.1.1.a Examine documented incident-response procedures to verify that procedures are defined for responding to tampered devices.	*<Report Findings Here>*
5D-3.1.1.b Interview response personnel to verify that procedures for responding to tampered devices are known and implemented.	*<Report Findings Here>*
5D-3.1.2 Implement procedures for responding to missing or substituted devices.	
5D-3.1.2.a Examine documented incident-response procedures to verify that procedures are defined for responding to missing or substituted devices.	*<Report Findings Here>*
5D-3.1.2.b Interview response personnel to verify that procedures for responding to missing or substituted devices are known and implemented.	*<Report Findings Here>*
5D-3.1.3 Implement procedures for responding to unauthorized key-management procedures or configuration changes.	
5D-3.1.3.a Examine documented incident-response procedures to verify that procedures are defined for responding to unauthorized key-management procedures or configuration changes.	*<Report Findings Here>*
5D-3.1.3.b Interview response personnel to verify that procedures for responding to unauthorized key-management procedures or configuration changes are known and implemented.	*<Report Findings Here>*
5D-3.1.4 Implement procedures for responding to disconnect/reconnect of devices.	
5D-3.1.4.a Examine documented incident-response procedures to verify that procedures are defined for responding to disconnect/reconnect of devices.	*<Report Findings Here>*
5D-3.1.4.b Interview response personnel to verify that procedures for responding to disconnect/reconnect of devices are known and implemented.	*<Report Findings Here>*
5D-3.1.5 Implement procedures for responding to failure of any device security control.	

Copyright 2012 PCI Security Standards Council LLC

5D-3.1.5.a Examine documented incident-response procedures to verify that procedures are defined for responding to failure of any device security control.	*<Report Findings Here>*
5D-3.1.5.b Interview response personnel to verify that procedures for responding to failure of any device security control are known and implemented.	*<Report Findings Here>*
5D-3.1.6 Implement procedures for responding to encryption/decryption failures.	
5D-3.1.6.a Examine documented incident-response procedures to verify that procedures are defined for responding to encryption failure.	*<Report Findings Here>*
5D-3.1.6.b Interview response personnel to verify that procedures for responding to encryption failure are known and implemented.	*<Report Findings Here>*
5D-3.2 Procedures must incorporate any response procedures defined by all applicable PCI payment brands, including timeframes for reporting incidents.	
5D-3.2.a Examine documented incident-response procedures to verify that procedures incorporate any response procedures defined by all applicable PCI payment brands, including timeframes for reporting incidents.	*<Report Findings Here>*
5D-3.2.b Interview response personnel to verify that any response procedures defined by all applicable PCI payment brands, including timeframes for reporting incidents, are known and implemented.	*<Report Findings Here>*
5D-4 PCI DSS compliance of decryption environment.	
5D-4.1 Decryption environment must be secured according PCI DSS	
5D-4.1.a Review the "Scope of Work" section of the solution provider's current PCI DSS Report on Compliance (ROC) to verify the PCI DSS assessment scope fully covers the P2PE decryption environment.	*<Report Findings Here>*
5D-4.1.b Review PCI DSS ROC and/or Attestation of Compliance (AOC) to verify that all applicable PCI DSS requirements are "in place" for the P2PE decryption environment.	*<Report Findings Here>*
5D-4.1.c Review PCI DSS ROC and/or Attestation of Compliance (AOC) to verify that the PCI DSS assessment of the P2PE decryption environment was performed by a QSA.	*<Report Findings Here>*
5D-4.1.d Review PCI DSS ROC and/or Attestation of Compliance (AOC) to verify that the P2PE solution provider's decryption environment was assessed as meeting PCI DSS requirements within the previous 12 months.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

Domain 6: P2PE Cryptographic Key Operations

Table 6.1 – Key Matrix. List of all cryptographic keys (by type) used in the P2PE solution						
Key type / description	Description of level in the key hierarchy	Purpose/ function of the key (including types of devices using key)	Key-creation method	How is key distributed – e.g. manually via courier, and/or via remote key distribution (Annex A) and/ or via KIF (Annex B)?*	Types of media used for key storage	Method of key destruction

** Note: Keys distributed by remote key distribution must be included in Annex A; keys distributed via injection must be included in Annex B.*

Table 6.2 – List of devices used to generate keys or key components ***Note:*** *All keys identified in Table 6.1 must be included in Table 6.2.*							
Device name/ identifier	Device Manufacturer/ Model	Type of key(s) generated (per Table 6.1)	Device location	Approved key-generation function (PTS, FIPS, or other approved per NIST SP800-22)	PTS approval number, FIPS approval number, or other certification details	Approved Hardware version #	Approved Firmware version #

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6A-1 Key management, cryptographic algorithms and cryptographic-key lengths must be consistent with international and/or regional standards.	
6A-1.1 Cryptographic keys must be managed in accordance with internationally recognized key-management standards (for example, ISO 11568 (all parts) or ANSI X9.24 (all parts) or equivalent).	
6A-1.1 Interview responsible personnel and examine technical documentation to verify that all keys are managed in accordance with internationally recognized key-management standards—for example, ISO 11568 (all parts) or ANSI X9.24 (all parts) or equivalent.	*<Report Findings Here>*
6A-1.1.1 Account data, cryptographic keys, and components must be encrypted using only approved encryption algorithmsand key lengths, as listed in Appendix A: Minimum Key Sizes and Equivalent Key Strengths.	
6A-1.1.1.a Examine documented key-management policies and procedures to verify that all cryptographic keys use algorithms , and key lengths are in accordance with Appendix A: Minimum Key Sizes and Equivalent Key Strengths.	*<Report Findings Here>*
6A-1.1.1.b Observe key-management operations and devices to verify the following: All cryptographic algorithms and key lengths are in accordance with Appendix A: Minimum Key Sizes and Equivalent Key Strengths.	*<Report Findings Here>*
6A-1.1.2 Cryptographic-key changes must be implemented for keys that have reached the end of their crypto-period (for example, after a defined period of time and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, *NIST Special Publication 800-57*). *See Appendix A: Minimum Key Sizes and Equivalent Key Strengths for minimum required key lengths for commonly used algorithms.*	
6A-1.1.2.a Examine documented key-management procedures to verify: Crypto-periods are defined for every type of key in use. Crypto-periods are based on industry best practices and guidelines (for example, *NIST Special Publication 800-57*). A process/methodology is in place to determine when the crypto-period is reached for each cryptographic key. Cryptographic key changes are implemented whenever a key reaches the end of its defined crypto-period.	*<Report Findings Here>*
6A-1.1.2.b Through observation of key-management operations and inspection of SCDs, verify that crypto-periods are defined for every type of key in use.	*<Report Findings Here>*
6A-1.1.3 Ensure that any key-management requirements of the mode of operation used for encryption of account data are enforced. *For example, if a stream-cipher mode of operation is used, ensure that the same key stream cannot be re-used for different sets of data.*	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6A-1.1.3.a For each mode of operation in use, review the applicable ISO or ANSI standard to identify any key-management requirements for that mode.	*<Report Findings Here>*
6A-1.1.3.b Verify that all such requirements are enforced for each mode of operation	*<Report Findings Here>*
6A-1.1.4 Documentation describing the architecture (including all participating devices and cryptographic protocols), set-up and operation of the key-management solution must exist and must be demonstrably in use for all key-management processes.	
6A-1.1.4.a Verify documentation exists describing the architecture (including all participating devices and cryptographic protocols), set-up and operation of the key-management solution.	*<Report Findings Here>*
6A-1.1.4.b Observe architecture and key-management operations to verify that the documentation reviewed in 6A-1.1.4.a is demonstrably in use for all key-management processes.	*<Report Findings Here>*
6B-1 All keys and key components are generated using an approved random (or pseudo-random) process to ensure the integrity and security of cryptographic systems.	
6B-1.1 Keys must be generated so that it is not feasible to determine that certain keys are more probable than other keys from the set of all possible keys. Cryptographic keys or key components must be generated by one of the following: • An approved key-generation function of a PCI–approved HSM • An approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM • An approved random number generator that has been certified by an independent laboratory to comply with *NIST SP800-22* *Random number generation is critical to the security and integrity of all cryptographic systems. All cryptographic key-generation relies upon good quality, randomly generated values.*	
6B-1.1.a Examine key-management policy document to verify that it requires that all devices used to generate cryptographic keys meet one of the following • An approved key-generation function of a PCI–approved HSM • An approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM • An approved random number generator that has been certified by an independent qualified laboratory according to *NIST SP 800-22*.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6B-1.1.b Examine certification letters or technical documentation to verify that all devices used to generate cryptographic keys or key components meet one of the following: • An approved key-generation function of a PCI–approved HSM • An approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM • An approved random that has been certified by an independent qualified laboratory according to *NIST SP 800-22*	*<Report Findings Here>*
6B-1.1.c Observe device performing key-generation functions to verify that all cryptographic keys or key components are generated using the method that is approved/certified.	*<Report Findings Here>*
6B-2 Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals.	
6B-2.1 Implement security controls, including dual control and tamper protection to prevent the unauthorized disclosure of keys/key components.	
6B-2.1 Perform the following:	
6B-2.1.1 Any clear-text output of the key-generation process must be overseen by at least two authorized individuals who ensure there is no unauthorized mechanism that might disclose a clear-text key or key component as it is transferred between the key-generation SCD and the device or medium receiving the key or key component.	
6B-2.1.1.a Examine documented procedures to verify the following. Any clear-text output of the key-generation process is overseen by at least two authorized individuals. There is no unauthorized mechanism that might disclose a clear-text key or key component between the key-generation device and the device or medium receiving the key or key component.	*<Report Findings Here>*
6B-2.1.1.b Observe key-generation processes and interview responsible personnel to verify: Any clear-text output of the key-generation process is overseen by at least two authorized individuals. There is no unauthorized mechanism that might disclose a clear-text key or key component between the key-generation device and the device or medium receiving the key or key component.	*<Report Findings Here>*
6B-2.1.2 There must be no point in the process where a single individual has the ability to determine, obtain, or ascertain any part of a clear-text key or all the components for a key.	
6B-2.1.2.a Observe the process from end-to-end to verify there is no point in the process where a single person has the ability to determine, obtain, or ascertain any part of a clear-text key or all the components for a key.	*<Report Findings Here>*
6B-2.1.2.b Examine key-generation logs to verify that at least two individuals monitor the key-generation processes.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6B-2.1.3 Key-generation devices must be logged off when not in use.	
6B-2.1.3.a Examine documented procedures for all key-generation methods. Verify procedures require that key-generation devices are logged off when not in use.	*<Report Findings Here>*
6B-2.1.3.b Observe key-generation processes and devices to verify that key-generation devices are logged off when not in use.	*<Report Findings Here>*
6B-2.1.4 Key-generation equipment must not show any signs of tampering (for example, unnecessary cables).	
6B-2.1.4.a Review documented procedures for all key-generation methods to verify they include inspections of the key-generation equipment for evidence of tampering, prior to use.	*<Report Findings Here>*
6B-2.1.4.b Observe key-generation processes for all key types to verify that key-generation equipment is inspected prior to use, to ensure equipment does not show any signs of tampering.	*<Report Findings Here>*
6B-2.1.5 Physical security controls must be used to prevent unauthorized personnel from accessing the key-generation area and observing the key-component/key-generation process.	
6B-2.1.5.a Examine documentation to verify that physical security controls are defined to ensure the key component/key-generation process cannot be observed or accessed by unauthorized personnel.	*<Report Findings Here>*
6B-2.1.5.b Observe the physical security controls to verify that key-component/key-generation process cannot be observed or accessed by unauthorized personnel.	*<Report Findings Here>*
6B-2.2 Multi-use/purpose computing systems shall not be used for key generation where any clear-text secret key or private key, or key component thereof, appears in unprotected memory. *For example, it is not permitted for the cryptographic key to be passed through the memory of a computer that has not been specifically tasked for the sole purpose of key loading. Computers that have been specifically purposed for key loading and are not used for any other purpose are permitted for use if all other requirements can be met. Additionally, this requirement is not intended to include in its scope computers used only for administration of SCDs, or key-generation devices where they have no ability to access clear-text cryptographic keys or components.*	
6B-**2.2.a** Examine documented procedures to verify that multi-purpose computing systems are not used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory.	*<Report Findings Here>*
6B-2.2.b Observe generation process for each type of key to verify that multi-purpose computing systems are not used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6B-2.3 Printed key components must be printed within blind mailers or sealed immediately after printing to ensure that: • Only approved key custodians can observe their own key component. • Tampering can be detected.	
6B-2.3.a Examine documented procedures for printed key components and verify that they require printed key components to be printed within blind mailers or sealed immediately after printing such that: • Only approved key custodians can observe their own key component. • Tampering can be detected.	*<Report Findings Here>*
6B-2.3.b Observe processes for printing key components to verify that key components are printed within blind mailers or sealed immediately after printing, such that no one but the authorized custodian ever has physical access to the output.	*<Report Findings Here>*
6B-2.3.c Observe blind mailers or other sealed containers used for key components to verify that tampering can be detected.	*<Report Findings Here>*
6B-2.4 Any residue that may contain clear-text keys or components must be destroyed immediately after generation of that key to prevent disclosure of a key or key component. *Examples of where such key residue may exist include (but are not limited to):* • *Printing material, including ribbons and paper waste* • *Memory storage of a key-loading device, after loading the key to a different device or system* • *Other types of displaying or recording*	
6B-2.4.a Examine documented procedures to identify all locations where key residue may exist. Verify procedures are implemented to ensure the following: • Any residue that may contain clear-text keys or components is destroyed immediately after generation. • If a key is generated in a separate device before being exported into the end-use device, the key and all related critical security parameters (e.g., secret seeds) are deleted (zeroized) from the generation and/or injection device immediately after the transfer to the device that will use the key.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6B-2.4.b Observe the destruction process of the identified key residue and verify the following: • Any residue that may contain clear-text keys or components is destroyed immediately after generation. • If a key is generated in a separate device before being exported into the end-use device, the key and all related critical security parameters (e.g., secret seeds) are deleted (zeroized) from the generation and/or injection device immediately after the transfer to the device that will use the key.	*<Report Findings Here>*
6B-2.5 Policy and procedures must ensure the following is not performed: • Dictate keys or components • Record key or component values on voicemail • Fax, e-mail, or otherwise convey clear-text keys or components • Write key or component values into startup instructions • Tape key or component values to or inside devices • Write key or component values in procedure manuals	
6B-2.5.a Examine documented policy and procedures to verify that key components are prohibited from being transmitted across insecure channels, including but not limited to: • Dictating keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text keys or components • Writing key or component values into startup instructions • Taping key or component values to or inside devices • Writing key or component values in procedure manual	*<Report Findings Here>*
6B-2.5.b From observation of key-management processes verify that key components are not transmitted across insecure channels, including but not limited to: • Dictating keys or components • Recording key or component values on voicemail • Faxing, e-mailing, or otherwise conveying clear-text keys or components • Writing key or component values into startup instructions • Taping key or component values to or inside devices • Writing key or component values in procedure manual	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6B-3 Documented procedures must exist and must be demonstrably in use for all key-generation processing.	
6B-3.1 Written key-generation procedures must exist and be known by all affected parties (key custodians, supervisory staff, technical management, etc.).	
6B-3.1.a Examine documented key-generation procedures to confirm that they include all aspects of key-generation operations.	*<Report Findings Here>*
6B-3.1.b Interview those responsible for the key-generation processes (including key custodians, supervisory staff, technical management, etc.) to verify that the documented procedures are known and understood by all affected parties.	*<Report Findings Here>*
6B-3.1.c Observe key-generation ceremonies and verify that the documented procedures are demonstrably in use.	*<Report Findings Here>*
6B-3.2 All key-generation events must be logged. *Keys that are generated on the POI device do not need to generate an audit-log entry, but the creation of any keys to decrypt data sent from such a POI must be logged at the solution provider.*	
6B-3.2.a Examine documented key-generation procedures to verify that all key-generation events must be logged.	*<Report Findings Here>*
6B-3.2.b Observe demonstrations for all types of key-generation events to verify that all key-generation events are logged.	*<Report Findings Here>*
6B-3.2.c Examine logs of key generation to verify that all events have been recorded.	*<Report Findings Here>*
6C-1 Cryptographic keys must be conveyed or transmitted securely.	
6C-1.1 No single person can ever have access to more than one component of a particular cryptographic key. A person with access to one component/share of a key, or to the media conveying this component/share, must not have access to any other component/share of this key or to any other medium conveying any other component of this key.	
6C-1.1.a Examine documented procedures to verify they include controls to ensure that no single person can ever have access to more than one component of a particular cryptographic key. Verify procedures include: • Any person with access to one component/share of a key must not have access to any other component/share of this key, or to any other medium conveying any other component of this key. • Any person with access to the media conveying a component/share of a key must not have access to any other component/share of this key, or to any other medium conveying any other component of this key.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6C-1.1.b Observe key-transfer processes and interview personnel to verify that controls are implemented to ensure that no single person can ever have access to more than one component of a particular cryptographic key. Verify the implemented controls ensure the following: • An individual with access to a key component or key share does not have access to any other component/share of this key or to any other medium conveying any other component of this key. • Any person with access to the media conveying a key component or key share must not have access to any other component/share of this key or to any other medium conveying any other component of this key.	*<Report Findings Here>*
6C-1.2 Components of cryptographic keys must be transferred using different communication channels, such as different courier services. ***Note:*** *It is not sufficient to send key components for a specific key on different days using the same communication channel.*	
6C-1.2.a Examine documented procedures to verify that cryptographic-key components are transferred using different communications channels.	*<Report Findings Here>*
6C-1.2.b Examine records of key transfers and interview responsible personnel to verify that cryptographic key components are transferred using different communications channels.	*<Report Findings Here>*
6C-1.3 Ensure that the method used does not allow any personnel to have access to all components—for example, key custodians, mail room and courier staff.	
6C-1.3.a Examine documented procedures and interview responsible personnel to verify that the method used does not allow for any personnel to have access to all components.	*<Report Findings Here>*
6C-1.3.b Observe the method used to transport key components to verify that the method does not allow for any personnel to have access to all components.	*<Report Findings Here>*
6C-1.4 Where key components are transmitted in clear-text using tamper-evident mailers, ensure that details of the serial number of the package are transmitted separately from the package itself.	
6C-1.4 If key components are ever transmitted in clear-text using tamper-evident mailers, perform the following:	*<Report Findings Here>*
6C-1.4.a Examine documented procedures to verify they define how details of the serial number are transmitted separately from the package itself.	*<Report Findings Here>*
6C-1.4.b Observe the method used to transport clear-text key components using tamper-evident mailers and interview responsible personnel to verify that details of the serial number of the package are transmitted separately from the package itself.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6C-1.5 Public keys must be conveyed in a manner that protects their integrity and authenticity. Examples of acceptable methods include: • Use of a key check value that can be verified using a separate channel • Use of public-key certificates created by a trusted C • A hash of the public key sent by a separate channel (for example, mail or phone) • A new public-key certificate signed by an existing authenticated key ***Note:*** *Self-signed certificates must not be used as the sole method of authentication.*	
6C-1.5 For all methods used to convey public keys, perform the following:	
6C-1.5.a Examine documented procedures for conveying public keys to verify that methods are defined to convey public keys in a manner that protects their integrity and authenticity.	*<Report Findings Here>*
6C-1.5.b Observe the process for conveying public keys and interview responsible personnel to verify that the implemented method ensures public keys are conveyed in a manner that protects their integrity and authenticity.	*<Report Findings Here>*
6C-1.5.c Verify that the mechanism used to validate the integrity and authenticity of the public key is independent of the conveyance method.	*<Report Findings Here>*
6C-2 Key components must be protected at all times during transmission, conveyance, or movement between locations.	
6C-2.1 Any single clear-text key component must at all times be either: • Under the continuous supervision of a person with authorized access to this component, or • In one of the approved forms listed in 6F-1.1.	
6C-2.1.a Examine documented procedures for transmission, conveyance, or movement of keys between any two locations to verify that any single clear-text key component must at all times be either: • Under the continuous supervision of a person with authorized access to this component, or • In one of the approved forms listed in 6F-1.1.	*<Report Findings Here>*
6C-2.1.b Observe key-management processes and interview responsible personnel to verify processes are implemented to ensure that any single clear-text key component is at all times either: • Under the continuous supervision of a person with authorized access to this component, or • In one of the approved forms listed in 6F-1.1.	*<Report Findings Here>*
6C-2.2 Packaging or mailers containing clear-text key components are examined for evidence of tampering before being used.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6C-2.2.a Verify documented procedures include requirements for all packaging or mailers containing clear-text key components to be examined for evidence of tampering before being used.	*<Report Findings Here>*
6C-2.2.b Interview responsible personnel and observe process to verify that all packaging or mailers containing clear-text key components are examined for evidence of tampering before being used.	*<Report Findings Here>*
6C-2.2.1 Any sign of package tampering must result in the destruction and replacement of: The set of components Any keys encrypted under this (combined) key	
6C-2.2.1.a Verify documented procedures require that any sign of package tampering results in the destruction and replacement of both: The set of components Any keys encrypted under this (combined) key	*<Report Findings Here>*
6C-2.2.1.b Interview responsible personnel and observe process to verify that, if a package shows signs of tampering, processes are implemented that result in the destruction and replacement of both: The set of components Any keys encrypted under this (combined) key	*<Report Findings Here>*
6C-2.3 No one but the authorized key custodian (and designated backup(s)) shall have physical access to a key component prior to transmittal or upon receipt of a component.	
6C-2.3.a Verify that a list(s) of key custodians (and designated backup(s)) that are authorized to have physical access to key components prior to transmittal or upon receipt of a component is defined and documented.	*<Report Findings Here>*
6C-2.3.b Observe implemented access controls and processes to verify that only those authorized key custodians (and designated backup(s)) have physical access to key components prior to transmittal or upon receipt.	*<Report Findings Here>*
6C-2.3.c Examine physical access logs (e.g., to security containers for key components) to verify that only the authorized individual(s) have access to each component.	*<Report Findings Here>*
6C-2.4 Mechanisms must exist to ensure that only authorized custodians: • Place key components into tamper-evident packaging for transmittal. • Open tamper-evident packaging containing key components upon receipt. • Check the serial number of the tamper-evident packing upon receipt of a component package.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6C-2.4.a Verify that a list(s) of key custodians authorized to perform the following activities is defined and documented: • Place the key component into tamper-evident packaging for transmittal. • Open tamper-evident packaging containing the key component upon receipt. • Check the serial number of the tamper-evident packing upon receipt of a component package.	*<Report Findings Here>*
6C-2.4.b Observe implemented mechanisms and processes to verify that only the authorized key custodians can perform the following: • Place the key component into tamper-evident packaging for transmittal. • Open tamper-evident packaging containing the key component upon receipt. • Check the serial number of the tamper-evident packing upon receipt of a component package.	*<Report Findings Here>*
6C-3 Documented procedures must exist and must be demonstrably in use for all key transmission and conveyance processing.	
6C-3.1 Written procedures must exist and be known to all affected parties.	
6C-3.1.a Verify documented procedures exist for all key transmission and conveyance processing.	*<Report Findings Here>*
6C-3.1.b Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for key transmission and conveyance processing.	*<Report Findings Here>*
6C-3.2 Methods used for the conveyance or receipt of keys must be documented.	
6C-3.2 Verify documented procedures include all methods used for the conveyance or receipt of keys.	*<Report Findings Here>*
6D-1 Unencrypted secret or private keys must be entered into cryptographic devices using the principles of dual control and split knowledge.	
6D-1.1 The loading of clear-text cryptographic keys, including public keys, requires dual control to authorize any key-loading session. *For example: Dual control can be implemented using two or more passwords of five characters or more, multiple cryptographic tokens (such as smartcards), or physical keys.*	
6D-1.1.a Examine documented procedures for loading of clear-text cryptographic keys, including public keys, to verify they require dual control to authorize any key-loading session.	*<Report Findings Here>*
6D-1.1.b For all types of SCDs, observe processes for loading clear-text cryptographic keys, including public keys, to verify that dual control is required to authorize any key-loading session.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6D-1.1.c Examine documented records of key-loading processes to verify the presence of two authorized persons during each type of key-loading activity.	*<Report Findings Here>*
6D-1.1.d Ensure that any default dual-control mechanisms (e.g., default passwords—usually printed in the vendor's manual)—in a key-loading device have been disabled or changed.	*<Report Findings Here>*
6D-1.2 For loading of secret or private cryptographic keys, split knowledge is enforced by either: • Manual entry of the key as multiple key-components, using a different custodian for each component • The use of a key-loading device managed under dual control ***Note:*** *Manual key loading may involve the use of media such as paper, magnetic stripe or smart cards, or other physical tokens.*	
6D-1.2.a Examine documented procedures for loading of secret and private cryptographic keys to verify they require split knowledge be enforced through: • Manual entry of the key as multiple-key components, using a different custodian for each component • The use of a key-loading device managed under dual control	*<Report Findings Here>*
6D-1.2.b For all types of SCDs, observe processes for loading secret and private cryptographic keys to verify that split knowledge is enforced through: • Manual entry of the key as multiple-key components, using a different custodian for each component • The use of a key-loading device managed under dual control	*<Report Findings Here>*
6D-1.3 For any given set of key components, each device shall compose the same final key from the reverse of the process used to create the components.	
6D-1.3 Through examination of documented procedures, interviews, and observation confirm that any devices that are loaded with the same key components use the same mathematical process to derive the final key, and that this is the reverse of the process used to create the key components.	*<Report Findings Here>*
6D-1.4 If key-establishment protocols using public-key cryptography are used to distribute secret keys, these must meet the requirements detailed in Annex A of this document.	
6D-1.4 If key-establishment protocols using public-key cryptography are used to distribute secret keys, verify that the requirements detailed in Annex A of this document are met.	*<Report Findings Here>*
6D-1.5 If keys are injected into a POI either by the solution provider or a third-party key-injection facility (KIF), these must also meet the additional requirements set out in Annex B of this document.	
6D-1.5 If POI keys are injected in a key-injection facility (KIF), verify that the KIF also meets the additional requirements set out in Annex B of this document.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6D-2 The mechanisms used to load secret and private keys—such as terminals, external PIN pads, key guns, or similar devices and methods—must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.	
6D-2.1 Clear-text secret and private keys and key components must be transferred into a cryptographic device only when it can be ensured that: • Any cameras in the environment are positioned to ensure they cannot monitor the entering of clear-text key components. • There is no unauthorized mechanism at the interface between the conveyance medium and the cryptographic device that might disclose the transferred keys. • The device has not been subject to any prior tampering that could lead to the disclosure of keys or account data.	
6D-2.1 Observe key-loading environments, processes, and mechanisms (for example, terminals, PIN pads, key guns, etc.) used to transfer keys and key components. Perform the following:	*<Report Findings Here>*
6D-2.1.a Ensure cameras are positioned to ensure they cannot monitor the entering of clear-text key components.	*<Report Findings Here>*
6D-2.1.b Verify that keys and components are transferred into a cryptographic device only after an inspection of the devices and mechanism ensures: • There is no unauthorized mechanism at the interface between the conveyance medium and the cryptographic device that might disclose the transferred keys. • The device has not been subject to any prior tampering that could lead to the disclosure of keys or account data.	*<Report Findings Here>*
6D-2.2 The injection of secret or private key components from electronic medium to a cryptographic device (and verification of the correct receipt of the component, if applicable) results in either of the following: • The medium is placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-insertion of the component into the cryptographic device); or • All traces of the component are erased or otherwise destroyed from the electronic medium.	
6D-2.2.a Examine documented procedures for the injection of secret or private key components from electronic medium to a cryptographic device. Verify procedures define specific instructions to be followed as a result of key injection, including: • Instructions for the medium to be placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-insertion of the component into the cryptographic device); or • Instructions to erase or otherwise destroy all traces of the component from the electronic medium.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6D-2.2.b Observe key-injection processes to verify that the injection process results in one of the following: • The medium used for key injection is placed into secure storage and managed under dual control (only if there is a possibility it will be required for future re-insertion of the component into the cryptographic device); or • All traces of the component are erased or otherwise destroyed from the electronic medium.	*<Report Findings Here>*
6D-2.3 For electronic key-loading devices used to inject keys into POIs, the following must be in place:	
6D-2.3 Review documented procedures and observe processes for the use of key-loading devices. Perform the following:	*<Report Findings Here>*
6D-2.3.1 The key-loading device is a physically secure SCD, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected.	
6D-2.3.1 Verify the key-loading device is a physically secure SCD, designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected.	*<Report Findings Here>*
6D-2.3.2 The key-loading device is under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it.	
6D-2.3.2 Verify the key-loading device is under the supervision of a person authorized by management, or stored in a secure container such that no unauthorized person can have access to it.	*<Report Findings Here>*
6D-2.3.3 The key-loading device is designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD. Such personnel must ensure that a key-recording device is not inserted between the SCDs.	
6D-2.3.3.a Verify the key-loading device is designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another SCD.	*<Report Findings Here>*
6D-2.3.3.b Verify that authorized personnel inspect the key-loading device, prior to use to ensure that a key-recording device has not been inserted between the SCDs.	*<Report Findings Here>*
6D-2.3.4 The key-loading device does not retain any information that might disclose the key or a key that it has successfully transferred.	
6D-2.3.4 Verify the key-loading device does not retain any information that might disclose the key or a key that it has successfully transferred.	*<Report Findings Here>*
6D-2.4 Any media (electronic or otherwise) containing secret or private key components used for loading cryptographic keys must be maintained in a secure location and accessible only to authorized custodian(s).	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6D-2.4.a Inspect all media (electronic or otherwise) containing key components used in the loading of cryptographic keys to verify that any such media is maintained in a secure location.	*<Report Findings Here>*
6D-2.4.b Interview personnel and observe media locations to verify that the media is accessible only to custodian(s) authorized to access the key components.	*<Report Findings Here>*
6D-2.5 When removed from secure storage, media or devices containing key components or used for the injection of clear-text cryptographic keys must be in the physical possession of only the designated component holder(s), and only for the minimum practical time necessary to complete the key-loading process. *Key components that can be read/displayed (for example, those printed on paper or stored on magnetic cards, PROMs, or smartcards) must be managed so they are visible only at one point in time to only one designated key custodian,*	
6D-2.5.a Examine documented procedures for removing media or devices containing key components, or that are otherwise used for the injection of cryptographic keys, from secure storage. Verify procedures include the following: • Requirement that media / devices be in the physical possession of only the designated component holder(s). • The media/ devices are removed from secure storage only for the minimum practical time necessary to complete the key-loading process.	*<Report Findings Here>*
6D-2.5.b Interview designated component holder(s) and examine key-management logs to verify that media or devices removed from secure storage are in the physical possession of only the designated component holder.	*<Report Findings Here>*
6D-2.5.c Interview key-injection personnel and examine logs for the removal of media/devices from secure storage to verify they are removed only for the minimum practical time necessary to complete the key-loading process.	*<Report Findings Here>*
6D-2.6 Written or printed key component must not be opened until immediately prior to use.	
6D-2.6.a Review documented procedures and confirm that printed/written key components are not opened until immediately prior to use.	*<Report Findings Here>*
6D-2.6.b Observe key-loading processes and verify that printed/written key components are not opened until immediately prior to use.	*<Report Findings Here>*
6D-3 All hardware and access/authentication mechanisms used for key loading or the signing of authenticated applications (for example, for "whitelists") must be managed under dual control.	
6D-3.1 Any hardware and passwords used in the key-loading function or for the signing of authenticated applications must be controlled and maintained in a secure environment under dual control. ***Note:*** *Where key-loading is performed for POIs, the secure environment is defined in Annex B.*	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6D-3.1.a Examine documented procedures to verify they require the following: • Any hardware used in the key-loading function or for the signing of authenticated applications must be controlled and maintained in a secure environment under dual control. • Any passwords used in the key-loading function or for the signing of authenticated applications must be controlled and maintained in a secure environment under dual control.	*<Report Findings Here>*
6D-3.1.b Observe key-loading environments and controls to verify the following: • All hardware used in the key-loading function or for the signing of authenticated applications is controlled and maintained in a secure environment under dual control. • All passwords used for key-loading functions and for the signing of authenticated applications are controlled and maintained in a secure environment under dual control.	*<Report Findings Here>*
6D-3.1.1 Dual-control practices must be specified in emergency procedures and in place during emergency situations. ***Note:*** *Emergency procedures may include but are not limited to incident-response and disaster-recovery procedures.*	
6D-3.1.1.a Examine documented emergency procedures to verify dual-control practices are specified in emergency procedures.	*<Report Findings Here>*
6D-3.1.1.b Interview responsible personnel to verify that dual-control practices are maintained during emergency situations.	*<Report Findings Here>*
6D-3.1.2 Default dual-control mechanisms must be changed.	
6D-3.1.2.a Verify that documented procedures require default dual-control mechanisms be changed.	*<Report Findings Here>*
6D-3.1.2.b Interview personnel and observe dual-control mechanisms for key-loading functions to verify there are no default dual-control mechanisms (for example, default passwords) used for key loading or the signing of authenticated applications.	*<Report Findings Here>*
6D-3.2 All cable attachments must be examined before each key-loading or signing operation to ensure they have not been tampered with or compromised.	
6D-3.2.a Review documented procedures to ensure they require that cable attachments be examined prior to key-loading function or signing operation.	*<Report Findings Here>*
6D-3.2.b Observe key-loading processes to verify that all cable attachments are properly examined prior to a key-loading function or signing operation.	*<Report Findings Here>*
6D-3.3 Any physical tokens used to enable key loading or the signing of authenticated applications—for example, physical (brass) keys, or smartcards—must not be in the control or possession of any one individual who could use those tokens to load secret cryptographic keys or sign applications under single control.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6D-3.3.a Examine documented procedures for the use of physical tokens to enable key loading or the signing of authenticated applications. Verify procedures require that physical tokens must not be in the control or possession of any one individual.	*<Report Findings Here>*
6D-3.3.b Inspect locations and controls for physical tokens to verify that tokens used to enable key loading or the signing of authenticated applications are not in the control or possession of any one individual.	*<Report Findings Here>*
6D-3.4 Use of the equipment must be monitored and a log of all key-loading and application-signing activities maintained for audit purposes.	
6D-3.4.a Observe key-loading and application-signing activities to verify that use of the equipment is monitored.	*<Report Findings Here>*
6D-3.4.b Verify logs of all key-loading and application-signing activities are maintained.	*<Report Findings Here>*
6D-4 The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.	
6D-4.1 A cryptographic-based validation mechanism is in place to ensure the authenticity and integrity of keys and components (for example, testing key check values, hashes, or other similar unique values that are based upon the keys or key components being loaded).	
6D-4.1.a Examine documented procedures to verify a cryptographic-based validation mechanism is in place to ensure the authenticity and integrity of keys and components.	*<Report Findings Here>*
6D-4.1.b Observe the key-loading processes to verify that the defined cryptographic-based validation mechanism used to ensure the authenticity and integrity of keys and components is being used.	*<Report Findings Here>*
6D-4.1.1 Methods used for key validation are consistent with ISO 11568 and prevent exposure of the actual key values.	
6D-4.1.1.a Verify that the methods used for key validation are consistent with ISO 11568 (for example, if check values are used, they should return a value of no more than 4-6 hexadecimal characters).	*<Report Findings Here>*
6D-4.1.1.b Verify that the implemented methods prevent exposure of the actual key values.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6D-4.2 Public keys must only be stored in the following approved forms: • Within a certificate, • Within a secure cryptographic device, • Encrypted using strong cryptography, or • Authenticated with strong cryptography using one of the following methods: ○ ISO16608-2004 compliant MAC ○ NIST SP800-38B CMAC ○ PKCS #7 compliant public-key signature	
6D-4.2.a Interview personnel and review documented procedures to verify that all public keys exist only in an approved form.	*<Report Findings Here>*
6D-4.2.b Observe public-key stores and mechanisms to verify that public keys exist only in an approved form.	*<Report Findings Here>*
6D-4.2.1 Procedures exist to ensure the integrity and authenticity of public keys prior to storage (for example, during transmission as part of a certificate request operation).	
6D-4.2.1.a Interview personnel and review documentation to verify that procedures exist to ensure the integrity and authenticity of public keys prior to storage.	*<Report Findings Here>*
6D-4.2.1.b Observe public-key transmissions and processes to verify the implemented procedures ensure the integrity and authenticity of public keys prior to storage.	*<Report Findings Here>*
6D-5 Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities.	
6D-5.1 Procedures must be documented for all key-loading operations, be known to all affected parties and demonstrably be in use.	
6D-5.1.a Verify documented procedures exist for all key-loading operations.	*<Report Findings Here>*
6D-5.1.b Interview responsible personnel to verify that the documented procedures are known and understood by all affected parties for all key-loading operations.	*<Report Findings Here>*
6D-5.1.c Observe key-loading process and verify that the documented procedures are demonstrably in use.	*<Report Findings Here>*
6D-5.2 Audit trails must be in place for all key-loading events.	
6D-5.2 Examine log files and observe logging processes to verify that audit trails are in place for all key-loading events.	*<Report Findings Here>*
6E-1 Unique secret cryptographic keys must be in use for each identifiable link between encryption and decryption points.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6E-1.1 Where two organizations share a key for securing account data (including a key-encryption key used to encrypt a data-encryption key), that key must meet the following: • Be unique to those two entities and • Not be given to, or used by, any other entity.	
6E-1.1.a Examine the documented key matrix and operational procedures and interview personnel to determine whether any keys are shared between organizations. For all keys shared between two organizations (including data-encryption keys for account data, and key-encryption keys used to encrypt a data-encryption key) perform the following:	*<Report Findings Here>*
6E-1.1.b Obtain key check values for any master file keys to verify key uniqueness between the two organizations. If a remote key-establishment and distribution scheme is implemented between networks, examine public keys and/or hash values and/or fingerprints of the keys to verify key uniqueness of the asymmetric-key pairs.	*<Report Findings Here>*
6E-1.1.c For internally developed systems, review system-design documentation or source code for uniqueness of cryptograms and/or hash values/fingerprints and/or public keys.	*<Report Findings Here>*
6E-1.1.d For application packages, examine parameter files where the cryptograms of keys shared with other network nodes are specified. If a remote key-establishment and distribution scheme is implemented between networks, examine the parameter files where the public keys of keys shared with other network nodes are specified and ensure the correct number of public keys exist (a unique one for each network link implemented).	*<Report Findings Here>*
6E-1.1.e Compare key check values against those for known or default keys to verify that known or default key values are not used.	*<Report Findings Here>*
6E-1.2 Key-generation keys (such as a base derivation key) that are used to derive multiple keys for different devices must never be output from a secure cryptographic device in clear text.	
6E-1.2.a Examine documented procedures to confirm that key-generation keys (such as a base derivation key), that are used to derive multiple keys for different devices, are never output from a secure cryptographic device in clear text.	*<Report Findings Here>*
6E-1.2.b Observe the process for managing key-generation keys (such as a base derivation key), that are used to derive multiple keys for different devices, to ensure they are never output from a secure cryptographic device in clear text.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6E-2 Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another key or the operation of any cryptographic device without legitimate keys.	
6E-2.1 The unauthorized replacement or substitution of one stored key for another or the replacement or substitution of any portion of a key, whether encrypted or unencrypted, must be prevented or detected.	
6E-2.1 Examine documented procedures and technical documentation to confirm that procedures exist to prevent or detect • The unauthorized replacement or substitution of any stored key for another • The replacement or substitution of any portion of a key, whether encrypted or unencrypted	*<Report Findings Here>*
6E-2.1.1 TDEA cryptographic keys must be managed as key bundles (for example, using ANSI TR-31) at all times when external to an SCD. Management of key bundles and the individual keys must include: Assurance of key integrity Appropriate usage as specified by the particular mode Preventing manipulation of individual keys Keys cannot be unbundled for any purpose	
6E-2.1.1.a Examine documented procedures and observe key operations to verify that secret cryptographic keys are managed as key bundles at all times.	*<Report Findings Here>*
6E-2.1.1.b Verify that key bundles and the individual keys are managed as follows: Key integrity ensures that each key in the bundle has not been altered in an unauthorized manner since the time it was generated, transmitted, or stored by an authorized source. Keys are used in the appropriate order as specified by the particular mode. Key bundles are a "fixed quantity," such that an individual key cannot be manipulated while leaving the other two keys unchanged; and Key bundles cannot be unbundled for any purpose.	*<Report Findings Here>*
6E-2.2 Documented procedures must exist and be demonstrably in use describing how the replacement and/or substitution of one key for another is prevented. These procedures must specifically include the following:	
6E-2.2 Verify documented procedures exist defining how the replacement and/or substitution of one key for another is prevented, including 6E-2.2.1 through 6E-2.2.4, below. Perform the following:	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6E-2.2.1 HSMs (including CA's HSMs) must not remain in a "sensitive" state when connected to online production systems. ***Note:*** *A "sensitive state" allows an HSM to perform privileged or sensitive functions that are not available during routine HSM operations. Examples of sensitive functions include but are not limited to: loading of key components, outputting clear-text key components, and altering HSM configuration.*	
6E-2.2.1.a Examine HSMs to ensure they do not remain in a "sensitive" state when connected to online production systems.	*<Report Findings Here>*
6E-2.2.1.b If a CA is used, examine the CA's HSMs and observe CA process to ensure that HSMs do not remain in the "sensitive" state when connected to online production systems.	*<Report Findings Here>*
6E-2.2.2 Keys no longer needed are destroyed.	
6E-2.2.2 Verify that keys no longer needed are destroyed.	*<Report Findings Here>*
6E-2.2.3 Procedures for monitoring and alerting to the presence of multiple cryptographic synchronization errors, including the following: Specific actions that determine whether the legitimate value of the cryptographic key has changed. (For example, encryption of a known value to determine whether the resulting cryptogram matches the expected result.) Proactive safeguards that shut down the source of any synchronization errors and start an investigative process to determine the true cause of the event.	
6E-2.2.3.a Verify procedures have been implemented for monitoring and alerting to the presence of multiple cryptographic synchronization errors.	*<Report Findings Here>*
6E-2.2.3.b Verify that implemented procedures include: Specific actions that determine whether the legitimate value of the cryptographic key has changed. (For example, encryption of a known value to determine whether the resulting cryptogram matches the expected result.) Proactive safeguards that shut down the source of any synchronization errors and start an investigative process to determine the true cause of the event.	*<Report Findings Here>*
6E-2.2.4 Physical and logical controls exist over the access to and use of SCDs used to create cryptograms to prevent misuse	
6E-2.2.4.a Verify physical controls exist over the access to and use of devices used to create cryptograms.	*<Report Findings Here>*
6E-2.2.4.b Verify logical controls exist over the access to and use of devices used to create cryptograms.	*<Report Findings Here>*
6E-2.3 Key-component documents and their packaging that show signs of tampering must result in the destruction and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6E-2.3.a Verify procedures are documented for the following: • Key-component documents showing signs of tampering must result in the destruction and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist. • Key-component packaging showing signs of tampering must result in the destruction and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.	*<Report Findings Here>*
6E-2.3.b Interview personnel and observe processes to verify procedures are implemented as follows: • Key-component documents showing signs of tampering result in the destruction and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist. • Key-component packaging showing signs of tampering results in the destruction and invalidation of all associated key components and the resultant cryptographic key(s) at all locations where they exist.	*<Report Findings Here>*
6E-3 Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.	
6E-3.1 To limit the magnitude of exposure should any key(s) be compromised, and to significantly strengthen the security of the underlying system, the device must enforce the following practices:	
6E-3.1.1 Cryptographic keys must only be used for the purpose they were intended—for example, key-encryption keys must not be used as data-encryption keys, PIN keys must not be used for account-data encryption, and these keys must not be used to encrypt any arbitrary data (data that is not account data).	
6E-3.1.1.a Examine key-management documentation and interview key custodians to verify that cryptographic keys are defined for a specific purpose.	*<Report Findings Here>*
6E-3.1.1.b Observe cryptographic devices and key-management processes to verify that cryptographic keys are used only for the defined purpose for which they were intended.	*<Report Findings Here>*
6E-3.1.2 Master keys (and any variants or keys derived from master keys) used by host processing systems for encipherment of keys for local storage are not used for other purposes—for example, key conveyance between platforms that are not part of the same logical configuration.	
6E-3.1.2 Observe cryptographic devices and key-management processes to verify that master keys—and any variants or keys derived from master keys—used for encipherment of keys for local storage are not used for other purposes.	*<Report Findings Here>*
6E-3.1.3 Account data keys, key-encipherment keys, and PIN-encryption keys have different values. *Ensuring key purpose is an essential part of key management, and compromise of key purpose can render even strong cryptography invalid. Review of HSM commands used to access keys for decryption of data will often show if keys are being misused; for example, where a key that is designed for account-data encryption is used to decrypt other data as well.*	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6E-3.1.3.a Examine key-management documentation and interview key custodians to verify that account data keys, key-encipherment keys, and PIN-encryption keys must have different values.	*<Report Findings Here>*
6E-3.1.3.b Observe key-generation processes and a sample of key check values to verify that account data keys, key-encipherment keys, and PIN-encryption keys must have different values.	*<Report Findings Here>*
6E-3.2 To limit the magnitude of exposure should any key(s) be compromised and to significantly strengthen the security of the underlying system, the following practices must be enforced for private/public keys:	
6E-3.2.1 Private keys must only be used as follows: To create digital signatures ***or*** to perform decryption operations. For a single purpose—a private key must only be used for either decryption or for creating digital signatures, but not both (except for transaction-originating SCDs).	
6E-3.2.1 Examine key-management documentation and interview key custodians to verify that private keys are only used: To create digital signatures ***or*** to perform decryption operations. For a single purpose—a private key must only be used for either decryption or for creating digital signatures, but not both.	*<Report Findings Here>*
6E-3.2.2 Public keys must only be used as follows: To perform encryption operations ***or*** to verify digital signatures. For a single purpose—a public key must only be used for either encryption or for verifying digital signatures, but not both (except for transaction-originating devices).	
6E-3.2.2 Examine key-management documentation and interview key custodians to verify that public keys are only used: To perform encryption operations ***or*** to verify digital signatures. For a single purpose—a public key must only be used for either encryption or for verifying digital signatures, but not both.	*<Report Findings Here>*
6E-3.3 Keys must never be shared or substituted between production and test systems. • Production keys must never be present or used in a test system, and • Test keys must never be present or used in a production system.	
6E-3.3.a Examine key-management documentation and interview key custodians to verify that cryptographic keys are never shared or substituted between production and development systems.	*<Report Findings Here>*
6E-3.3.b Observe processes for generating and loading keys into in production systems to ensure that they are in no way associated with test or development keys.	*<Report Findings Here>*
6E-3.3.c Observe processes for generating and loading keys into in test systems to ensure that they are in no way associated with production keys.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6E-3.3.d Compare check, hash, cryptogram, or fingerprint values for production and development keys to verify that development and test keys have different key values.	*<Report Findings Here>*
6E-4 All secret and private keys must be unique (except by chance) to that device.	
6E-4.1 All cryptographic keys that have ever been used in a transaction-originating POI device to encrypt account data or to protect account-data keys through encryption, must be: • Known only to a single POI device, and • Known only to HSMs in the solution provider's decryption environment for that POI device, at the minimum number of facilities consistent with effective system operations. *Disclosure of the key in one such device must not provide any information that could be feasibly used to determine the key in any other such device.* *The requirement for unique private and secret keys includes all keys that are used to secure account data or to provide security to account-data keys. This includes not only the account-data keys themselves, but also any KEKs, master keys, or any secret and private keys used to sign firmware updates or for other device-management operations.*	
6E-4.1.a Examine documented procedures for the generation, loading, and usage of all keys used in transaction-originating POI devices. Verify the procedures ensure that all keys used in transaction-originating POI devices are: • Known only to a single POI device, and • Known only to one or more HSMs in the solution provider's decryption environment for that POI device, at the minimum number of facilities consistent with effective system operations.	*<Report Findings Here>*
6E-4.1.b Observe HSM functions and procedures for generating and loading keys for use in transaction-originating POIs to verify that unique keys are generated and used for each POI device.	*<Report Findings Here>*
6E-4.1.c Examine check, hash, or fingerprint values for a sample of cryptographic keys from different POI devices to verify keys are unique for each POI device.	*<Report Findings Here>*
6E-4.1.d Compare all POI public keys, if used, across all decryption points as well as for every POI connection, to ensure there are no duplicates across POI devices.	*<Report Findings Here>*
6E-4.1.e Compare the number of POI devices in use to the number of cryptographic keys in use to verify that an individual key is defined for each device. (Having fewer keys than devices would indicate that the same key is being used for several devices.)	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6E-4.1.f Examine cryptograms of keys used between the POI and its decryption point and compare to cryptograms used in other decryption points to verify that the key exists at the minimum number of facilities consistent with effective system operations.	*<Report Findings Here>*
6E-4.2 These unique keys, or set of keys, must be totally independent and produced using a reversible process, such as that used to produce "key variants."	
6E-4.2.a Examine documented procedures for generating all types of keys and verify the procedures ensure: • That unique keys, or sets of keys, must be totally independent. • That unique keys, or sets of keys, are produced using a reversible process.	*<Report Findings Here>*
6E-4.2.b Interview personnel and observe key-generation processes to verify that keys are generated independently of other keys of the same type.	*<Report Findings Here>*
6E-4.2.c Interview personnel and observe key-generation processes to verify that variants of one key are not used across multiple POI devices, or multiple decryption end points.	*<Report Findings Here>*
6E-4.3 Emergency procedures must support requirements for unique device keys and not circumvent uniqueness controls.	
6E-4.3.a Examine documented emergency procedures and very they: • Support requirements for unique device keys. • Do not circumvent uniqueness controls.	*<Report Findings Here>*
6E-4.3.b Interview responsible personnel to verify: • Requirements for unique device keys are maintained during emergency situations. • Uniqueness controls are not circumvented during emergency situations.	*<Report Findings Here>*
6E-4.4 Where master keys are generated by a derivation process and derived from the same base derivation key, ensure the following: • Unique data must be used for the derivation process such that all transaction-originating SCDs receive unique secret keys. • Key derivation must be performed prior to a key being loaded/sent to the recipient transaction-originating POI. *This requirement refers to the use of a single "base" key to derive master keys for many different POI devices, using a key-derivation process as described above. This requirement does not preclude multiple unique keys being loaded on a single device, or for the device to use a unique key for derivation of other keys, once loaded.*	
6E-4.4.a Examine documented procedures and observe processes for generating master keys. Verify the following is implemented where master keys are generated by a derivation process and derived from the same base derivation key: • Unique data is used for the derivation process such that all transaction-originating SCDs receive unique secret keys. • Key derivation is performed prior to a key being loaded/sent to the recipient transaction-originating POI.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6E-4.4.b Verify that derivation keys used to generate keys for multiple devices are never loaded into a POI device.	*<Report Findings Here>*
6F-1 Secret keys used for encrypting account-data-encryption keys or for account-data encryption, or private keys used in connection with remote key-distribution implementations, must never exist outside of a secure cryptographic device, except when encrypted or managed using the principles of dual control and split knowledge.	
6F-1.1 Secret or private keys must only exist in one or more of the following forms at all times—including during generation, transmission, storage, and use: • At least two separate key shares or full-length components • Encrypted with a key of equal or greater strength • Contained within a secure cryptographic device	
6F-1.1.a Examine documented key-generation procedures and observe key-generation processes to verify that secret or private keys only exist in one or more approved forms at all times during key generation.	*<Report Findings Here>*
6F-1.1.b Examine documented procedures for transmission of keys and observe key-transmission processes to verify that secret or private keys only exist in one or more approved forms at all times during transmission.	*<Report Findings Here>*
6F-1.1.c Examine documented procedures for key storage and observe key stores to verify that secret or private keys only exist in one or more approved forms at all times when stored.	*<Report Findings Here>*
6F-1.1.d Examine documented key-usage procedures and observe operational processes to verify that secret or private keys only exist in one or more approved forms at all times during use.	*<Report Findings Here>*
6F-1.2 Wherever key components are used, they have the following properties:	
6F-1.2 Examine documented procedures and interview responsible personnel to determine all instances where key components are used. Perform the following wherever key components are used:	*<Report Findings Here>*
6F-1.2.1 Knowledge of any one key component does not convey any knowledge of any part of the actual cryptographic key.	
6F-1.2.1 Review processes for creating key components and examine key components to verify that knowledge of any one key component does not convey any knowledge of any part of the actual cryptographic key.	*<Report Findings Here>*
6F-1.2.2 Construction of the cryptographic key requires the use of at least two key components.	
6F-1.2.2 Observe processes for constructing cryptographic keys to verify that at least two key components are required for each key construction.	*<Report Findings Here>*
6F-1.2.3 Each key component has one or more specified custodians.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6F-1.2.3.a Examine documented procedures for the use of key components and interview key custodians to verify that each key component is assigned to a specific individual, or set of individuals, who are designated as key custodians for that component.	*<Report Findings Here>*
6F-1.2.3.b Observe key-component access controls and key-custodian authorizations/assignments to verify that all individuals with access to key components are designated as key custodians for that component.	*<Report Findings Here>*
6F-1.2.4 Procedures exist to ensure any custodian never has access to sufficient key components to reconstruct a cryptographic key. *For example, in an* m-of-n *scheme, where only two of any three components are required to reconstruct the cryptographic key, a custodian cannot have current or prior knowledge of more than one component. If a custodian was previously assigned component A, which was then reassigned, the custodian cannot then be assigned component B or C, as this would give them knowledge of two components, which gives them ability to recreate the key.* *In an* m-of-n *scheme where all three components are required to reconstruct the cryptographic key, a single custodian may be permitted to have access to two of the key components (for example, component A and component B), as a second custodian (with, in this example, component C) would be required to reconstruct the final key, ensuring that dual control is maintained.*	
6F-1.2.4.a Examine documented procedures for the use of key components to verify that procedures ensure that any custodian never has access to sufficient key components to reconstruct a cryptographic key.	*<Report Findings Here>*
6F-1.2.4.b Examine key-component access controls and access logs to verify that authorized custodians cannot access sufficient key components to reconstruct a cryptographic key.	*<Report Findings Here>*
6F-1.2.5 Key components must be combined using a process such that no active bit of the key can be determined without knowledge of the remaining components. (For example, via XOR'ing.) *Note that concatenation of key components together to form the key is unacceptable; e.g., concatenating two eight-hexadecimal character halves to form a sixteen-hexadecimal secret key.* The resulting key must only exist within the SCD.	
6F-1.2.5.a Examine documented procedures for combining key components and observe processes to verify that key components are combined using a process such that no active bit of the key can be determined without knowledge of the remaining components.	*<Report Findings Here>*
6F-1.2.5.b Examine key-component lengths for a key generated with those components to verify that key components are not concatenated to form the key.	*<Report Findings Here>*
6F-1.3 Key components must be stored as follows:	
6F-1.3 Examine documented procedures, interview responsible personnel and inspect key-component storage locations to verify that key components are stored as follows:	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6F-1.3.1 Key components that exist in clear text outside of an SCD must be sealed in opaque, tamper-evident packaging that prevents the determination of the key component without noticeable damage to the packaging. ***Note:*** *Tamper-evident packaging used to secure key components must ensure that the key component cannot be determined. For components written on paper, opacity may be sufficient, but consideration must be given to any embossing or other possible methods to "read" the component without opening of the packaging. Similarly, if the component is stored on a magnetic card, contactless card, or other media that can be read without direct physical contact, the packaging should be designed to prevent such access to the key component.*	
6F-1.3.1.a Examine key components and storage locations to verify that components are stored in opaque, tamper-evident packaging that prevents the determination of the key component without noticeable damage to the packaging.	*<Report Findings Here>*
6F-1.3.1.b Inspect any tamper-evident packaging used to secure key components and ensure that it prevents the determination of the key component without visible damage to the packaging.	*<Report Findings Here>*
6F-1.3.1.c Ensure clear-text key components do not exist in any other locations, including in non-secure containers, in databases, on floppy disks, or in software programs.	*<Report Findings Here>*
6F-1.3.1.d Confirm that start-up instructions and other notes used by service technicians do not contain initialization-key values written in the clear (e.g., at the point in the checklist where the keys are entered).	*<Report Findings Here>*
6F-1.3.2 Key components for each specific custodian must be stored in a separate secure container that is accessible only by the custodian and/or designated backup(s). ***Note:*** *Furniture-based locks or containers with a limited set of unique keys are not sufficient to meet this requirement (for example, desk drawers).* *Components for a specific key that are stored in separate envelopes, but within the same secure container, place reliance upon procedural controls and do not meet the requirement for physical barriers.*	
6F-1.3.2 Inspect each key component storage container and verify the following: Key components for different custodians are stored in separate secure containers. Each secure container is accessible only by the custodian and/or designated backup(s).	*<Report Findings Here>*
6F-1.3.3 If a key component is stored on a token, and a PIN or similar mechanism is used to access the token, only that token's owner (or designated backup(s)) must have possession of both the token and its corresponding PIN.	
6F-1.3.3 If a key component is stored on a token, and a PIN or similar mechanism is used to access the token, only that token's owner—or designated backup(s)—has possession of both the token and its corresponding PIN.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6F-2 Procedures must exist and must be demonstrably in use to replace any known or suspected compromised key, its subsidiary keys (those keys encrypted with the compromised key), and keys derived from the compromised key, to a value not feasibly related to the original key.	
6F-2.1 Procedures for known or suspected compromised keys must include the following:	
6F-2.1 Verify documented procedures exist for replacing known or suspected compromised keys, and include 6F-2.1.1 through 6F-2.1.9 below.	*<Report Findings Here>*
6F-2.1.1 Key components are never reloaded when there is any suspicion that either the originally loaded key or the SCD has been compromised.	
6F-2.1.1 Interview responsible personnel and observe implemented processes to verify key components are never reloaded when there is any suspicion that either the originally loaded key or the SCD has been compromised.	*<Report Findings Here>*
6F-2.1.2 If unauthorized alteration is suspected, new keys are not installed until the SCD has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.	
6F-2.1.2 Interview responsible personnel and observe implemented processes to verify that if unauthorized alteration is suspected, new keys are not installed until the SCD has been inspected and assurance reached that the equipment has not been subject to any form of unauthorized modification.	*<Report Findings Here>*
6F-2.1.3 If compromise of the cryptographic key is suspected, processing with that key is halted, and the key is replaced with a new unique key. This process includes any systems, devices, or processing that involves subordinate keys that have been calculated, derived, or otherwise generated, loaded, or protected using the compromised key. The replacement key must not be a variant of the original key, or an irreversible transformation of the original key.	
6F-2.1.3 Interview responsible personnel and observe implemented processes to verify that if compromise of the cryptographic key is suspected, all the following are performed: Processing with that key is halted, and the key is replaced with a new unique key. Any systems, devices, or processing involving subordinate keys that have been calculated, derived, or otherwise generated, loaded, or protected using the compromised key are included in the key-replacement process. The replacement key must not be a variant of the original key, or an irreversible transformation of the original key.	*<Report Findings Here>*
6F-2.1.4 For each key in the solution provider's key suite, including any subordinate keys that are generated, protected, or transported under other keys, the purpose of that key is listed.	
6F-2.1.4 Interview responsible personnel and observe documented key lists to verify the purpose of each key is listed, for all keys used by the solution provider.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6F-2.1.5 The names and/or functions of each staff member assigned to the recovery effort, as well as phone numbers and the place where the team is to assemble, are defined.	
6F-2.1.5 Interview responsible personnel and observe documentation to verify he following are defined: The names and/or functions of each staff member assigned to the recovery effort Contact phone numbers for staff members assigned to the recovery effort A designated place where the recovery team is to assemble	*<Report Findings Here>*
6F-2.1.6 A documented escalation process and notification to organizations that currently share or have previously shared the key(s), including: A damage assessment Specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.	
6F-2.1.6.a Interview responsible personnel and observe implemented processes to verify the escalation process includes notification to organizations that currently share or have previously shared the key(s).	*<Report Findings Here>*
6F-2.1.6.b Verify notifications include the following: A damage assessment Details of specific actions to be taken with system software and hardware, encryption keys, encrypted data, etc.	*<Report Findings Here>*
6F-2.1.7 Identification of specific events that would indicate a compromise may have occurred. Such events must include but are not limited to: Missing SCDs Tamper-evident seals or package numbers or dates and times not agreeing with log entries Tamper-evident seals or packages that have been opened without authorization or show signs of attempts to open or penetrate	
6F-2.1.7 Interview responsible personnel and observe implemented processes to verify that specific events that may indicate a compromise are identified. This must include, as a minimum, the following events: Missing SCDs Tamper-evident seals or package numbers or dates and times not agreeing with log entries Tamper-evident seals or packages that have been opened without authorization or show signs of attempts to open or penetrate	*<Report Findings Here>*
6F-2.1.8 Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities.	
6F-2.1.8 Interview responsible personnel and observe implemented processes to verify procedures address indications of physical or logical access attempts to the processing system by unauthorized individuals or entities.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6F-2.1.9 If attempts to load a secret key or key component into an SCD fail, the same key or component must not be loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased from or otherwise destroyed in the original SCD.	
6F-2.1.9 Interview responsible personnel and observe implemented processes to verify that if attempts to load a secret key or key component into an SCD fail, the same key or component is not loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased from or otherwise destroyed in the original SCD.	*<Report Findings Here>*
6F-3 Keys generated using reversible key-calculation methods, such as key variants, must only be used in devices that possess the original key. Keys generated using reversible key-calculation methods must not be used at different levels of the key hierarchy. For example, a variant of a key-encryption key used for key exchange cannot be used as a working key or as a master file key for local storage. *Key generation that uses a non-reversible process, such as key derivation with a base key using an encipherment process, is not subject to these requirements.*	
6F-3.1 Any key generated with a reversible process (such as a variant of a key) of another key must be protected in the same manner as the original key—that is, under the principles of dual control and split knowledge. *Exposure of keys that are created using reversible transforms of another (key-generation) key can result in the exposure of all keys that have been generated under that key-generation key. To limit this risk posed by reversible key calculation, such as key variants, the reversible transforms of a key must be secured in the same way as the original key-generation key.*	
6F-3.1.a Examine documented procedures and interview responsible personnel to determine whether keys are generated using reversible key-calculation methods.	*<Report Findings Here>*
6F-3.1.b Observe processes to verify that any key generated using a reversible process of another key is protected under the principles of dual control and split knowledge.	*<Report Findings Here>*
6F-3.1.1 Reversible transformations of a key must not be exposed outside of the secure cryptographic device that generated those transforms.	
6F-3.1.1 Verify that reversible transformations of keys are not exposed outside of the secure cryptographic device that generated those transforms.	*<Report Findings Here>*
6F-3.2 Reversible key transformations are not used across different levels of the key hierarchy. For example, reversible transformations must not generate data-encryption keys from master keys, or from key-encrypting keys. Such transformations are only used to generate different types of key-encrypting keys from an initial key-encrypting key, or different data-encryption keys from an initial data-encryption key. *Using transforms of keys across different levels of a key hierarchy—for example, generating an account-data key from a key-encrypting key—increases the risk of exposure of each of those keys.* *It is acceptable to use one "working" key to generate multiple reversible transforms to be used for different working keys, such as a PIN key, MAC key(s), and data key(s) (where a different reversible transform is used to generate each different working key). Similarly, it is acceptable to generate multiple key-encrypting keys from a single key-encrypting key. However, it is not acceptable to generate working keys from key-encrypting keys.*	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6F-3.2 Examine documented key-transformation procedures and observe implemented processes to verify that reversible key transformations are not used across different levels of the key hierarchy, as follows: • Master keys must only be generated from or be used to generate other master keys. • Key-encrypting keys must only be generated from or be used to generate other key-encrypting keys. • Data-encryption keys must only be generated from or be used to generate other data-encryption keys. • Any other type of key must only be generated from or be used to generate other keys of the same type.	*<Report Findings Here>*
6F-4 Secret keys and key components that are no longer used or have been replaced must be securely destroyed.	
6F-4.1 Instances of secret or private keys, or key components, that are no longer used or that have been replaced by a new key must be destroyed.	
6F-4.1.a Verify documented procedures are in place for destroying secret or private keys, or key components that are no longer used or that have been replaced by a new key.	*<Report Findings Here>*
6F-4.1.b Identify a sample of keys and key components that are no longer used or have been replaced. For each item in the sample, interview responsible personnel and examine key-history logs and key-destruction logs to verify that all keys have been destroyed.	*<Report Findings Here>*
6F-4.2 The procedures for destroying keys or key components that are no longer used or that have been replaced by a new key must be documented and sufficient to ensure that no part of the key or component can be recovered.	
6F-4.2.a Examine documented procedures for destroying keys and confirm they are sufficient to ensure that no part of the key or component can be recovered.	*<Report Findings Here>*
6F-4.2.b Observe key-destruction processes to verify that no part of the key or component can be recovered.	*<Report Findings Here>*
6F-4.2.1 Keys (including components or shares) maintained on paper must be burned, pulped, or shredded in a crosscut shredder.	
6F-4.2.1.a Examine documented procedures for destroying keys and confirm that any keys (including components or shares) maintained on paper must be burned, pulped, or shredded in a crosscut shredder.	*<Report Findings Here>*
6F-4.2.1.b Observe key-destruction processes to verify that any keys (including components or shares) maintained on paper is burned, pulped, or shredded in a crosscut shredder.	*<Report Findings Here>*
6F-4.2.2 Keys on all other storage media types in all permissible forms (physically secured, enciphered, or components) must be destroyed following the procedures outlined in ISO–9564 or ISO–11568.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6F-4.2.2.a Examine documented procedures for destroying keys and confirm that keys on all other storage media types in all permissible forms (physically secured, enciphered, or components) must be destroyed following the procedures outlined in ISO–9564 or ISO–11568.	*<Report Findings Here>*
6F-4.2.2.b Observe key-destruction processes to verify that keys on all other storage media types in all permissible forms (physically secured, enciphered, or components) are destroyed following the procedures outlined in ISO–9564 or ISO–11568.	*<Report Findings Here>*
6F-4.2.3 The key-destruction process must be observed by a third party other than the custodian.	
6F-4.2.3 Observe key-destruction process and verify that it is witnessed by a third party other than a key custodian.	*<Report Findings Here>*
6F-4.2.4 The third-party witness must sign an affidavit of destruction. ***Note:*** *For keys on paper, consider having the affidavit of destruction as a part of the same piece of paper that contains the key-component value itself. To destroy the key, tear off the section of the sheet that contains the value, destroy it, sign and witness the affidavit and log it. Affidavits of destruction can also be digitally signed if considered legally acceptable in the locale.*	
6F-4.2.4 Inspect key-destruction logs and verify that a third-party, non-key-custodian witness signs an affidavit as a witness to the key destruction process.	*<Report Findings Here>*
6F-4.3 Any residues of key-encryption keys used for the conveyance of working keys (such as components used to create the key) must be destroyed after successful loading and validation as being operational.	
6F-4.3.a Verify documented procedures exist for destroying any residues of key-encryption keys used for the conveyance of working keys, once the working keys are successfully loaded and validated as operational.	*<Report Findings Here>*
6F-4.3.b Observe key-conveyance/loading processes to verify that any residues of key-encryption keys used for the conveyance of working keys are destroyed, once the working keys are successfully loaded and validated as operational.	*<Report Findings Here>*
6F-5 Access to material which can be used to construct secret and private keys (such as key components) must be: Limited on to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use; and Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.	
6F-5.1 To reduce the opportunity for key compromise, limit the number of key custodians to a minimum as follows:	
6F-5.1 Interview key custodians and observe implemented processes to verify the following:	
6F-5.1.1 Designate a primary and a backup key custodian for each component, such that the fewest number of key custodians are assigned as necessary to enable effective key management.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6F-5.1.1 Review key-custodian assignments for each component to verify that: A primary and a backup key custodian are designated for each component. The fewest number of key custodians is assigned as necessary to enable effective key management.	*<Report Findings Here>*
6F-5.1.2 Document this designation by having each custodian and backup custodian sign a key-custodian form in some legally binding way.	
6F-5.1.2.a Examine completed key-custodian forms to verify that key custodians sign the form in some legally binding way.	*<Report Findings Here>*
6F-5.1.2.b Examine completed key-custodian forms to verify that backup custodians sign the form in some legally binding way.	*<Report Findings Here>*
6F-5.1.3 Each key-custodian form provides the following: Specific authorization for the custodian Identification of the custodian's responsibilities for safeguarding key components or other keying material entrusted to them An effective date and time for the custodian's access Signature of management authorizing the access	
6F-5.1.3 Examine all key-custodian forms to verify that they include the following: Specific authorization for the custodian Identification of the custodian's responsibilities for safeguarding key components or other keying material entrusted to them An effective date and time for the custodian's access Signature of management authorizing the access.	*<Report Findings Here>*
6F-5.1.4 Key custodians sufficient to form the necessary threshold to create a key must not directly report to the same individual. For example, for a key managed as three components, at least two custodians report to different individuals. In an *m-of-n* scheme, such as *three of five* key shares, no more than two key custodians can report to the same individual. In all cases, neither the direct reports nor the direct reports in combination with their immediate supervisor (if they are a key custodian) shall possess the necessary threshold of key components sufficient to form any given key.	
6F-5.1.4 Examine key-custodian assignments and organization charts to confirm the following: Key custodians that form the necessary threshold to create a key do not directly report to the same individual. Neither direct reports nor the direct reports in combination with their immediate supervisor possess the necessary threshold of key components sufficient to form any given key.	*<Report Findings Here>*
6F-6 Logs are kept for any time that keys, key components, or related materials are removed from secure storage or loaded to an SCD.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6F-6.1 Logs must be kept whenever keys, key components, or related materials are removed from secure storage or loaded to an SCD.	
6F-6.1 Review log files and audit log settings to verify that logs are kept for any time that keys, key components, or related materials are: • Removed from secure storage • Loaded to an SCD	*<Report Findings Here>*
6F-6.2 At a minimum, logs must include the following: • Date and time in/out • Key component identifier • Purpose of access • Name and signature of custodian accessing the component • Tamper-evident package number (if applicable)	
6F-6.2 Review log files and audit log settings to verify that logs include the following: • Date and time in/out • Key component identifier • Purpose of access • Name and signature of custodian accessing the component • Tamper-evident package number (if applicable)	*<Report Findings Here>*
6F-7 Backup copies of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.	
6F-7.1 The backup copies must be securely stored with proper access controls, under at least dual control, and subject to at least the same level of security control as operational keys in line with all requirements specified in this document.	
6F-7.1 Interview responsible personnel and examine documented procedures and backup records to determine whether any backup copies of keys or their components exist. Perform the following:	*<Report Findings Here>*
6F-7.1.a Verify that any backup copies of secret and private keys exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible.	*<Report Findings Here>*
6F-7.1.b Inspect backup storage locations and access controls to verify that backups are maintained as follows: • Securely stored with proper access controls • Under at least dual control • Subject to at least the same level of security control as operational keys as specified in this document	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6F-7.2 If backup copies are created, the following must be in place: • Creation (including cloning) must require a minimum of two authorized individuals to enable the process. • All requirements applicable for the original keys also apply to any backup copies of keys and their components. *It is not a requirement to have backup copies of key components or keys, but it is acceptable to maintain such backup copies for the purposes of business continuity if they are secured and maintained in approved forms.*	
6F-7.2 Interview responsible personnel and observe backup processes to verify the following: • The creation of any backup copies requires at least two authorized individuals to enable the process • All requirements applicable for the original keys also apply to any backup copies of keys and their components.	*<Report Findings Here>*
6F-7.3 If backup copies of secret and/or private keys exist, confirm that they are maintained in one of the approved forms noted in Requirement 6F-1.1 and are managed under dual control and split knowledge.	
6F-7.3 Interview responsible personnel and observe backup processes to verify the following • Backup copies of secret and/or private keys are maintained in one of the approved forms identified Requirement 6F-1.1 • Backup copies of secret and/or private keys are managed under dual control and split knowledge.	*<Report Findings Here>*
6F-8 Documented procedures must exist and must be demonstrably in use for all key-administration operations.	
6F-8.1 Written procedures must be in place and all affected parties must be aware of those procedures, as follows: • All aspects of and activities related to key administration must be documented, including: ○ A defined cryptographic-key change policy for each key layer defined in the key hierarchy (this applies to both symmetric and asymmetric-key types) ○ Security-awareness training ○ Role definition—nominated individual with overall responsibility ○ Background checks for personnel • Management of personnel changes, including revocation of access control and other privileges when personnel move	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
6F-8.1.a Examine documented procedures for key-administration operations to verify they include: • A defined cryptographic-key change policy for each key layer defined in the key hierarchy • Security-awareness training • Role definition—nominated individual with overall responsibility • Background checks for personnel • Management of personnel changes, including revocation of access control and other privileges when personnel move	<Report Findings Here>
6F-8.1.b Interview personnel responsible for key-administration operations to verify that the documented procedures are known and understood.	*<Report Findings Here>*
6F-8.1.c Interview personnel to verify that security-awareness training is provided for the appropriate personnel.	*<Report Findings Here>*
6F-8.1.d Interview personnel to verify background checks are performed.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

Domain 6 Annex A: Cryptographic Key Operations – Symmetric-Key Distribution using Asymmetric Techniques

Table 6A.1 – List of symmetric keys (by type) distributed using asymmetric techniques			
Key type / description*	Purpose/ function of the key (including types of devices using key)	Description / identifier of asymmetric techniques use for key distribution	Entity performing remote key distribution

**** Note:** Must include all keys from Table 6.1 identified as being distributed via remote key distribution techniques.*

P2PE Domain 6 Annex A Requirements and Testing Procedures	**P2PE Assessor Findings from Solution Provider Assessment**
RD-1 Compromise of the key-generation process must not be possible without collusion between at least two trusted individuals. *(Reference 6B-2)*	
RD-1.1 Asymmetric-key pairs must either be: • Generated by the device that will use the key pair; or • If generated externally, the key pair and all related critical security parameters (for example, secret seeds) must be deleted (zeroized) immediately after the transfer to the device that will use the key pair.	
RD-1.1.a Examine documented procedures for asymmetric-key generation to confirm that procedures are defined to ensure that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters must be deleted (zeroized) immediately after the transfer to the device that will use the key pair	*<Report Findings Here>*
RD-1.1.b Observe key-generation processes to verify that asymmetric-key pairs are either: • Generated by the device that will use the key pair, or • If generated externally, the key pair and all related critical security parameters are deleted (for example, zeroized) immediately after the transfer to the device that will use the key pair.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-2 Cryptographic keys must be conveyed or transmitted securely. *(Reference 6C-1)*	
RD-2.1 All key-encryption keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed	
RD-2.1.a Examine documented procedures to verify that all asymmetric keys used to transmit or convey other cryptographic keys must be (at least) as strong as any key transmitted or conveyed.	*<Report Findings Here>*
RD-2.1.b Observe key generation processes to verify that all asymmetric keys used to transmit or convey other cryptographic keys are at least as strong as any key transmitted or conveyed.	*<Report Findings Here>*
RD-3 The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised. *(Reference 6D)*	
RD-3.1 POIs and key-distribution hosts (KDHs) using public-key schemes must validate authentication credentials of other such devices involved in the communication immediately prior to any key transport, exchange, or establishment. Mutual authentication of the sending and receiving devices must be performed. ***Note:*** *Examples of this kind of validation include checking current certificate revocation lists or embedding valid authorized KDH certificates in devices and disallowing communication with unauthorized KDHs.*	
RD-3.1.a Examine documented procedures to confirm they define procedures for mutual authentication of the sending and receiving devices, as follows: • SCDs must validate authentication credentials of KDHs prior to any key transport, exchange, or establishment with that device. • KDHs must validate authentication credentials of POIs prior to any key transport, exchange, or establishment with that device.	*<Report Findings Here>*
RD-3.1.b Observe key-loading processes to verify that mutual authentication of the sending and receiving devices is performed, as follows: • SCDs validate authentication credentials of KDHs immediately prior to any key transport, exchange, or establishment with that device. • KDHs validate authentication credentials of POIs immediately prior to any key transport, exchange, or establishment with that device.	*<Report Findings Here>*
RD-3.2 Mechanisms must exist to prevent a non-authorized KDH from performing key transport, key exchange or key establishment with POIs. ***Note:*** *An example of this kind of mechanism is through limiting communication between the transaction-originating POI and KDH to only those KDHs contained in a list of valid KDHs managed by the POI.*	
RD-3.2.a Examine documented procedures to confirm they define mechanisms to prevent an unauthorized KDH from performing key transport, key exchange, or key establishment with POIs.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-3.2.b Observe mechanisms in use to verify they prevent an unauthorized KDH from performing key transport, key exchange, or key establishment with POIs.	*<Report Findings Here>*
RD-3.3 Key establishment and distribution procedures must be designed such that: • Within an implementation design, there shall be no means available for "man in middle" attacks. • System implementations must be designed and implemented to prevent replay attacks.	
RD-3.3.a Examine system and process documentation to verify that key establishment and distribution procedures are designed such that: • There are no means available in the implementation design for "man in middle" attacks. • System implementations are designed to prevent replay attacks.	*<Report Findings Here>*
RD-3.3.b Observe key-exchange and establishment operations to verify that system implementations are implemented such that: • There are no means available for "man in middle" attacks. • System implementations prevent replay attacks.	*<Report Findings Here>*
RD-3.4 Key pairs generated external to the device that uses the key pair must be securely transferred and loaded into the device: that is, the secrecy of private keys and the integrity of public keys must be ensured.	
RD-3.4 If key pairs are generated external to the device that uses the key pair, perform the following:	
RD-3.4.a Examine documented procedures to verify that controls are defined to ensure the secrecy of private keys and the integrity of public keys during key transfer and loading.	*<Report Findings Here>*
RD-3.4.b Observe key transfer and loading operations to verify that the secrecy of private keys and the integrity of the public keys are ensured.	*<Report Findings Here>*
RD-3.5 Once asymmetric keys are loaded for a specific P2PE solution provider, changing of those keys must not be permitted without the authorization of that solution provider.	
RD-3.5.a Examine documentation to verify that procedures are defined to ensure that, once asymmetric keys are loaded, changing of those keys is not permitted without authorization of that P2PE solution provider.	*<Report Findings Here>*
RD-3.5.b Interview responsible personnel and observe records of the authorization process to verify that once asymmetric keys have been loaded, authorization from the P2PE solution provider is obtained before those keys are changed.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-4 Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any encryption device without legitimate keys. *(Reference 6E-2)*	
RD-4.1 POIs shall only communicate with a Certification Authority (CA) for the purpose of certificate signing (or for key injection where the certificate-issuing authority generates the key pair on behalf of the POI); and with KDHs for key management, normal transaction processing, and certificate (entity) status checking.	
RD-4.1.a Examine documented procedures to verify that: • POIs are only required to communicate with CAs for the purpose of certificate signing, or for key injection where the certificate-issuing authority generates the key pair on behalf of the device; • POIs are only required to communicate with KDHs for key management, normal transaction processing, and certificate (entity) status checking.	*<Report Findings Here>*
RD-4.1.b Interview responsible personnel and observe POI configurations to verify that: • POIs only communicate with CAs for the purpose of certificate signing, or for key-injection where the certificate issuing authority generates the key pair on behalf of the device; • POIs only communicate with KDHs for key management, normal transaction processing, and certificate (entity) status checking.	*<Report Findings Here>*
RD-4.2 KDHs shall only communicate with POIs for the purpose of key management and normal transaction processing, and with CAs for the purpose of certificate signing and certificate (entity) status checking.	
RD-4.2.a Examine documented procedures to verify that: • KDHs are only required to communicate with POIs for the purpose of key management and normal transaction processing; • KDHs are only required to communicate with CAs for the purpose of certificate signing and certificate (entity) status checking.	*<Report Findings Here>*
RD-4.2.b Interview responsible personnel and observe KDH configurations to verify that: • KDHs only communicate with POIs for the purpose of key management and normal transaction processing; • KDHs only communicate with CAs for the purpose of certificate signing and certificate (entity) status checking.	*<Report Findings Here>*
RD-5 Cryptographic keys must only be used for their sole intended purpose and must never be shared between production and test systems. *(Reference 6E-3)*	
RD-5.1 Only one certificate shall be issued per key pair. Key pairs shall not be reused for certificate renewal or replacement.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-5.1.a Examine documented procedures for requesting certificate issue, renewal, and replacement to verify procedures include generation of a unique key pair for each: • New certificate issue request • Certificate renewal request • Certificate replacement request	*<Report Findings Here>*
RD-5.1.b Interview responsible personnel and observe certificate issuing, renewal, and replacement processes to verify that: • Only one certificate is requested for each key pair generated. • Expired certificates are renewed by generating a new key pair and requesting a new certificate. • Certificates are replaced by generating a new key pair and requesting a new certificate.	*<Report Findings Here>*
RD-5.2 Mechanisms must be utilized to preclude the use of a key for other than its designated and intended purpose—that is, keys must be used in accordance with their certificate policy (as required in Requirement RD-9.3). See *RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* for an example of content.	
RD-5.2.a Examine certificate policy and key-usage procedures and verify that documented key-usage procedures are defined in accordance with the certificate policy.	*<Report Findings Here>*
RD-5.2.b Verify that mechanisms are defined that preclude the use of a key for other than its designated and intended purpose.	*<Report Findings Here>*
RD-5.2.c Observe key-usage processes to verify that mechanisms are in use that preclude the use of a key for other than its designated and intended purpose.	*<Report Findings Here>*
RD-5.2.1 CA/RA: CA certificate signature keys, certificate (entity) status checking (for example, Certificate Revocation Lists) signature keys, or signature keys for updating valid/authorized host lists in encryption devices cannot be used for any purpose other than subordinate entity certificate requests, certificate status checking, and self-signed root certificates. ***Note:*** *The keys used for certificate signing and certificate (entity) status checking (and if applicable, self-signed roots) may be for combined usage or may exist as separate keys dedicated to either certificate-signing or certificate (entity) status checking.*	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-5.2.1.a Examine certificate policy and documented procedures to verify that: Certificate signature keys, Certificate status checking (for example, Certificate Revocation Lists) signature keys, or Signature keys for updating valid/authorized host lists in POIs Must not be used for any purpose other than: Subordinate entity certificate requests, Certificate status checking, and/or Self-signed root certificates	*<Report Findings Here>*
RD-5.2.1.b Interview responsible personnel and observe key-usage processes to verify that: Certificate signature keys, Status checking (for example, Certificate Revocation Lists) signature keys, or Signature keys for updating valid/authorized host lists in POIs Are not used for any purpose other than: Subordinate entity certificate requests, Certificate status checking, and/or Self-signed root certificates	*<Report Findings Here>*
RD-5.2.2 CAs that issue certificates to other CAs cannot be used to issue certificates to POIs.	
RD-5.2.2 if a CA issues certificates to POIs, examine CA certificate policy and documented procedures to verify that the CA does not issue certificates to other CAs.	*<Report Findings Here>*
RD-5.3 Public-key-based implementations must provide mechanisms for restricting and controlling the use of public and private keys. *For example, this can be accomplished through the use of X.509-compliant certificate extensions.*	
RD-5.3.a Examine documented procedures to verify that mechanisms are defined for restricting and controlling the use of public and private keys such that they can only be used for their intended purpose.	*<Report Findings Here>*
RD-5.3.b Observe the mechanisms in use to verify that they restrict and control the use of public and private keys.	*<Report Findings Here>*
RD-5.4 CA/RA: CA private keys cannot be shared between devices except for load balancing and disaster recovery.	
RD-5.4.a Examine CA's documented processes to verify that CA private keys are not permitted to be shared between devices, except for load balancing and disaster recovery.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-5.4.b Examine cryptograms of the private keys on CA systems and/or observe records of key-management operations to verify that CA private keys are not shared between devices, except for load balancing and disaster recovery.	*<Report Findings Here>*
RD-5.5 KDH private keys cannot be shared between devices except for load balancing and disaster recovery.	
RD-5.5.a Examine documented processes to verify that KDH private keys are not permitted to be shared between devices, except for load balancing and disaster recovery.	*<Report Findings Here>*
RD-5.5.b Examine cryptograms of the private keys and/or observe records of key-management operations to verify that KDH private keys are not shared between devices, except for load balancing and disaster recovery.	*<Report Findings Here>*
RD-5.6 POI private keys cannot be shared.	
RD-5.6.a Examine documented processes to verify that POI private keys are not permitted to be shared between devices.	*<Report Findings Here>*
RD-5.6.b Inspect public key certificates on the host processing system to confirm that a unique certificate exists for each connected POI.	*<Report Findings Here>*
RD-6 All secret and private keys must be unique (except by chance) to a POI device. *(Reference 6E-4)*	
RD-6.1 Keys in all hosts and POIs must be uniquely identifiable via cryptographically verifiable means (for example, through the use of digital signatures, "fingerprints," or key check values). The method used must not expose any part of the actual key value.	
RD-6.1.a Examine documented procedures to verify that a cryptographic method is defined which: • Uniquely identifies private keys stored within all hosts and POIs. • Does not expose any part of the actual key value.	*<Report Findings Here>*
RD-6.1.b Examine a sample of hosts and POIs to verify the method used: • Uniquely identifies the private keys stored within all hosts and POIs. • Does not expose any part of the actual key value.	*<Report Findings Here>*
RD-6.2 Private keys used to sign certificates, certificate-status lists, or messages must exist only in one of the following forms: • At least two separate key shares or full-length components; • Encrypted using an algorithm and key size of equivalent or greater strength; or • Within an SCD (for example, an HSM or POI) approved to FIPS140-2 Level 3, PCI HSM, or PCI PTS.	
RD-6.2.a Examine documented key-management procedures to verify that private keys used to sign certificates, certificate-status lists, or messages must exist only in one of the approved forms at all times.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-6.2.b Observe key-management operations and interview key custodians to verify that private keys used to sign certificates, certificate-status lists, or messages must exist only in one of the approved forms at all times.	*<Report Findings Here>*
RD-7 Procedures must exist and must be demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys encrypted with the compromised key) with a value not feasibly related to the original key. *(Reference 6F-2)*	
RD-7.1 Solution provider must provide for continuity of service in the event of the loss of a root key (for example, through compromise or expiration). *For example, a key-distribution management system and the associated end entities (KDHs, encryption devices) could provide support for more than one root.*	
RD-7.1.a Examine documented key-management procedures to verify the solution provider provides for continuity of service in the event of the loss of a root key.	*<Report Findings Here>*
RD-7.1.b Observe key-management operations and interview key custodians to verify the solution provider provides for continuity of service in the event of the loss of a root key.	*<Report Findings Here>*
RD-7.2 CA/RA: Root CAs must provide for segmentation of risk to address key compromise. An example of this would be the deployment of subordinate CAs.	
RD-7.2 Through the examination of documented procedures, interviews and observation confirm that Root CAs provide for segmentation of risk to address key compromise.	*<Report Findings Here>*
RD-7.3 CA/RA: Mechanisms must be in place to address compromise of a CA due to, for example, key compromise or mismanagement. This must include procedures to revoke subordinate certificates and notify affected entities.	
RD-7.3.a Examine documented procedures to verify that mechanisms are defined to address compromise of a CA. Verify the mechanisms include procedures to: • Revoke subordinate certificates, and • Notify affected entities.	*<Report Findings Here>*
RD-7.3.b Interview responsible personnel to verify that the defined mechanisms to address compromise of a CA are in place and include: • Revoking subordinate certificates, and • Notifying affected entities.	*<Report Findings Here>*
RD-7.3.1 CA/RA: If a compromise is known or suspected, the CA must cease issuance of certificates and perform a damage assessment, including a documented analysis of how and why the event occurred. The damage assessment should assume that a compromise has occurred unless and until it is unequivocally proven to be a false alarm. The damage assessment includes determining whether the known or suspected compromise has or could result in the issuance of fraudulent certificates.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-7.3.1.a Examine documented procedures to verify that the following are required in the event a compromise is known or suspected: The CA will cease issuance of certificates. The CA will perform a damage assessment, including a documented analysis of how and why the event occurred. The damage assessment should assume that a compromise has occurred unless and until it is unequivocally proven to be a false alarm. The damage assessment includes determining whether the known or suspected compromise has or could result in the issuance of fraudulent certificates.	*<Report Findings Here>*
RD-7.3.1.b Interview responsible personnel and observe process to verify that in the event a compromise is known or suspected: The CA ceases issuance of certificates. The CA performs a damage assessment, including a documented analysis of how and why the event occurred. The damage assessment should assume that a compromise has occurred unless and until it is unequivocally proven to be a false alarm. The damage assessment includes determining whether the known or suspected compromise has or could result in the issuance of fraudulent certificates.	*<Report Findings Here>*
RD-7.3.2 In the event of the issuance of fraudulent certificates with the compromised key, the CA should determine whether to recall and reissue all signed certificates with a newly generated signing key.	
RD-7.3.2.a Examine documented procedures to verify that in the event of the issuance of fraudulent certificates with the compromised key, procedures are defined for the CA to determine whether to recall and reissue all signed certificates with a newly generated signing key.	*<Report Findings Here>*
RD-7.3.2.b Interview responsible personnel to verify procedures are followed for the CA to determine whether to recall and reissue all signed certificates with a newly generated signing key.	*<Report Findings Here>*
RD-7.3.3 Mechanisms (for example, time stamping) must exist to ensure that fraudulent certificates cannot be successfully used.	
RD-7.3.3.a Examine documented procedures to verify that mechanisms are defined to ensure that fraudulent certificates cannot be successfully used.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-7.3.3.b Interview responsible personnel and observe implemented mechanisms to verify that fraudulent certificates cannot be successfully used.	*<Report Findings Here>*
RD-7.4 CA/RA: The compromised CA must notify any superior or subordinate CAs of the compromise. The compromised CA must re-issue and distribute certificates or notify affected parties to apply for new certificates. ***Note:*** *Affected parties may include subordinate CAs or solution providers (KDHs and POIs), depending upon the function of the compromised CA.*	
RD-7.4.a Examine documented procedures to verify that the following procedures are required in the event of a compromise: • The CA will notify any superior CAs. • The CA will notify any subordinate CAs. • The CA will either: ○ Reissue and distribute certificates to affected parties, or ○ Notify the affected parties to apply for new certificates.	*<Report Findings Here>*
RD-7.4.b Interview responsible personnel to verify that the following procedures are performed in the event a compromise: • The CA notifies any superior CAs. • The CA will notifies any subordinate CAs. • The CA either: ○ Reissues and distributes certificates to affected parties, or ○ Notifies the affected parties to apply for new certificates.	*<Report Findings Here>*
RD-8 Access to material that can be used to construct secret and private keys (such as key components) must be: • Limited on to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use, and • Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component. *(Reference 6F-5)*	
RD-8.1 CA/RA: All user access to material that can be used to construct secret and private keys (such as key components) must be directly attributable to an individual user (for example, through the use of unique IDs).	
RD-8.1.a Examine documented procedures to confirm that access to material that can be used to construct secret and private keys is directly attributable to an individual user.	*<Report Findings Here>*
RD-8.1.b Observe the access-control mechanisms in place to verify that access to material that can be used to construct secret and private keys is directly attributable to an individual user.	*<Report Findings Here>*
RD-8.1.1 CA/RA: All user access must be restricted to actions authorized for that role ***Note:*** *Examples of how access can be restricted include the use of CA software, operating-system, and procedural controls.*	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-8.1.1.a Examine documented procedures to confirm that access to material that can be used to construct secret and private keys must be restricted to actions authorized for that role.	*<Report Findings Here>*
RD-8.1.1.b Observe user role assignments and access-control mechanisms to verify that access to material that can be used to construct secret and private keys is restricted to actions authorized for that role.	*<Report Findings Here>*
RD-8.2 CA/RA: The system enforces an explicit and well-defined certificate security policy and certification practice statement (as required in RD-9.2 and RD-9.3). This must include the following:	
RD-8.2.1 CA systems that issue certificates to other CAs and KDHs must be operated offline using a dedicated closed network (not a network segment). The network must only be used for certificate issuance and/or revocation. Outside network access shall exist only for the purposes of "pushing" certificate-status information to relying parties (for example, KDHs). ***Note:*** *Requirements for CA systems that issue certificates to POIs are covered at RD-8.6.*	
RD-8.2.1 Examine network diagrams and observe network and system configurations to verify: CA systems that issue certificates to other CAs and KDHs are operated offline using a dedicated closed network (not a network segment). The network is only used for certificate issuance and/or revocation, or both certificate issuance and revocation. Outside network access shall exist only for the purposes of "pushing" certificate-status information to relying parties (for example, KDHs).	*<Report Findings Here>*
RD-8.2.2 No CA or Registration Authority (RA) software updates are done over the network (local console access must be used for CA or RA software updates).	
RD-8.2.2 Examine software update processes to verify that local console access is used for all CA or RA software updates.	*<Report Findings Here>*
RD-8.2.3 Non-console access requires two-factor authentication. This also applies to the use of remote console access.	
RD-8.2.3 Examine remote access mechanisms and system configurations to verify that all non-console access, including remote access, requires two-factor authentication.	*<Report Findings Here>*
RD-8.2.4 Non-console user access to the CA or RA system environments shall be protected by authenticated encrypted sessions. No other remote access is permitted to the host platform(s) for system or application administration. ***Note:*** *Access for monitoring only (no create, update, delete capability) of online systems may occur without restriction.*	
RD-8.2.4.a Examine non-console access mechanisms and system configurations to verify that all non-console user access is protected by authenticated encrypted sessions.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-8.2.4.b Observe an authorized CA personnel attempt non-console access to the host platform without the authenticated encrypted session to verify that non-console access is not permitted.	*<Report Findings Here>*
RD-8.2.5 CA certificate (for SCD/KDH authentication and validity status checking) signing keys must only be enabled under at least dual control. ***Note:*** *Certificate requests may be vetted (approved) using single user logical access to the RA application.*	
RD-8.2.5.a Examine certificate security policy and certification practice statement to verify that CA certificate-signing keys must only be enabled under at least dual control.	*<Report Findings Here>*
RD-8.2.5.b Observe certificate-signing processes to verify that signing keys are enabled only under at least dual control.	*<Report Findings Here>*
RD-8.3 CA/RA: The CA shall require a separation of duties for critical CA functions to prevent one person from maliciously using a CA system without detection, the practice referred to as "dual control." At a minimum, there shall be multi-person control for operational procedures such that no one person can gain control over the CA signing key(s).	
RD-8.3.a Examine documented procedures to verify they include following: • Critical functions of the CA are defined. • Separation of duties is required to prevent one person from maliciously using a CA system without detection. • At a minimum, multi-person control is required for operational procedures such that no one person can gain control over the CA signing key(s).	*<Report Findings Here>*
RD-8.3.b Observe CA operations and interview responsible personnel to verify: • Critical functions of the CA are identified. • Separation of duties is required to prevent one person from maliciously using a CA system without detection. • At a minimum, multi-person control is required for operational procedures such that no one person can gain control over the CA signing key(s).	*<Report Findings Here>*
RD-8.4 CA/RA: CA systems must be hardened to include: • Services that are not necessary or that allow non-secure access (for example, rlogin, rshell, telnet, ftp, etc.) must be removed or disabled. • Unnecessary ports must also be disabled. • Documentation must exist to support the enablement of all active services and ports.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-8.4.a Examine system documentation to verify the following is required: • Services that are not necessary or that allow non-secure access (for example, rlogin, rshell, etc., commands in Unix) must be removed or disabled. • Unnecessary ports must also be disabled. • Documentation must exist to support the enablement of all active services and ports.	*<Report Findings Here>*
RD-8.4.b For a sample of systems, examine documentation supporting the enablement of active services and ports, and observe system configurations to verify: • Services that are not necessary or that allow non-secure access (for example, rlogin, rshell, etc., commands in Unix) are removed or disabled. • Unnecessary ports are disabled. • There is documentation to support all active services and ports.	*<Report Findings Here>*
RD-8.4.1 CA/RA: Vendor-default IDs that are required only as owners of objects or processes, or for installation of patches and upgrades, must be disabled from login except as necessary for a documented and specific business reason.	
RD-8.4.1.a Examine documented procedures to verify that vendor-default IDs required as owners of objects or processes, or for installation of patches and upgrades, must be disabled from login except as necessary for a documented and specific business reason.	*<Report Findings Here>*
RD-8.4.1.b Examine system configurations and interview responsible personnel to verify that vendor-default IDs required as owners of objects or processes, or for installation of patches and upgrades, are disabled from login except as necessary for a documented and specific business reason.	*<Report Findings Here>*
RD-8.4.2 Vendor defaults (for example, passwords, SNMP strings, and IDs such as “Guest”) must be changed, removed, or disabled before installing a system on the network.	
RD-8.4.2.a Examine documented procedures to verify that vendor defaults (for example, passwords, SNMP strings, and IDs such as “Guest”) must be changed, removed, or disabled before installing a system on the network.	*<Report Findings Here>*
RD-8.4.2.b Examine system configurations and interview responsible personnel to verify that vendor defaults (for example, passwords, SNMP strings, and IDs such as “Guest”) are changed, removed, or disabled before installing a system on the network.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-8.5 CA/RA: Audit trails must include but not be limited to the following: • All key-management operations, such as key generation, loading, transmission, backup, recovery, compromise, and destruction and certificate generation or revocation • The identity of the person authorizing the operation • The identities of all persons handling any key material (such as key components or keys stored in portable devices or media)	
RD-8.5.a Examine system configurations and audit trails to verify that all key-management operations are logged.	*<Report Findings Here>*
RD-8.5.b For a sample of key-management operations, examine audit trails to verify they include: • The identity of the person authorizing the operation • The identities of all persons handling any key material	*<Report Findings Here>*
RD-8.5.1 Audit logs must be archived for a minimum of two years.	
RD-8.5.1 Examine audit trail files to verify that audit trails are archived for a minimum of two years.	*<Report Findings Here>*
RD-8.5.2 Records pertaining to certificate issuance and revocation must at a minimum be retained for the life of the associated certificate.	
RD-8.5.2.a For a sample of certificate issuances, examine audit records to verify that the records are retained for at least the life of the associated certificate.	*<Report Findings Here>*
RD-8.5.2.b For a sample of certificate revocations, examine audit records to verify that the records are retained for at least the life of the associated certificate.	*<Report Findings Here>*
RD-8.5.3 Logical events are divided into operating-system and CA application events. For both events the following must be recorded in the form of an audit record: Date and time of the event, Identity of the entity and/or user that caused the event, Type of event, and Success or failure of the event.	
RD-8.5.3.a Examine audit trails to verify that logical events are divided into operating-system and CA application events.	*<Report Findings Here>*
RD-8.5.3.b Examine a sample of operating system logs to verify they contain the following information: Date and time of the event, Identity of the entity and/or user that caused the event, Type of event, and Success or failure of the event.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-8.5.3.c Examine a sample of application logs to verify they contain the following information: Date and time of the event, Identity of the entity and/or user that caused the event, Type of event, and Success or failure of the event.	*<Report Findings Here>*
RD-8.5.4 Mechanisms must be in place to prevent and detect attempted tampering of CA application and operating system logs. *For example: A digital signature or a symmetric MAC (based on TDES) may be used to protect logs from alteration.*	
RD-8.5.4 Examine log security controls to verify that mechanisms are in place to prevent and detect attempted tampering of application and operating system logs.	*<Report Findings Here>*
RD-8.6 CA/RA: Certificate-processing systems may only be operated on-line for the issuance of certificates to POIs.	
RD-8.6.a Examine certificate security policy and certification practice statement to verify that certificate-processing systems are only operated on-line for the issuance of certificates to POIs.	*<Report Findings Here>*
RD-8.6.b Examine certificate-processing systems to verify they are only operated on-line for the issuance of certificates to POIs.	*<Report Findings Here>*
RD-8.6.1 Online certificate-processing system components must be protected by a firewall(s) from all unauthorized access, including casual browsing and deliberate attacks. Firewalls must minimally be configured to: Deny all services not explicitly permitted. Disable or remove all unnecessary services, protocols, and ports. Fail to a configuration that denies all services, and require a firewall administrator to re-enable services after a failure. Disable source routing on the firewall and external router. Not accept traffic on its external interfaces that appears to be coming from internal network addresses. Notify the firewall administrator in near real time of any item that may need immediate attention such as a break-in, little disk space available, or other related messages so that an immediate action can be taken. Run on a dedicated computer: All non-firewall related software, such as compilers, editors, communications software, etc., must be deleted or disabled.	
RD-8.6.1.a Examine network and system configurations to verify that on-line certificate-processing system are protected from unauthorized access by firewall(s).	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-8.6.1.b Examine firewall configurations to verify they are configured to: Deny all services not explicitly permitted. Disable or remove all unnecessary services, protocols, and ports. Fail to a configuration that denies all services, and require a firewall administrator to re-enable services after a failure. Disable source routing on the firewall and external router. Not accept traffic on its external interfaces that appears to be coming from internal network addresses. Notify the firewall administrator in near real time of any item that may need immediate attention such as a break-in, little disk space available, or other related messages so that an immediate action can be taken. Run on a dedicated computer: All non-firewall related software, such as compilers, editors, communications software, etc., must be deleted or disabled.	*<Report Findings Here>*
RD-8.6.2 Online certificate-processing systems must employ individually or in combination network and host-based intrusion detection systems (IDS) to detect inappropriate access. At a minimum, database servers and the application servers for RA and web, as well as the intervening segments, must be covered.	
RD-8.6.2.a Observe network-based and/or host-based IDS configurations to verify that on-line certificate-processing systems are protected by IDS to detect inappropriate access.	*<Report Findings Here>*
RD-8.6.2.b Verify that IDS coverage includes all database servers, RA application servers and web servers, as well as the intervening segments.	*<Report Findings Here>*
RD-8.7 CA/RA: Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system-hardening standards.	
RD-8.7.a Examine system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.	*<Report Findings Here>*
RD-8.7.b Verify system configuration standards address all known security vulnerabilities.	*<Report Findings Here>*
RD-8.7.c Examine a sample of system configurations to verify that system configuration standards are applied when new systems are configured.	*<Report Findings Here>*
RD-8.8 CA/RA: Implement user-authentication management for all system components as follows:	
RD-8.8.1 Employ at least one of the following methods to authenticate all users: Something you know, such as a password or pass phrase Something you have, such as a token device or smart card Something you are, such as a biometric	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-8.8.1.a Examine documented procedures to verify that at least one of the defined authentication methods is required to authenticate all users to CA processing systems.	*<Report Findings Here>*
RD-8.8.1.b Examine system configurations and observe authorized personnel authenticate to CA processing systems to verify that at least one of the defined authentication methods is used to authenticate all users to CA processing systems.	*<Report Findings Here>*
RD-8.8.2 Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.	
RD-8.8.2 Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use.	*<Report Findings Here>*
RD-8.8.3 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	
RD-8.8.3.a For a sample of system components, examine user ID lists to verify the following: Generic user IDs and accounts are disabled or removed. Shared user IDs for system administration activities and other critical functions do not exist. Shared and generic user IDs are not used to administer any system components.	*<Report Findings Here>*
RD-8.8.3.b Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.	*<Report Findings Here>*
RD-8.8.3.c Interview system administrators to verify that group and shared passwords or other authentication methods are not distributed, even if requested.	*<Report Findings Here>*
RD-8.8.4 Change user passwords at least every 30 days.	
RD-8.8.4 For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 30 days.	*<Report Findings Here>*
RD-8.8.5 Require a minimum password length of at least eight characters.	
RD-8.8.5 For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least eight characters long.	*<Report Findings Here>*
RD-8.8.6 Use passwords containing numeric, alphabetic, and special characters.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-8.8.6 For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain numeric, alphabetic, and special characters.	*<Report Findings Here>*
RD-8.8.7 Limit repeated access attempts by locking out the user ID after not more than five attempts.	
RD-8.8.7 For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than five invalid logon attempts.	*<Report Findings Here>*
RD-8.8.8 Passwords are not stored on any of the systems except in encrypted form or as part of a proprietary one-way transformation process, such as those used in UNIX systems.	
RD-8.8.8 For a sample of system components, obtain and inspect system configuration settings to verify that passwords are not stored unless encrypted as part of a proprietary one-way hash.	*<Report Findings Here>*
RD-8.8.9 The embedding of passwords in shell scripts, command files, communication scripts, etc., is strictly prohibited.	
RD-8.8.9 For a sample of system components, obtain and inspect system configuration settings to verify that passwords are not embedded in shell scripts, command files, or communication scripts.	*<Report Findings Here>*
RD-8.8.10 Where log-on security tokens (for example, smart cards) are used, the security tokens must have an associated usage-authentication mechanism, such as a biometric or associated PIN/pass phrase to enable their usage. The PIN/pass phrase must be at least eight decimal digits in length, or equivalent. ***Note:*** *Log-on security tokens (for example, smart cards) and encryption devices are not subject to the pass-phrase management requirements for password expiry as stated above.*	
RD-8.8.10.a If log-on security tokens are used, observe devices in use to verify that the security tokens have an associated usage-authentication mechanism, such as a biometric or associated PIN/pass phrase to enable their usage.	*<Report Findings Here>*
RD-8.8.10.b Examine token-configuration settings to verify parameters are set to require PINs/passwords be at least eight decimal digits in length, or equivalent.	*<Report Findings Here>*
RD-8.9 CA/RA: Implement a method to synchronize all critical system clocks and times for all systems involved in key-management operations, including any physical access to the CA environment. If the synchronization process is manual, ensure that it occurs at least quarterly.	
RD-8.9.a Examine documented procedures and system configuration standards to verify a method is defined to synchronize all critical system clocks and times for: • All systems involved in key-management operations • Any physical access to the CA environment	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-8.9.b For a sample of critical systems, review the time-related system parameters to verify that system clocks and times are synchronized for: • All systems involved in key-management operations • Any physical access to the CA environment	*<Report Findings Here>*
RD-8.9.c If a manual process is defined, verify that the documented procedures require that it occurs at least quarterly.	*<Report Findings Here>*
RD-8.9.d If a manual process is defined, examine system configurations and synchronization logs to verify that the process occurs at least quarterly.	*<Report Findings Here>*
RD-9 Documented procedures must exist and must be demonstrably in use for all key-administration operations. *(Reference 6F-8)*	
RD-9.1 CA/RA: CA operations must be dedicated to certificate issuance and management. All physical and logical CA system components must be separated from key-distribution systems.	
RD-9.1.a Examine documented procedures to verify: • CA operations must be dedicated to certificate issuance and management. • All physical and logical CA system components must be separated from key-distribution systems.	*<Report Findings Here>*
RD-9.1.b Observe CA system configurations and operations to verify they are dedicated to certificate issuance and management.	*<Report Findings Here>*
RD-9.1.c Observe system and network configurations, and physical access controls to verify that all physical and logical CA system components are separated from key-distribution systems.	*<Report Findings Here>*
RD-9.2 CA/RA: Each CA operator must develop a certification practice statement (CPS). (See *RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* for an example of content.) • The CPS must be consistent with the requirements described within this document. • The CA shall operate in accordance with its CPS. ***Note:*** *This may take the form of a declaration by the CA operator of the details of its trustworthy system and the practices it employs in its operations and in support of the issuance of certificates. A CPS may take the form of either a specific, single document or a collection of specific documents.*	
RD-9.2.a Examine documented certification practice statement (CPS) to verify that the CPS is consistent with the requirements described within this document.	*<Report Findings Here>*
RD-9.2.b Examine documented operating procedures to verify they are defined in accordance with the CPS.	*<Report Findings Here>*
RD-9.2.c Interview personnel and observe CA processes to verify that CA operations are in accordance with its CPS.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-9.3 CA/RA: Each CA operator must develop a certificate policy. (See *RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* for an example of content.)	
RD-9.3.a Examine documented certificate policy to verify that the CA has one in place.	*<Report Findings Here>*
RD-9.3.b Examine documented operating procedures to verify they are defined in accordance with the certificate policy.	*<Report Findings Here>*
RD-9.3.c Interview personnel and observe CA processes to verify that CA operations are in accordance with its certificate policy.	*<Report Findings Here>*
RD-9.4 CA/RA: Documented procedures exist and are demonstrably in use by CAs to validate the identity of the certificate requestor and recipient before issuing a digital certificate for the recipient's associated public key.	
RD-9.4.a Examine documented procedures to verify they include validating the identity of the certificate requestor and recipient before issuing a digital certificate for the recipient's associated public key.	*<Report Findings Here>*
RD-9.4.b Observe certificate issuing processes to verify that the identity of the certificate requestor and recipient are validated before issuing a digital certificate for the recipient's associated public key.	*<Report Findings Here>*
RD-9.4.1 For CA and KDH certificate-signing requests, including certificate or key-validity status changes (for example, revocation. suspension, replacement), verification must include validation that: The entity submitting the request is who it claims to be. The entity submitting the request is authorized to submit the request on behalf of the certificate request's originating entity. The entity submitting the request has a valid business relationship with the issuing authority (for example, the vendor) consistent with the certificate being requested. The certificate-signing request has been transferred from the certificate request's originating entity to the RA in a secure manner.	
RD-9.4.1.a Examine documented procedures to verify that certificate-signing requests, including certificate or key-validity status changes, require validation that: The entity submitting the request is who it claims to be. The entity submitting the request is authorized to submit the request on behalf of the certificate request's originating entity. The entity submitting the request has a valid business relationship with the issuing authority (for example, the vendor) consistent with the certificate being requested. The certificate-signing request has been transferred from the certificate request's originating entity to the RA in a secure manner.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-9.4.1.b Observe certificate-signing requests, including certificate or key-validity status changes, to verify they include validation that: The entity submitting the request is who it claims to be. The entity submitting the request is authorized to submit the request on behalf of the certificate request's originating entity. The entity submitting the request has a valid business relationship with the issuing authority (for example, the vendor) consistent with the certificate being requested. The certificate-signing request has been transferred from the certificate request's originating entity to the RA in a secure manner.	*<Report Findings Here>*
RD-9.4.2 RAs must retain documentation and audit trails relating to the identification of entities for all certificates issued and certificates whose status had changed for the life of the associated certificates.	
RD-9.4.2 Examine documentation and audit trails to verify that the identification of entities is retained for the life of the associated certificates: For all certificates issued For all certificates whose status had changed	*<Report Findings Here>*
RD-10 Certificate and Registration Authorities must implement physical security to reduce the risk of compromise of their systems. Physical security must be implemented to provide three tiers of physical security, as indicated below.	
RD-10.1 The certificate-processing operations center must implement a three-tier physical security boundary, as follows: • Level One Barrier – Consists of the entrance to the facility. • Level Two Barrier – Secures the entrance beyond the foyer/reception area to the CA facility. • Level Three Barrier – Provides access to the physically secure, dedicated room housing the CA and RA database and application servers and cryptographic devices.	
RD-10.1.a Examine physical security policies to verify three tiers of physical security are defined as follows: • Level One Barrier – The entrance to the facility. • Level Two Barrier – The entrance beyond the foyer/reception area to the CA facility. • Level Three Barrier – Access to the physically secure, dedicated room housing the CA and RA database and application servers and cryptographic devices	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-10.1.b Observe the physical facility to verify three tiers of physical security are implemented as follows: • Level One Barrier – The entrance to the facility. • Level Two Barrier – The entrance beyond the foyer/reception area to the CA facility. • Level Three Barrier – Access to the physically secure, dedicated room housing the CA and RA database and application servers and cryptographic devices	*<Report Findings Here>*
RD-10.2 The entrance to the CA facility/building must include the following controls:	
RD-10.2.1 The facility entrance only allows authorized personnel to enter the facility.	
RD-10.2.1.a Examine physical-security procedures and policies to verify they require that the facility entrance only allows authorized personnel to enter the facility.	*<Report Findings Here>*
RD-10.2.1.b Observe the facility entrance and observe personnel entering the facility to verify that only authorized personnel are allowed to enter the facility.	*<Report Findings Here>*
RD-10.2.2 The facility has a guarded entrance or a foyer with a receptionist.	
RD-10.2.2.a Examine physical-security procedures and policies to verify they require that the facility have a guarded entrance or a foyer with a receptionist.	*<Report Findings Here>*
RD-10.2.2.b Observe the facility entrance to verify it has a guarded entrance or a foyer with a receptionist.	*<Report Findings Here>*
RD-10.2.3 Visitors (guests) to the facility must be authorized and be registered in a logbook.	
RD-10.2.3.a Examine physical-security procedures and policies to verify they require visitors to the facility to be authorized and be registered in a logbook.	*<Report Findings Here>*
RD-10.2.3.b Observe the facility entrance and observe personnel entering the facility to verify that visitors are authorized and registered in a logbook.	*<Report Findings Here>*
RD-10.3 The Level 2 barrier/entrance must only allow authorized personnel beyond this entrance.	
RD-10.3.a Examine physical-security procedures and policies to verify that only authorized personnel are allowed beyond the level 2 barrier/entrance.	*<Report Findings Here>*
RD-10.3.b Observe personnel entering the Level 2 barrier/entrance to verify that only authorized personnel are allowed through.	*<Report Findings Here>*
RD-10.3.1 Visitors must be authorized and escorted at all times within the Level 2 environment.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-10.3.1.a Examine documented policies and procedures to verify that authorized visitors must be escorted at all times within the Level 2 environment.	*<Report Findings Here>*
RD-10.3.1.b Interview CA personnel and observe visitors entering the environment to verify that visitors are authorized and escorted at all times within the Level 2 environment.	*<Report Findings Here>*
RD-10.3.2 Access logs must record all personnel entering the Level 2 environment. ***Note:*** *The logs may be electronic, manual, or both.*	
RD-10.3.2.a Examine documented policies and procedures to verify that access logs are required to record all personnel entering the Level 2 environment.	*<Report Findings Here>*
RD-10.3.2.b Observe personnel entering the Level 2 barrier and review corresponding access logs to verify that all entry through the Level 2 barrier is logged.	*<Report Findings Here>*
RD-10.4 The Level 2 entrance must be monitored by a video-recording system.	
RD-10.4.a Observe the Level 2 entrance to verify that a video-recording system is in place.	*<Report Findings Here>*
RD-10.4.b Review a sample of recorded footage to verify that the video-recording system captures all entry through the Level 2 entrance.	*<Report Findings Here>*
RD-10.5 The Level 3 environment must consist of a physically secure, dedicated room not used for any other business activities but certificate operations. ***Note:*** *All certificate-processing operations must operate in the Level 3 environment.*	
RD-10.5.a Examine documented policies and procedures to verify that all certificate-processing systems must be located within a Level 3 environment.	*<Report Findings Here>*
RD-10.5.b Examine physical locations of certificate operations to verify that all certificate-processing systems are located within a Level 3 secure room.	*<Report Findings Here>*
RD-10.5.c Observe operations and interview personnel to confirm that the Level 3 secure room is not used for any business activity other than certificate operations.	*<Report Findings Here>*
RD-10.5.1 Doors to the Level 3 area must have locking mechanisms.	
RD-10.5.1 Observe Level 3 environment entrances to verify that all doors to the Level 3 environment have locking mechanisms.	*<Report Findings Here>*
RD-10.5.2 The Level 3 environment must have true floor-to-ceiling (slab-to-slab) walls, or use solid materials (such as steel mesh or bars) below floors and above ceilings to protect against intrusions. (For example, the Level 3 environment may be implemented within a "caged" environment.)	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-10.5.2.a Examine physical security documentation for the Level 3 environment to verify that true floor-to-ceiling walls, or enclosure on all sides with solid materials (such as steel mesh or bars), including below floors and above ceilings, is required.	*<Report Findings Here>*
RD-10.5.2.b Examine the physical boundaries of the Level 3 environment to verify that it has true floor-to-ceiling walls, or is enclosed on all sides with solid materials (such as steel mesh or bars), including below floors and above ceilings.	*<Report Findings Here>*
RD-10.6 Documented procedures must exist for: • Granting, revocation, and review of access privileges • Specific access authorizations, whether logical or physical	
RD-10.6.a Examine documented procedures to verify they include the following: • Granting, revocation, and review of access privileges • Specific access authorizations, whether logical or physical	*<Report Findings Here>*
RD-10.6.b Interview responsible personnel to verify that the documented procedures are followed for: • Granting, revocation, and review of access privileges • Specific access authorizations, whether logical or physical	*<Report Findings Here>*
RD-10.6.1 The Level 3 entrance requires dual access, as follows: • Personnel with access must be divided into an "A" group and a "B" group, such that access requires at least one member from each group. • The A and B groups must correlate to separate organizational units.	
RD-10.6.1.a Examine documented access-control procedures to verify they require dual access to the Level 3 environment, as follows: Personnel with access are divided into an "A" group and a "B" group. Access requires at least one member from the "A" group and the "B" group. The "A" and "B" groups must correlate to separate organizational units.	*<Report Findings Here>*
RD-10.6.1.b Examine Level 3 access controls to verify that: All personnel with access are included in either the "A" group or the "B" group. Access requires at least one member from the "A" group and one from the "B" group.	*<Report Findings Here>*
RD-10.6.1.c Examine organizational charts and interview a sample of personnel from the "A" and "B" groups to verify that the groups correlate to separate organizational units.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-10.6.2 All authorized personnel with access through the Level 3 barrier must: Have successfully completed a background security check. Be assigned resources (staff, dedicated personnel) of the CA operator with defined business needs and duties. ***Note:*** *This requirement applies to all personnel with pre-designated access to the Level 3 environment.*	
RD-10.6.2.a Examine documented policies and procedures to verify they require personnel authorized as having access through the Level 3 barrier to: Have successfully completed a background security check. Be assigned resources of the CA operator with defined business needs and duties.	*<Report Findings Here>*
RD-10.6.2.b Interview responsible HR personnel to verify that background checks are conducted (within the constraints of local laws) on CA personnel prior such personnel being authorized for access through the Level 3 barrier.	*<Report Findings Here>*
RD-10.6.2.c Interview a sample of personnel authorized for access through the Level 3 barrier to verify that they are assigned resources of the CA with defined business needs and duties.	*<Report Findings Here>*
RD-10.6.3 Other personnel requiring entry to this level (who have not been authorized per RD-10.6.2 above) must be accompanied by two (2) authorized and assigned resources at all times.	
RD-10.6.3.a Examine documented policies and procedures to verify that personnel requiring entry to this level (who have not been authorized per RD-10.6.2 above) must be accompanied by two (2) authorized and assigned resources at all times.	*<Report Findings Here>*
RD-10.6.3.b Interview a sample of responsible personnel to verify that personnel requiring entry to this level (who have not been authorized per RD-10.6.2 above) are accompanied by two (2) authorized and assigned resources at all times.	*<Report Findings Here>*
RD-10.7 The Level 3 environment must require dual-control access and dual-occupancy such that the room is never occupied by a single individual for more than thirty (30) seconds. *For example: The Level 3 room is never occupied by a single individual except during the time of entry and/or exit, and the period for entry/exit does not exceed 30 seconds.*	
RD-10.7.a Examine documented policies and procedures to verify that the Level 3 environment requires dual-control access and dual-occupancy such that the room is never occupied by a single individual for more than thirty (30) seconds.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-10.7.b Observe authorized personnel access the Level 3 environment to verify that dual-control access and dual-occupancy is enforced such that the room is never occupied by a single individual for more than thirty (30) seconds.	*<Report Findings Here>*
RD-10.7.1 The mechanism for enforcing dual-control and dual-occupancy must be automated	
RD-10.7.1.a Examine documented policies and procedures to verify that the defined enforcement mechanism is automated.	*<Report Findings Here>*
RD-10.7.1.b Observe enforcement mechanism configuration to verify it is automated.	*<Report Findings Here>*
RD-10.7.2 The system must enforce anti-pass-back.	
RD-10.7.2.a Examine documented policies and procedures to verify that the system is required to enforce anti-pass-back.	*<Report Findings Here>*
RD-10.7.2.b Observe mechanisms in use and authorized personnel within the environment to verify that anti-pass-back is enforced.	*<Report Findings Here>*
RD-10.7.3 Dual occupancy requirements are managed using electronic (for example, badge, and/or biometric) systems.	
RD-10.7.3.a Examine documented policies and procedures to verify that dual occupancy requirements are defined to be managed using electronic (for example, badge and/or biometric) systems.	*<Report Findings Here>*
RD-10.7.3.b Observe mechanisms in use and authorized personnel within the environment to verify that dual-occupancy requirements are managed using electronic systems.	*<Report Findings Here>*
RD-10.7.4 Any time a single occupancy exceeds 30 seconds, the system must automatically generate an audit event that is followed up by security personnel.	
RD-10.7.4.a Examine documented policies and procedures to verify that the system must automatically generate an audit event that is followed up by security personnel, any time a single occupancy exceeds 30 seconds.	*<Report Findings Here>*
RD-10.7.4.b Observe mechanisms in use to verify that the system automatically generates an audit event when single occupancy exceeds 30 seconds.	*<Report Findings Here>*
RD-10.7.4.c Examine a sample of audit events and interview security personnel to verify that the audit events are followed up by security personnel.	*<Report Findings Here>*
RD-10.8 Access to the Level 3 room must create an audit event, which must be logged.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-10.8 Observe authorized personnel enter the environment and examine correlating audit logs to verify that access to the Level 3 room creates an audit log event.	*<Report Findings Here>*
RD-10.8.1 Invalid access attempts to the Level 3 room must create audit records, which must be followed up by security personnel.	
RD-10.8.1 Observe authorized personnel perform an invalid access attempt and examine correlating audit logs to verify that invalid access attempts to the Level 3 room create an audit log event.	*<Report Findings Here>*
RD-10.9 The Level 3 environment must be monitored as follows:	
RD-10.9.1 One or more cameras must provide continuous monitoring (for example, CCTV system) of the Level 3 environment, including the entry and exit. ***Note:*** *Motion-activated systems that are separate from the intrusion-detection system may be used to activate recording activity.*	
RD-10.9.1.a Observe the Level 3 physical environment to verify that cameras are in place to monitor the Level 3 environment, including the entry and exit.	*<Report Findings Here>*
RD-10.9.1.b Examine monitoring system configurations (e.g., CCTV systems) to verify that continuous monitoring is provided.	*<Report Findings Here>*
RD-10.9.1.c If motion-activated systems are used for monitoring, observe system configurations for the motion-activated systems to verify they are separate from the intrusion-detection system.	*<Report Findings Here>*
RD-10.9.2 The cameras must record to time-lapse VCRs or similar mechanisms, with a minimum of five frames equally recorded over every three seconds.	
RD-10.9.2 Examine monitoring system configurations to verify; The system records to time-lapse VCRs or similar mechanisms. A minimum of five frames are recorded every three seconds.	*<Report Findings Here>*
RD-10.9.3 Continuous, or motion-activated, appropriate lighting must be provided for the cameras. ***Note:*** *Visible spectrum lighting may not be necessary if the cameras do not require such lighting to capture images (for example, if intra-red cameras are used).*	
RD-10.9.3.a Observe the Level 3 physical environment to verify that continuous or motion-activated lighting is provided for the cameras monitoring the environment.	*<Report Findings Here>*
RD-10.9.3.b Examine a sample of captured footage from different days and times to ensure that the lighting is adequate.	*<Report Findings Here>*
RD-10.9.4 Surveillance cameras must be configured to prevent the monitoring of computer screens, keyboards, PIN pads, or other systems which may expose sensitive data.	
RD-10.9.4.a Observe camera locations in the Level 3 environment to verify they are not set to monitor computer screens, keyboards, PIN pads, or other systems that may expose sensitive data.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-10.9.4.b Examine a sample of captured footage to verify it does not allow for the monitoring of computer screens, keyboards, PIN pads, or other systems that may expose sensitive data.	*<Report Findings Here>*
RD-10.9.5 Personnel with access to the Level 3 environment must not have access to the media (for example, VCR tapes, digital-recording systems, etc.) with the recorded surveillance data.	
RD-10.9.5.a Examine documented access policies and procedures to verify that personnel with access to the Level 3 environment are not permitted to have access to the media containing recorded surveillance data for that environment.	*<Report Findings Here>*
RD-10.9.5.b Examine Level 3 access lists as well as access controls to the media containing surveillance data, to verify that personnel with access to the Level 3 environment do not have access to the media containing recorded surveillance data.	*<Report Findings Here>*
RD-10.9.6 Images recorded from the CCTV system must be securely archived for a period of no less than 45 days. If digital-recording mechanisms are used, they must have sufficient storage capacity and redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.	
RD-10.9.6.a Examine storage of captured recordings to verify that at least the most recent 45 days of images are securely archived.	*<Report Findings Here>*
RD-10.9.6.b If digital-recording mechanisms are used, examine system configurations to verify that the systems have sufficient redundancy to prevent the loss of information necessary to reconstruct events for the most recent 45-day period.	*<Report Findings Here>*
RD-10.10 The environment must have continuous (24/7) intrusion-detection systems in place, which protect the secure area by motion detectors when unoccupied.	
RD-10.10.a Examine security policies and procedures to verify they require: • Continuous (24/7) intrusion-detection monitoring of the Level 3 environment • Motion detectors must be active when the environment is unoccupied	*<Report Findings Here>*
RD-10.10.b Examine intrusion-detection system configurations to verify: • Continuous (24/7) intrusion-detection monitoring of the Level 3 environment is in place • Motion detectors are active when the environment is unoccupied	*<Report Findings Here>*
RD-10.10.1 Any windows in the secure area must be locked and protected by alarmed sensors.	
RD-10.10.1.a Observe all windows in the secure areas to verify they are locked and protected by alarmed sensors.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-10.10.1.b Examine configuration of window sensors to verify that the alarm mechanism is active.	*<Report Findings Here>*
RD-10.10.2 Any windows must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.	
RD-10.10.2 Observe all windows in the secure areas to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.	*<Report Findings Here>*
RD-10.10.3 The intrusion-detection system(s) must be connected to the alarm system and automatically activated every time all authorized personnel have exited the secure area.	
RD-10.10.3.a Examine security system configurations to verify: The intrusion-detection system(s) is connected to the alarm system. The intrusion-detection system(s) is automatically activated every time all authorized personnel have exited the secure area.	*<Report Findings Here>*
RD-10.10.3.b Observe a system test to verify that the intrusion-detection system(s) activates the alarm if a person is detected in the Level 3 area when the system is activated.	*<Report Findings Here>*
RD-10.10.4 Alarm activity must include unauthorized entry attempts or any actions that disable the intrusion-detection system.	
RD-10.10.4 Examine security-system configurations to verify that an alarm event is generated for: Unauthorized entry attempts Actions that disable the intrusion-detection system	*<Report Findings Here>*
RD-10.11 All personnel (including CA personnel and visitors) must sign an access logbook when entering the Level 3 environment. ***Note:*** *The logs may be electronic, manual, or both.*	
RD-10.11.a Examine security policies and procedures to verify they require all personnel (including CA personnel and visitors) to sign an access logbook when entering the Level 3 environment.	*<Report Findings Here>*
RD-10.11.b For a sample of personnel authorized to access the Level 3 environment, examine the access logbook to verify that they signed in when entering the Level 3 environment.	*<Report Findings Here>*
RD-10.11.1 The access log must include the following details: Name and signature of the individual Organization Date and time in and out Reason for access or purpose of visit For visitor access, the initials of the person escorting the visitor	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-10.11.1 Examine the access logbook to verify it contains the following information: Name and signature of the individual Organization Date and time in and out Reason for access or purpose of visit For visitor access, the initials of the person escorting the visitor	*<Report Findings Here>*
RD-10.11.2 The logbook must be maintained within the Level 3 secure environment.	
RD-10.11.2 Observe the location of the access logbook and verify that it is maintained within the Level 3 secure environment.	*<Report Findings Here>*
RD-10.12 All access-control and monitoring systems (including intrusion detection systems) are powered through an uninterruptible power source (UPS).	
RD-10.12 Inspect uninterruptible power source (UPS) system configurations to verify that all access-control and monitoring systems, including intrusion-detection systems, are powered through the UPS.	*<Report Findings Here>*
RD-10.13 All alarm events must be documented.	
RD-10.13.a Examine security policies and procedures to verify they require that all alarm events are logged.	*<Report Findings Here>*
RD-10.13.b Examine security-system configurations and documented alarm events to verify that all alarm events are logged.	*<Report Findings Here>*
RD-10.13.1 Under no circumstances shall an individual sign off on an alarm event in which they were involved.	
RD-10.13.1.a Examine documented procedures for responding to alarm events to verify that the procedure does not permit a person who was involved in an alarm event to sign-off on that alarm event.	*<Report Findings Here>*
RD-10.13.1.b For a sample of documented alarm events, interview personnel who signed off on the event to verify that person was not involved in the event.	*<Report Findings Here>*
RD-10.13.2 The use of any emergency entry or exit mechanism must cause an alarm event.	
RD-10.13.2 Examine security system configurations to verify that an alarm event is generated upon use of any emergency entry or exit mechanism.	*<Report Findings Here>*
RD-10.13.3 All alarms for physical intrusion necessitate an active response within 30 minutes by personnel assigned security duties.	
RD-10.13.3.a Review documented procedures to verify they require that all alarms for physical intrusion must be responded to within 30 minutes by personnel assigned security duties.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex A Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
RD-10.13.3.b Examine a sample of alarm events and interview personnel assigned with security-response duties to verify that alarms for physical intrusion are responded to within 30 minutes.	*<Report Findings Here>*
RD-10.14 A process must be implemented for synchronizing the time and date stamps of the access, intrusion-detection, and monitoring (camera) systems to ensure accuracy of logs. ***Note:*** *This may be done by either automated or manual mechanisms.*	
RD-10.14.a Examine documented procedures to verify that mechanisms are defined (may be automated or manual) for synchronizing the time and date stamps of the access, intrusion-detection, and monitoring (camera) systems to ensure accuracy of logs.	*<Report Findings Here>*
RD-10.14.b Examine system configurations for access, intrusion-detection, and monitoring (camera) systems to verify that time and date stamps are synchronized.	*<Report Findings Here>*
RD-10.14.c Examine a sample of logs from the access, intrusion-detection, and monitoring (camera) systems to verify log time and date stamps are synchronized.	*<Report Findings Here>*
RD-10.14.1 If a manual synchronization process is used, synchronization must occur at least quarterly, and documentation of the synchronization must be retained for at least a one-year period.	
RD-10.14.1.a If a manual synchronization process is implemented, interview responsible personnel an examine records of synchronization to verify the mechanism is performed at least quarterly.	*<Report Findings Here>*
RD-10.14.1.b Examine records of the synchronization process to verify that documentation is retained for at least one year.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

Domain 6 Annex B: Cryptographic Key Operations – Key-Injection Facilities

Table 6B.1 – List of keys (by type) loaded onto POI devices via key-injection		
Key type / description*	Purpose/ function of the key (including types of devices using key)	Identity of KIF

**** Note:** Must include all keys from Table 6.1 identified as being distributed via KIF.*

P2PE Domain 6 Annex B Requirements and Testing Procedures	**P2PE Assessor Findings from Solution Provider Assessment**
KF-1 Account data must be encrypted in equipment that is resistant to physical and logical compromise. *(Reference 1A-1, 6D-2)*	
KF-1.1 Key-injection facilities must have processes in place to ensure: • Only keys specifically generated for use in a particular P2PE solution are injected into that P2PE solution's POI devices. • Keys generated for use in a particular P2PE solution are not injected into any devices other than those designated by the specific P2PE solution provider.	
KF-1.1.a Examine documented procedures to verify that procedures are defined to ensure: • Only keys specifically generated for use in a particular P2PE solution may be injected into that P2PE solution's POI devices. • Keys generated for use in a particular P2PE solution must not be injected into any devices other than those designed by the specific P2PE solution provider.	*<Report Findings Here>*
KF-1.1.b Interview responsible personnel and observe key-generation and loading processes to verify: • Only keys specifically generated for use in a particular P2PE solution may be injected into that P2PE solution's POI devices. • Keys generated for use in a particular P2PE solution must not be injected into any devices other than those designed by the specific P2PE solution provider.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex B Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
KF-1.2 Key-injection platforms and systems that include hardware devices for managing (for example, generating and storing) cryptographic keys must ensure those hardware devices conform to the requirements for SCDs. ***Note:*** *These devices must be managed in accordance with Domain 5 of this document.*	
KF-1.2.a Examine documented procedures and system documentation to verify that key-injection platforms and systems used for managing cryptographic keys are required to conform to the requirements for SCDs.	*<Report Findings Here>*
KF-1.2.b Examine key-injection platforms and systems used for managing cryptographic keys to verify they conform to the requirements for SCDs.	*<Report Findings Here>*
KF-2 Unencrypted secret or private keys must be entered into encryption devices using the principles of dual control and split knowledge. *(Reference 6D-1)*	
KF-2.1 Key-injection facilities must implement dual control and split-knowledge controls for the loading of keys into devices (for example, POIs and other SCDs). ***Note:*** *Such controls may include but are not limited to:* • *Physical dual-access controls that electronically provide for restricted entry and egress from a room dedicated to key injection such that the badge-access system enforces the presence of at least two authorized individuals at all times in the room so no one person can singly access the key-loading equipment. Access is restricted to only appropriate personnel involved in the key-loading process.* • *Logical dual control via multiple logins with unique user IDs to the key-injection platform application such that no one person can operate the application to singly inject cryptographic keys into devices.* • *Key-injection platform applications that force the entry of multiple key components and the implementation of procedures that involve multiple key custodians who store and access key components under dual-control and split-knowledge mechanisms.* • *Demonstrable procedures that prohibit key custodians from handing their components to any other individual for key entry.*	
KF-2.1.a Examine documented key-injection procedures to verify that the procedures define use of dual control and split knowledge controls for the loading of keys into devices.	*<Report Findings Here>*
KF-2.1.b Interview responsible personnel and observe key-loading processes and controls to verify that dual control and split-knowledge controls are in place for the loading of keys into devices.	*<Report Findings Here>*
KF-2.1.c Examine records of key-loading processes and controls to verify that the loading of keys does not occur without dual control and split knowledge.	*<Report Findings Here>*
KF-2.2 Controls must be in place to prevent and detect the loading of keys by any one single person. ***Note:*** *Controls include physical access to the room, logical access to the key-loading application, video surveillance of activities in the key-injection room, physical access to secret or private cryptographic key components or shares, etc*	
KF-2.2.a Examine documented key-injection procedures to verify that controls are defined to prevent and detect the loading of keys by any one single person.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex B Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
KF-2.2.b Interview responsible personnel and observe key-loading processes and controls to verify that controls are implemented to prevent and detect the loading of keys by any one single person.	*<Report Findings Here>*
KF-3 Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any encryption device without legitimate keys. *(Reference 6E-2)*	
KF-3.1 Key-injection facilities must implement controls to protect against unauthorized substitution of keys and to prevent the operation of devices without legitimate keys. Examples include but are not limited to: • All devices loaded with keys must be tracked at each key-loading session by serial number. • Key-injection facilities must use something unique about the POI (for example, serial number) when deriving the key (for example, DUKPT, TMK) injected into it.	
KF-3.1.a Examine documented procedures to verify they include: • Controls to protect against unauthorized substitution of keys, and • Controls to prevent the operation of devices without legitimate keys.	*<Report Findings Here>*
KF-3.1.b Interview responsible personnel and observe key-loading processes and controls to verify that: • Controls are implemented that protect against unauthorized substitution of keys, and • Controls are implemented that prevent the operation of devices without legitimate keys.	*<Report Findings Here>*
KF-4 All secret and private keys must be unique (except by chance) to that device. *(Reference 6E-4)*	
KF-4.1 Key-injection facilities must ensure that unique keys are loaded into each device. The same key(s) must not be loaded into multiple devices.	
KF-4.1.a Examine documented procedures to verify they include controls to ensure that unique keys are loaded into each device, and that keys are not loaded into multiple devices.	*<Report Findings Here>*
KF-4.1.b Interview responsible personnel and observe key-loading processes and controls to verify controls are implemented to ensure that only unique keys can be loaded into each device, and that keys cannot be loaded into multiple devices.	*<Report Findings Here>*
KF-4.2 Key-injection facilities that use DUKPT or other key-derivation methodologies on behalf of multiple acquirers must use different BDKs for each acquirer.	
KF-4.2.a Examine documented procedures for generation and use of BDKs to verify they require separate BDKs be used for different acquirers.	*<Report Findings Here>*
KF-4.2.b Observe key-loading processes for a sample of POIs to verify that separate BDKs are used for different acquirers.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex B Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
KF-4.2.1 Key-injection facilities that load DUKPT keys for various POI types for the same entity must use separate BDKs per terminal type if the terminal IDs can be duplicated among the multiple types of terminals. In other words, the key-injection facility must ensure that any one given key cannot be derived for multiple devices except by chance.	
KF-4.2.1.a If the key-injection facility loads DUKPT keys, examine documented procedures for generation and use of BDKs to verify they require use of separate BDKs per terminal type.	*<Report Findings Here>*
KF-4.2.1.b Observe key-loading processes for a sample of terminal types used by a single entity, to verify that separate BDKs are used for each terminal type	*<Report Findings Here>*
KF-4.3 Keys that are generated by a derivation process and derived from the same BDK must use unique data for the derivation process so that all POIs receive unique initial secret keys.	
KF-4.3.a Examine documented key-generation procedures to verify they require that keys derived from the same BDK must use unique data for the derivation process so that all POIs receive unique initial secret keys.	*<Report Findings Here>*
KF-4.3.b Observe key-loading processes to verify that keys which are derived from the same BDK use unique data for the derivation process so that all POIs receive unique initial secret keys.	*<Report Findings Here>*
KF-4.4 In a master/session key approach, the master key(s) and all session keys must be unique to each POI.	
KF-4.4.a Examine documented key-generation procedures to verify they require that, in a master/session key approach, the master key(s) and all session keys must be unique to each POI.	*<Report Findings Here>*
KF-4.4.b Observe key-loading processes to verify that in a master/session key approach, the master key(s) and all session keys must be unique to each POI.	*<Report Findings Here>*
KF-4.5 If injecting keys onto a single POI for more than one acquirer, the POI must have a completely different and unique key, or set of keys, for each acquirer. These different keys, or set of keys, must be totally independent and not variants of one another.	
KF-4.5.a Examine documented key-generation and injection procedures to verify that the following is required when injecting keys onto a single POI for more than one acquirer: • The POI must have a completely different and unique key, or set of keys, for each acquirer. • These different keys, or set of keys, must be totally independent and not variants of one another.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex B Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
KF-4.5.b Observe processes for generation and injection of keys onto a single POI for more than one acquirer, to verify: • The POI has a completely different and unique key, or set of keys, for each acquirer. • These different keys, or set of keys, are totally independent and not variants of one another.	*<Report Findings Here>*
KF-5 Key-injection facilities must ensure protection against unauthorized use for SCDs (e.g., HSMs) used in the key-injection platform that are capable of encrypting a key and producing cryptograms of that key.	
KF-5.1 The KIF must implement a physically secure area (secure room) for key injection. The secure room for key injection must include the following.	
KF-5.1 Observe the physical facility to verify that a secure room is designated for key injection and that all SCDs and other devices used in the key-injection platform are physically located in this room.	*<Report Findings Here>*
KF-5.1.1 The secure area must have extended walls from the real floor to the real ceiling using sheetrock or wire mesh.	
KF-5.1.1 Inspect the secure area designated for key injection to verify that it is constructed with extended walls from the real floor to the real ceiling using sheetrock or wire mesh.	*<Report Findings Here>*
KF-5.1.2 Any windows into the secure room must be locked and protected by alarmed sensors.	
KF-5.1.2.a Observe all windows in the secure room to verify they are locked and protected by alarmed sensors.	*<Report Findings Here>*
KF-5.1.2.b Examine configuration of window sensors to verify that the alarm mechanism is active.	*<Report Findings Here>*
KF-5.1.3 Any windows must be covered, rendered opaque, or positioned to prevent unauthorized observation of the secure area.	
KF-5.1.3 Observe all windows in the secure room to verify they are covered, rendered opaque, or positioned to prevent unauthorized observation of the secure room.	*<Report Findings Here>*
KF-5.1.4 A solid-core door or a steel door must be installed to ensure that door hinges cannot be removed from outside the room.	
KF-5.1.4 Inspect the secure area to verify that it is only accessed through a solid-core or a steel door, with door hinges that cannot be removed from outside the room.	*<Report Findings Here>*
KF-5.1.5 A badge-control system must be in place that enforces: Dual-access requirements for entry into the secure area, and Anti-pass-back requirements.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex B Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
KF-5.1.5 Observe authorized personnel entering the secure area to verify that a badge-control system is in place that enforces the following requirements: Dual-access for entry to the secure area Anti-pass-back	*<Report Findings Here>*
KF-5.1.6 The badge-control system must support generation of an alarm when one person remains alone in the secure area for more than 30 seconds. ***Note:*** *Examples of alarm-generation mechanisms include but are not limited to motion detectors, login/logout controls, biometrics, badge sensors, etc.*	
KF-5.1.6 Examine alarm mechanisms and interview alarm-response personnel to verify that the badge-control system supports generation of an alarm when one person remains alone in the secure area for more than 30 seconds.	*<Report Findings Here>*
KF-5.1.7 A CCTV system must be in place that monitors on a continuous (24/7) basis.	
KF-5.1.7 Inspect CCTV configuration and review a sample of recordings to verify that CCTV monitoring is in place on a24/7 basis.	*<Report Findings Here>*
KF-5.1.8 Monitoring must be supported on a continuous (24/7) basis such that alarms can be resolved by authorized personnel.	
KF-5.1.8 Inspect configuration of monitoring systems and interview monitoring personnel to verify that monitoring is supported on a continuous (24/7) basis and alarms can be resolved by authorized personnel.	*<Report Findings Here>*
KF-5.1.9 The CCTV server and digital storage must be secured in a separate secure area that is not accessible to personnel that have access to the key-injection area.	
KF-5.1.9.a Inspect location of the CCTV server and digital-storage area to verify that the CCTV server and digital storage are located in a secure area that is separate to the key-injection area.	*<Report Findings Here>*
KF-5.1.9.b Inspect access-control configurations for the CCTV server/storage area and the key-injection area to identify all personnel that have access to each area. Compare access lists to verify that personnel with access to the key-injection area do not have access to the CCTV server/storage area.	*<Report Findings Here>*
KF-5.1.10 The CCTV cameras must be positioned to monitor: The entrance door, SCDs, both pre and post key injection, Any safes that are present, and The equipment used for key injection.	

Copyright 2012 PCI Security Standards Council LLC

P2PE Domain 6 Annex B Requirements and Testing Procedures	P2PE Assessor Findings from Solution Provider Assessment
KF-5.1.10 Inspect CCTV positioning and review a sample of recordings to verify that CCTV cameras are positioned to monitor: The entrance door, SCDs, both pre and post key injection, Any safes that are present, and The equipment used for key injection.	*<Report Findings Here>*
KF-5.1.11 CCTV cameras must be positioned so they do not monitor any combination locks, PIN pads, or keyboards used to enter passwords or other authentication credentials.	
KF-5.1.11 Inspect CCTV positioning and review a sample of recordings to verify that CCTV cameras do not monitor any combination locks, PIN pads, or keyboards used to enter passwords or other authentication credentials.	*<Report Findings Here>*

Copyright 2012 PCI Security Standards Council LLC