Security
Standards Council®

Payment Card Industry (PCI)
Token Service Providers

Report on Compliance –Token Service Providers

Reporting Template for use with the Additional Security Requirements and Assessment Procedures for Token Service Providers (EMVCo Payment Tokens)

Version 1.0

February 2016

Document Changes

Date	Version	Description
February 2016	1.0	To introduce the template for submitting Supplemental Reports on Compliance for Tokenisation Service Providers *This document is intended for use with the Additional Requirements and Assessment Procedures for TSPs, v1.0*

Table of Contents

Introduction to the ROC Template for Payment Card Industry (PCI) Token Service Providers

Instructions for Submission

This document, the *Reporting Template for use with the PCI Additional Requirements and Assessment Procedures for Token Service Providers, Revision 1.0* ("TSP ROC Template" or "T-ROC"), is the mandatory template for P2PE Qualified Security Assessors (QSAs) completing assessment of a Token Service Provider (as defined by EMVCo) against the *PCI Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens), Version 1.0.*

Note that an entity is *ONLY* required to undergo an assessment according to this document if instructed to do so by an acquirer or a payment brand.

This "TSP ROC Template" or "T-ROC" document is to be completed according to the same instructions provided in the Reporting Template for PCI DSS v3. Refer to the *Reporting Template(s) for use with PCI DSS v3* and the *ROC Reporting Template for PCI DSS v3: Frequently Asked Questions (FAQs)* documents on the PCI SSC website for detailed instruction on how to complete these reporting templates. As such, do not delete any content from any place in this document, including this section and the versioning above. Excessive personalization and changes to sections – including additional sections - may not be accepted by accepting entities, and personalization should be limited to the title page.

The "T-ROC" template is additional to the ROC Reporting Template, and completion of this T-ROC assumes a ROC Reporting Template for PCI DSS has already been completed. Because of this, details related to Scope of Work, Details of Reviewed Environment and so on that are applicable to the environment reviewed for the T-ROC must be included in the applicable sections in the full ROC for that entity. If the PCI DSS ROC does not include all details relevant to the TSP Assessment, those additional details must be addressed in a partial ROC or within the T-ROC.

Token Service Providers should contact their payment brand and/or acquirer with any questions about completing and submitting these reports.

Scope of Requirements

The requirements in this document are intended to apply in addition to applicable PCI DSS requirements to the token data environment (TDE). The TDE is a dedicated, secure area within the TSP, where one or more of the following services are performed:

- Token generation, issuing, and mapping processes
- Assignment of token usage parameters
- Token lifecycle management
- Processes to map or re-map tokens, or perform de-tokenization
- Cryptographic processes to support tokenization functions
- Maintenance of underlying token security and related processing controls, such as domain restrictions during transaction processing.

These services are critical to the integrity of the Payment Token ecosystem, and the requirements in this document are intended to apply wherever the above services are performed. Examples of TDE system components that perform these functions include, but are not limited to:

- Token Vault
- APIs that support external interactions/interfaces
- HSMs performing key-management functions for the Token Vault and other tokenization services
- Systems used to process token-related functions and data, such as token mapping data, token metadata, token domain restriction data, Identification and Verification (ID&V) data, and so on.

> ***Note:*** *For a full description of the Token Vault, Payment Tokens, and other terminology, refer to the EMV® Payment Tokenisation Specification Technical Framework (www.emvco.com).*

As the TDE contains payment card data, it is also a cardholder data environment (CDE) and subject to the security requirements within PCI DSS as well as the additional security requirements defined within this document.

Conceptual illustrations showing two examples of how the TDE is typically integrated into the CDE are provided on the following pages.

Examples of TDE/CDE integration within TSP

Figure 1: TDE as a Subnetwork of CDE

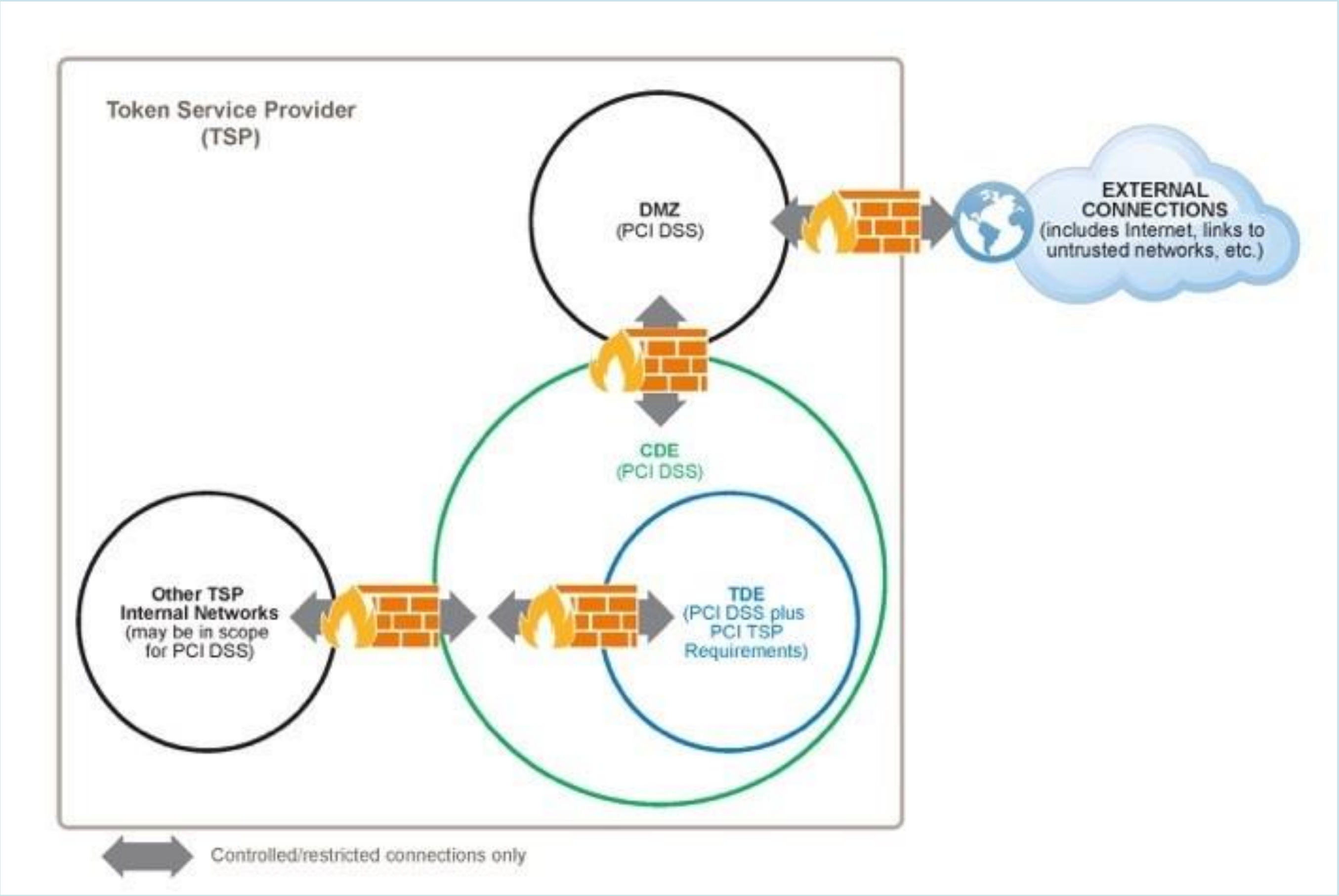
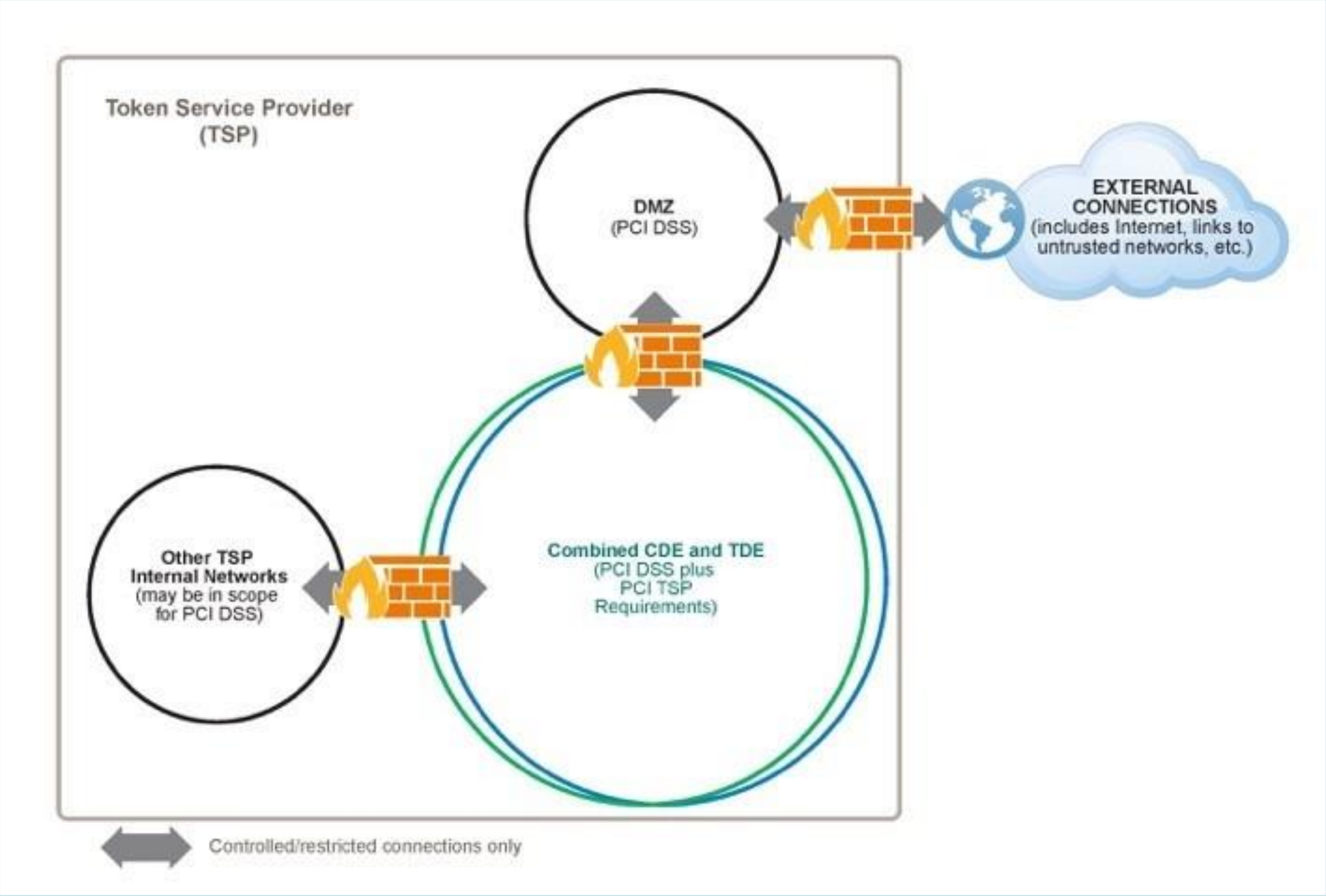

Token Service Provider (TSP)
DMZ (PCI DSS)
EXTERNAL CONNECTIONS (includes Internet, links to untrusted networks, etc.)
CDE (PCI DSS)
Other TSP Internal Networks (may be in scope for PCI DSS)
TDE (PCI DSS plus PCI TSP Requirements)
Controlled/restricted connections only

Figure 2: Combined CDE and TDE


Token Service Provider (TSP)
DMZ (PCI DSS)
EXTERNAL CONNECTIONS (includes Internet, links to untrusted networks, etc.)
Other TSP Internal Networks (may be in scope for PCI DSS)
Combined CDE and TDE (PCI DSS plus PCI TSP Requirements)
Controlled/restricted connections only

Note: *These diagrams are provided for illustrative purposes only, and do not supersede any PCI DSS requirement. The locations of firewalls in the diagrams are not all-inclusive, and represent the minimum locations where firewall controls exist.*

Where the CDE and TDE are combined, all CDE components in the TDE must also meet these TSP Requirements.

In addition to providing services related to payment card data and Payment Tokens, TSPs often perform other functions or services that include the presence of Payment Tokens. The requirements in this document only apply to the TDE (as defined and illustrated above), and do not apply to other environments where Payment Tokens exist.

Applicability of PCI DSS Requirements 1-12 to TSPs

As the TDE contains payment card data, it must be PCI DSS compliant. When applying PCI DSS to the TDE, the provisions set forth in this document also apply. The applicability of PCI DSS to TSPs extends beyond that described in the "PCI DSS Applicability Information" and "Scope of PCI DSS Requirements" sections within the PCI DSS to also encompass the TDE.

Regarding applicability of PCI DSS to Payment Tokens:

- Within the TDE, Payment Tokens must be secured in the same way as a PAN
- Outside the TDE, Payment Tokens do not require protection and are not in scope for PCI DSS

When applying PCI DSS Requirements 1-12 to the TDE, the following principles also apply:

- Where a PCI DSS requirement specifically mentions the CDE, the requirement also applies to the TDE.
- Where a PCI DSS requirement specifically mentions PAN or cardholder data (CHD), the requirement also applies to Payment Tokens or Payment Token Data, respectively, within the TDE.

A summary of additional considerations for PCI DSS Requirements 1-12 that affect TSPs is provided below.

PCI DSS Requirement	Additional Applicability for TSPs
1. Install and maintain a firewall configuration to protect cardholder data	▪ Firewall controls in PCI DSS Requirement 1 also apply to internal firewalls used to separate TDE from non-TDE networks. ▪ The current network and data flow diagrams (PCI DSS Requirements 11.2 and 1.1.3) must also include all connections between the TDE and other networks, and all flows of Payment Tokens across systems and networks in the TDE.
2. Do not use vendor-supplied defaults for system passwords and other security parameters	▪ PCI DSS Requirement 2 applies to all system components in the TDE. ▪ Wireless environments are not permitted to be connected to the TDE.
3. Protect stored cardholder data	▪ Data retention and disposal policies, procedures and processes (PCI DSS Requirement 3.1) also apply to Payment Token Data. ▪ Payment Tokens must also be masked when displayed such that only personnel with a legitimate business need can see the full Payment Token (PCI DSS Requirement 3.3), and rendered unreadable wherever they are stored (PCI DSS Requirement 3.4) in the TDE. ▪ The key-management requirements in this document are in addition to those in PCI DSS Requirements 3.5 – 3.6

PCI DSS Requirement	Additional Applicability for TSPs
4. Encrypt transmission of cardholder data across open, public networks	▪ Wireless environments are not permitted to be connected to the TDE.
5. Protect all systems against malware and regularly update anti-virus software or programs	▪ PCI DSS Requirement 5 applies to all system components in the TDE.
6. Develop and maintain secure systems and applications	▪ PCI DSS Requirement 6 applies to all system components in the TDE. ▪ All changes made to system components in the TDE must be in accordance with PCI DSS Requirement 6.4.5.
7. Restrict access to cardholder data by business need to know	▪ Access to Payment Token Data in the TDE must also be restricted according to principles of need-to-know and least privilege.
8. Identify and authenticate access to system components	▪ Strong authentication controls are required for all accounts used to access Payment Tokens or to access systems in the TDE.
9. Restrict physical access to cardholder data	▪ Physical security controls also apply to secure access to Payment Token Data in the TDE.
10. Track and monitor all access to network resources and cardholder data	▪ Audit log requirements include all individual user access to Payment Token Data in the TDE (PCI DSS Requirement 10.2.1).
11. Regularly test security systems and processes	▪ Internal vulnerability scans, penetration tests (for example, to verify segmentation controls), intrusion detection, and change detection apply to the TDE.
12. Maintain a policy that addresses information security for all personnel	▪ PCI DSS Requirement 12 also applies to personnel with access to the TDE.

T-ROC Template for Token Service Providers

This template is to be used for creating a TSP Report on Compliance. Content and format for a T-ROC is defined as follows:

1. Contact Information and Report Date

1.1 Contact information

Client	
▪ Company name:	
▪ Company address:	
▪ Company URL:	
▪ Company contact name:	
▪ Contact phone number:	
▪ Contact e-mail address:	
Assessor Company	
▪ Company name:	
▪ Company address:	
▪ Company website:	
Assessor	
▪ Assessor name:	
▪ Assessor PCI credentials: (QSA, PA-QSA, etc.)	
▪ Assessor phone number:	
▪ Assessor e-mail address:	
Assessor Quality Assurance (QA) Primary Reviewer for this specific report (not the general QA contact for the QSA)	
▪ QA reviewer name:	
▪ QA reviewer phone number:	
▪ QA reviewer e-mail address:	

1.2 Date and timeframe of assessment

▪ Date of Report:	
▪ Timeframe of assessment (start date to completion date):	
▪ Identify date(s) spent onsite at the entity:	
▪ Descriptions of time spent onsite at the entity and time spent performing remote assessment activities, including time spent on validation of remediation activities.	

1.3 Additional services provided by QSA company

The PCI DSS Validation Requirements for QSAs v2.0, Section 2.2 “Independence” specifies requirements for QSAs around disclosure of such services and/or offerings that could reasonably be viewed to affect independence of assessment. Complete the below after review of this portion of the Validation Requirements, to ensure responses are consistent with documented obligations.

▪ Disclose all services offered to the assessed entity by the QSAC, including but not limited to whether the assessed entity uses any security-related devices or security-related applications that have been developed or manufactured by the QSA, or to which the QSA owns the rights or that the QSA has configured or manages:	
▪ Describe efforts made to ensure no conflict of interest resulted from the above mentioned services provided by the QSAC:	

2. Summary Overview

2.1 Description of the entity's token services business

Provide an overview of the entity's token services business:

▪ Describe the nature of the entity's business (what kind of work they do, etc.) ***Note:*** *This is not intended to be a cut-and-paste from the entity's website, but should be a tailored description that shows the assessor understands the business of the entity being assessed.*	

2.2 High-level network diagram(s)

Provide a ***high-level*** network diagram (either obtained from the entity or created by assessor) of the entity's networking topography, showing the overall architecture of the environment being assessed. This high-level diagram should summarize all locations and key systems, and the boundaries between them and should include the following:

- Connections into and out of the network including demarcation points between the token data environment (TDE) and other networks/zones
- Critical components within the token data environment, including (but not limited to)
  - Token vault
  - APIs that support external interactions/interfaces
  - HSMs performing key-management functions for the Token Vault and other tokenization services
  - Systems used to process token-related functions and data, such as token mapping data, token metadata, token domain restriction data, Identification and Verification (ID&V) data, and so on.
- Other necessary payment components, as applicable

<Insert high-level network diagram(s)>

2.3 Applicability of PCI DSS Requirements 1-12 to TSPs

Confirm whether the additional considerations for PCI DSS Requirements 1-12 that affect TSPs below were included in the PCI DSS Assessment or assessed separately. Include the date of the assessment.

Note: If the TSP assessor was unable to confirm that the TDE was assessed fully, a partial ROC must be completed to address those TDE portions deemed necessary.

Indicate whether each item below was assessed and verified as being met during this TSP engagement or in a separate PCI DSS engagement.		
	Assessed and verified as being met during this TSP engagement	**Assessed and verified as being met in a separate PCI DSS engagement as documented on** *<Date>*
1. Install and maintain a firewall configuration to protect cardholder data		
▪ Firewall controls in PCI DSS Requirement 1 were assessed and verified for internal firewalls used to separate TDE from non-TDE networks.	□	□
▪ The current network and data flow diagrams (PCI DSS Requirements 11.2 and 1.1.3) were assessed and verified to include all connections between the TDE and other networks, and all flows of Payment Tokens across systems and networks in the TDE.	□	□
2. Do not use vendor-supplied defaults for system passwords and other security parameters		
▪ PCI DSS Requirement 2 was assessed and verified for all system components in the TDE.	□	□
3. Protect stored cardholder data		
▪ Data retention and disposal policies, procedures and processes (PCI DSS Requirement 3.1) were assessed and verified to include Payment Token Data.	□	□
▪ Payment Tokens were assessed and verified to be masked when displayed such that only personnel with a legitimate business need can see the full Payment Token (PCI DSS Requirement 3.3), and rendered unreadable wherever they are stored (PCI DSS Requirement 3.4) in the TDE.	□	□
▪ Key-management requirements in this document were assessed and verified in addition to those in PCI DSS Requirements 3.5 – 3.6	□	□
4. Encrypt transmission of cardholder data across open, public networks		

▪ The TDE was verified as not having any wireless environments connected	□	□
5. Protect all systems against malware and regularly update anti-virus software or programs		
▪ PCI DSS Requirement 5 was assessed and verified for all system components in the TDE.	□	□
6. Develop and maintain secure systems and applications		
▪ PCI DSS Requirement 6 was assessed and verified for all system components in the TDE.	□	□
▪ Changes made to system components in the TDE were assessed and verified to be in accordance with PCI DSS Requirement 6.4.5.	□	□
7. Restrict access to cardholder data by business need to know		
▪ Access to Payment Token Data in the TDE was assessed and verified to be restricted according to principles of need-to-know and least privilege.	□	□
8. Identify and authenticate access to system components		
▪ All accounts used to access Payment Tokens or to access systems in the TDE were assessed and verified to require strong authentication controls.	□	□
9. Restrict physical access to cardholder data		
▪ Physical security controls were assessed and verified to secure access to Payment Token Data in the TDE.	□	□
10. Track and monitor all access to network resources and cardholder data		
▪ Audit log requirements were assessed and verified to include all individual user access to Payment Token Data in the TDE (PCI DSS Requirement 10.2.1).	□	□
11. Regularly test security systems and processes		
▪ Internal vulnerability scans, penetration tests (for example, to verify segmentation controls), intrusion detection, and change detection were assessed and verified for the TDE.	□	□
12. Maintain a policy that addresses information security for all personnel		
▪ PCI DSS Requirement 12 was assessed and verified for personnel with access to the TDE.	□	□

2.4 Network segmentation

▪ Identify whether the TDE is combined with the CDE **(yes/no)** *If "yes," mark the remainder of this section as "Not Applicable"*	
▪ Identify whether the TDE is a subnetwork of the CDE **(yes/no)** *If "no," complete the following:*	
▪ Briefly describe how the segmentation is implemented.	
• Identify the technologies used and any supporting processes	
• Explain how the assessor validated the effectiveness of the segmentation, as follows:	
(a) Describe the methods used to validate the effectiveness of the segmentation (for example, observed configurations of implemented technologies, tools used, network traffic analysis, etc.).	
(b) Describe how it was verified that the segmentation is functioning as intended.	
(c) Describe how it was verified that adequate security controls are in place to ensure the integrity of the segmentation mechanisms (e.g., access controls, change management, logging, monitoring, etc.).	
▪ Provide the name of the assessor who attests that the segmentation was verified to be adequate to reduce the scope of the assessment AND that the technologies/processes used to implement segmentation were included in the PCI DSS assessment.	

2.5 Sample sets for reporting

***Note:** When a reporting instruction asks for a sample, the assessor may either refer to the Sample Set Identifier here (for example "Sample Set-1") OR list the sampled items individually in the response. Examples of sample sets may include, but are not limited to, firewalls, application servers, retail locations, data centers, User IDs, people, etc. Add rows as needed.*

Sample Set Reference Number	**Sample Type/ Description** (e.g., firewalls, datacenters, etc.)	**Listing of all components (devices, locations, etc.) of the Sample Set** (with make/model, as applicable)	**Total Sampled**	**Total Population**
Sample Set-1				

Sample Set Reference Number	**Sample Type/ Description** (e.g., firewalls, datacenters, etc.)	**Listing of all components (devices, locations, etc.) of the Sample Set** (with make/model, as applicable)	**Total Sampled**	**Total Population**
Sample Set-2				
Sample Set-3				
Sample Set-4				

2.6 Documentation reviewed

Identify and list all reviewed documents. Include the following:

Reference Number	**Document Name** (including version, if applicable)	**Brief description of document purpose**	**Document date** (latest version date)
Doc-1			
Doc-2			
Doc-3			
Doc-4			
Doc-5			

2.7 *Individuals interviewed*

Identify and list the individuals interviewed. Include the following:

Reference Number	Employee Name	Role/Job Title	Organization	Is this person an ISA? (yes/no)	Summary of Topics Covered / Areas or Systems of Expertise (high-level summary only)
Int-1					
Int-2					
Int-3					
Int-4					

2.8 *Disclosure summary for "Not Tested" responses*

▪ Identify whether there were any responses indicated as "Not Tested": **(yes/no)**	
▪ *If "yes," complete the table below:*	

List of all requirements/testing procedures with this result	**Summary of the issue** (for example, not deemed in scope for the assessment)

3. Findings and Observations

TSP 1. Document and validate PCI DSS scope

TSP 1. Document and validate PCI DSS scope					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 1.1 Document and validate scope for PCI DSS and TSP Requirements					
TSP 1.1.1 Document and confirm the accuracy of scope for PCI DSS and these TSP Requirements at least quarterly and upon significant changes to the in-scope environment. At a minimum, the quarterly scoping validation must include: • Identifying all in-scope networks and system components • Identifying all out-of-scope networks and justification for networks being out of scope, including descriptions of all segmentation controls implemented • Identifying all connected entities—e.g., third-party entities with access to the TDE and/or CDE		□	□	□	□
TSP 1.1.1.a Examine documented results of scope reviews and interview personnel to verify that the reviews are performed: • At least quarterly • After significant changes to the in-scope environment	**Identify the documented results of scope reviews** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 1.1.1.b Examine documented results of quarterly scope reviews to verify the following is performed: • Identification of all in-scope networks and system components • Identification of all out-of-scope networks and justification for networks being out of scope, including descriptions of all segmentation controls implemented • Identification of all connected entities—e.g., third-party entities with access to the TDE and/or CDE	**Identify the quarterly scope review document(s)** examined for this testing procedure.	*<Report Findings Here>*			

<table>
<tr><th colspan="6"><b><i>TSP 1. Document and validate PCI DSS scope</i></b></th></tr>
<tr><th rowspan="2">Requirements and Testing Procedures</th><th rowspan="2">Reporting Instructions & Assessor’s Findings</th><th colspan="4">Summary of Assessment Findings
(check one)</th></tr>
<tr><th>In Place</th><th>In Place w/ CCW</th><th>N/A</th><th>Not in Place</th></tr>
<tr><td colspan="2"><b>TSP 1.1.2</b> Determine scope impact for PCI DSS and TSP Requirements, for all changes to systems or networks, including additions of new systems and new network connections. Processes must include:
• Performing a formal impact assessment for PCI DSS and these TSP Requirements
• Identifying applicable requirements for the affected system or network
• Updating scope for PCI DSS and these TSP Requirements as appropriate
• Documented sign-off of the results of the impact assessment by responsible personnel (as defined in TSP 8.2.3).</td><td>□</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td rowspan="2"><b>TSP 1.1.2</b> Examine change documentation and interview personnel to verify that for each change to systems or networks:
• A formal impact assessment for PCI DSS and these TSP Requirements was performed.
• All requirements applicable to the system or network changes were identified.
• Scope for PCI DSS and these TSP Requirements was updated as appropriate for the change.
• Sign-off by responsible personnel (as defined in TSP 8.2.3) was obtained and documented.</td><td><b>Identify the change documentation</b> examined for this testing procedure.</td><td colspan="4"><i>&lt;Report Findings Here&gt;</i></td></tr>
<tr><td><b>Identify the responsible personnel</b> interviewed for this testing procedure.</td><td colspan="4"><i>&lt;Report Findings Here&gt;</i></td></tr>
<tr><td colspan="2"><b>TSP 1.1.2.1</b> Upon completion of a change, all relevant PCI DSS and TSP Requirements must be verified on all new or changed systems and networks, and documentation must be updated as applicable. Examples of requirements that must be verified include, but are not limited to:
• Network diagram is updated to reflect changes.
• Systems are configured per configuration standards, with all default passwords changed and unnecessary services disabled.
• Systems are protected with required controls—e.g., file-integrity monitoring (FIM), anti-virus, patches, audit logging.
• Verify that sensitive authentication data (SAD) is not stored and that all cardholder data (CHD) and Payment Token storage is documented and incorporated into data-retention policy and procedures.
• New systems are included in the quarterly vulnerability scanning process.</td><td>□</td><td>□</td><td>□</td><td>□</td></tr>
</table>

TSP 1. Document and validate PCI DSS scope

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 1.1.2.1 For a sample of systems and network changes, examine change records, interview personnel and observe the affected systems/networks to verify that applicable PCI DSS and TSP Requirements were implemented and documentation updated as part of the change.	**Identify the sample of system components** selected for this testing procedure.	*<Report Findings Here>*			
	Identify the sample of network changes examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how the applicable PCI DSS and TSP requirements were implemented for the affected systems/networks.				
	<Report Findings Here>				
	Describe how the documentation was updated as part of the change.				
	<Report Findings Here>				
TSP 1.1.3 Changes to organizational structure—for example, a company merger or acquisition, change or reassignment of personnel with responsibility for security controls—result in a formal (internal) review of the impact to scope for PCI DSS and these TSP Requirements and applicability of controls.		□	□	□	□
TSP 1.1.3 Examine policies and procedures to verify that a change to organizational structure results in formal review of the impact to scope for PCI DSS and these TSP Requirements and applicability of controls.	**Identify the policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 1.1.4 If segmentation is used, confirm scope for PCI DSS and these TSP Requirements by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.		□	□	□	□

TSP 1. Document and validate PCI DSS scope

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 1.1.4 Examine the results from the most recent penetration test to verify that: • Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE/TDE.	**Identify the documented penetration test results** examined for this testing procedure.	*<Report Findings Here>*			
TSP 1.1.5 Implement mechanisms for detecting and preventing clear-text PAN and/or Payment Tokens from leaving the CDE/TDE ***via an unauthorized*** channel, method, or process, including generation of audit logs and alerts.		□	□	□	□
TSP 1.1.5.a Examine documentation and observe implemented mechanisms to verify that the mechanisms are: • Implemented and actively running • Configured to detect and prevent clear-text PAN leaving the CDE via an unauthorized channel, method, or process • Configured to generate logs and alerts upon detection of clear-text PAN and/or Payment Tokens leaving the CDE/TDE via an unauthorized channel, method, or process • Tested at least annually to confirm the mechanism is working as intended	**Identify the documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the implemented mechanisms examined for this testing procedure.	*<Report Findings Here>*			
	Provide the name of the assessor who attests that the mechanisms are: • Implemented and actively running • Configured to detect and prevent clear-text PAN leaving the CDE via an unauthorized channel, method, or process • Configured to generate logs and alerts upon detection of clear-text PAN and/or Payment Tokens leaving the CDE/TDE via an unauthorized channel, method, or process • Tested at least annually to confirm the mechanism is working as intended	*<Report Findings Here>*			

TSP 1. Document and validate PCI DSS scope

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 1.1.5.b Examine audit logs and alerts, and interview responsible personnel to verify that alerts are investigated	**Identify the audit logs** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the alerts examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 1.1.5.1 Implement response procedures to be initiated upon the detection of attempts to remove clear-text PAN and/or Payment Tokens from the CDE/TDE via an unauthorized channel, method, or process. Response procedures must include: • Procedures for the timely investigation of alerts by responsible personnel • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss		□	□	□	□
TSP 1.1.5.1.a Examine documented response procedures to verify that procedures for responding to the attempted removal of clear-text PAN and/or Payment Tokens from the CDE/TDE via an unauthorized channel, method, or process include: • Procedures for the timely investigation of alerts by responsible personnel • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss	**Identify the documented response procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 1.1.5.1.b Interview personnel and examine records of actions taken when clear-text PAN and/or Payment Tokens is detected leaving the CDE/TDE via an unauthorized channel, method, or process, and verify that remediation activities were performed.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the records of action taken examined for this testing procedure.	*<Report Findings Here>*			
	Describe the remediation activities performed when clear-text PAN and/or Payment Tokens is detected leaving the CDE/TDE via an unauthorized channel, method, or process.				
	<Report Findings Here>				

TSP 2. Secure TDE Systems and Network

The requirements in this section build on PCI DSS Requirements 1 and 2. When applying PCI DSS Requirements 1 and 2 to the TDE, the following principles apply:

- Firewall controls in PCI DSS Requirement 1 also apply to internal firewalls used to separate TDE from non-TDE networks.
- Where PCI DSS Requirement 1 specifically mentions the CDE, the requirement also applies to the TDE.
- Where PCI DSS Requirement 1 specifically mentions PAN or CHD, the requirement also applies to Payment Tokens within the TDE. For example, TSPs must maintain a current data flow diagram (PCI DSS requirement 1.1.3) that shows all flows of CHD and all flows of Payment Tokens across systems and networks.
- PCI DSS Requirement 2 applies to all system components in the TDE.
- Wireless environments are not permitted to be connected to the TDE.

TSP 2. Secure TDE Systems and Network					
		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 2.1 Dedicated Systems					
TSP 2.1.1 System components in the TDE must be dedicated to performing and/or supporting tokenization services. ***Note:*** *Where there is a legitimate, documented business or technical justification, it is permissible for system components in the TDE to also perform other functions.*		□	□	□	□
TSP 2.1.1 Examine system documentation and system configurations to identify the functions performed. Verify all systems in the TDE are dedicated to performing and/or supporting tokenization services, or have a documented business/technical justification for performing non-tokenization services.	**Identify the system documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify all systems in the TDE examined for this testing procedure.	*<Report Findings Here>*			
	For each system in the TDE performing ***non-tokenization services***, **identify** the documented business/technical justification.	*<Report Findings Here>*			
	For each system in the TDE performing ***tokenization services***, **describe** the functions performed.				

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
	<Report Findings Here>				
TSP 2.2 Network Infrastructure					
TSP 2.2.1 The TDE must be on a dedicated network(s) that is separated by a firewall(s) from all non-TDE networks and any Internet-connected networks. ***Notes:*** - *A virtual LAN (VLAN) is not considered a separate network segment.* - *Where there is a legitimate, documented business or technical justification, it is permissible for non-TDE systems to be included within the same network as the TDE. All systems within the TDE are subject to the requirements in this document.*		□	□	□	□
TSP 2.2.1.a Examine systems in the TDE to verify they are required for tokenization services, or have a documented business or technical justification for being in the TDE.	**Identify the system in the TDE** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** each system in the TDE is required for tokenization services, or have a documented business or technical justification for being in the TDE.				
	<Report Findings Here>				
TSP 2.2.1.b Observe network configurations to verify a firewall(s) is in place between the TDE and all other networks, including any Internet-connected networks.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** network configurations confirm that a firewall(s) is in place between the TDE and all other networks, including any Internet-connected networks.				
	<Report Findings Here>				
TSP 2.2.1.c Review network and firewall configurations to verify that all connections between the TDE and other networks are controlled and occur only via approved interfaces.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how network and firewall configurations confirm that all connections between the TDE and other networks are controlled and occur only via approved interfaces.				
	<Report Findings Here>				

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 2.2.2 All APIs that can be accessed from outside the TDE must be identified, defined, and tested to verify it performs as expected.		□	□	□	□
TSP 2.2.2.a Examine network and data-flow diagrams and system configurations to verify that all exposed APIs are documented, and only approved interfaces are used.	**Identify the network and data-flow diagram(s)** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how system configurations and relevant documentation verify that all exposed APIs are documented and only approved interfaces are used.				
	<Report Findings Here>				
TSP 2.2.2.b Review TSP documentation for API testing. Interview TSP personnel that perform API testing to verify that testing is performed in accordance with the TSP's documented testing procedures.	**Identify the TSP documentation for API testing** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.2.3 Virtual systems must not span different network domains.		□	□	□	□
TSP 2.2.3 If virtualization technologies are utilized in the TDE, review system configurations to verify systems are not a member of multiple domains.	**Indicate whether** virtualization technologies are utilized in the TDE. **(yes/no)** *If "no," mark 2.2.3 as "Not Applicable."* *If "yes":*	*<Report Findings Here>*			
	Identify the system component(s) examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** system configurations ensure that virtual systems are not a member of multiple domains.				
	<Report Findings Here>				
TSP 2.3 Network Devices					
TSP 2.3.1 Change control processes must include back-ups of network devices prior to any change to the device. Back-up media must be securely stored and managed.		□	□	□	□

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 2.3.1.a Review change control documentation to verify there is a process for backing up network devices prior to any changes of those devices.	**Identify the change control documentation** reviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how the change control documentation shows that there is a process for backing up network devices prior to any changes of those devices.				
	<Report Findings Here>				
TSP 2.3.1.b Review procedures for back-ups and managing back-up media to verify media is securely stored and managed.	**Identify the procedure(s) reviewed for this testing procedure.**	*<Report Findings Here>*			
	Describe how back-up media is securely stored and managed:				
	<Report Findings Here>				
TSP 2.4 Firewalls ***Note:*** *These requirements apply to firewalls protecting the TDE.*					
TSP 2.4.1 All documents relating to firewall configurations must be stored securely.		□	□	□	□
TSP 2.4.1 Observe storage of firewall configuration documents to verify documents are stored securely: • Hard copy and non-digital documentation are stored in locked/secured areas with access only to authorized personnel. • Digital records are stored in a secure directory with access limited to authorized personnel.	**Provide the name of the assessor** who attests that firewall configuration documents are stored securely.	*<Report Findings Here>*			
TSP 2.4.2 For any TDE system that does not need to connect to systems outside of the TDE, firewall rule sets must be configured to prevent all connections to/from that system and any system outside the TDE.		□	□	□	□
TSP 2.4.2 For all TDE systems that do not need to connect to systems outside of the TDE, examine firewall and router configurations, including ingress and egress rules for all interfaces,	**Identify all TDE systems** that do not need to connect to systems outside of the TDE.	*<Report Findings Here>*			

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
and verify that no connections are permitted between that system and any system outside the TDE.	*For each TDE system identified,* **describe how** the firewall and router configurations, including ingress and egress rules for all interfaces, ensure that no connections are permitted between that system and any system outside the TDE.				
	<Report Findings Here>				
TSP 2.4.3 Firewalls must be run on dedicated hardware. All non-firewall-related software, such as compilers, editors, and communication software, must be deleted or disabled.		□	□	□	□
TSP 2.4.3.a Examine firewall configurations to verify that devices performing firewall functions are not performing any other function.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how firewall configurations confirm that devices performing firewall functions are not performing any other function.				
	<Report Findings Here>				
TSP 2.4.3.b Examine firewall documentation and configurations to verify that all software not required for firewall functionality is deleted or disabled.	**Identify the firewall documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the system component(s) examined for this testing procedure.	*<Report Findings Here>*			
	Describe how firewall configurations confirm that all software not required for firewall functionality is deleted or disabled.				
	<Report Findings Here>				
TSP 2.4.4 Source routing must be disabled on firewalls.		□	□	□	□
TSP 2.4.4 Examine firewall configurations to verify that source routing is disabled.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how source routing is disabled in the firewall configurations.				

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
	<Report Findings Here>				
TSP 2.5 Remote and Non-Console Access					
TSP 2.5.1 The remote access process must be fully documented and include at least the following components: • System components for which remote access is permitted • The location(s) from which remote access is permitted • The conditions under which remote access is acceptable • Users with remote access permission • The access privileges applicable to each authorized user		□	□	□	□
TSP 2.5.1 Examine policies and procedures to verify the remote access process is fully documented and identifies the following: • System components for which remote access is permitted • The location from which remote access is permitted • The conditions under which remote access is acceptable • Users with remote access permission • The access privileges applicable to each authorized user	**Identify the policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 2.5.2 Remote access to the TDE is permitted only from pre-determined and authorized locations and systems.		□	□	□	□
TSP 2.5.2.a Review documented procedures and interview personnel to verify that remote access for administrative activities is permitted only from pre-determined and authorized locations and systems.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 2.5.2.b Examine remote access system configuration and access logs to verify access is accepted only from authorized locations and systems.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** remote access logs confirm that access is accepted only from authorized locations and systems.				
	<Report Findings Here>				
	For each system component, **describe how** remote access system configurations ensure that access is accepted only from authorized locations and systems.				
	<Report Findings Here>				
TSP 2.5.3 Remote access using a personally owned device is prohibited, where that access could impact the security of the TDE or a TDE system.		□	□	□	□
TSP 2.5.3.a Review policies and procedures and interview personnel to verify that remote access using a personally owned device is prohibited unless verified that the device could not impact the security of the TDE or a TDE system.	**Identify the policies and procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.5.3.b Examine remote access system configuration and access logs to verify that remote access from personally owned devices is not permitted unless and until verified that the hardware could not impact the security of the TDE or a TDE system.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** the remote access system configurations do not permit remote access from personally owned devices unless and until verified that the hardware could not impact the security of the TDE or a TDE system.				
	<Report Findings Here>				
	For each system component, **describe how** the remote access system access logs show that remote access from personally owned devices is not permitted unless and until verified that the hardware could not impact the security of the TDE or a TDE system.				
	<Report Findings Here>				

<table>
<tr><th colspan="6"><em>TSP 2. Secure TDE Systems and Network</em></th></tr>
<tr><th rowspan="2">Requirements and Testing Procedures</th><th rowspan="2">Reporting Instructions & Assessor’s Findings</th><th colspan="4">Summary of Assessment Findings
(check one)</th></tr>
<tr><th>In Place</th><th>In Place w/ CCW</th><th>N/A</th><th>Not in Place</th></tr>
<tr><td colspan="2"><strong>TSP 2.5.4</strong> Remote access from non-TSP networks is not permitted to:
• The physical access-control system (e.g., badge access system).
• SCDs containing clear-text cryptographic keys or clear-text key components/shares.</td><td>□</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td rowspan="5"><strong>TSP 2.5.4</strong> Examine remote access policies and system configurations to verify that remote access is not permitted from non-TSP networks to:
• The physical access-control system (e.g., badge access system).
• SCDs containing clear-text cryptographic keys or clear-text key components/shares.</td><td><strong>Identify the remote access policies</strong> examined for this testing procedure.</td><td colspan="4"><em>&lt;Report Findings Here&gt;</em></td></tr>
<tr><td><strong>Identify the system component(s)</strong> examined for this testing procedure.</td><td colspan="4"><em>&lt;Report Findings Here&gt;</em></td></tr>
<tr><td colspan="5"><strong>Describe how</strong> system configurations do not permit remote access from non-TSP networks to:</td></tr>
<tr><td>• The physical access-control system (e.g., badge access system).</td><td colspan="4"><em>&lt;Report Findings Here&gt;</em></td></tr>
<tr><td>• SCDs containing clear-text cryptographic keys or clear-text key components/shares.</td><td colspan="4"><em>&lt;Report Findings Here&gt;</em></td></tr>
<tr><td colspan="2"><strong>TSP 2.5.5</strong> Remote changes must comply with PCI DSS change-management requirements.</td><td>□</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td rowspan="4"><strong>TSP 2.5.5</strong> Examine change-management records and interview personnel to verify that all changes performed via remote access are in adherence with PCI DSS change-management requirements.</td><td><strong>Identify the change management records for changes performed via remote access</strong> examined for this testing procedure.</td><td colspan="4"><em>&lt;Report Findings Here&gt;</em></td></tr>
<tr><td><strong>Identify the responsible personnel</strong> interviewed for this testing procedure.</td><td colspan="4"><em>&lt;Report Findings Here&gt;</em></td></tr>
<tr><td colspan="5"><em>For each change,</em> <strong>describe how</strong> the changes performed via remote access are in adherence with PCI DSS change management requirements.</td></tr>
<tr><td colspan="5"><em>&lt;Report Findings Here&gt;</em></td></tr>
<tr><td colspan="2"><strong>TSP 2.5.6</strong> All remote access privileges must be reviewed at least quarterly by an authorized individual to confirm access is still required. Retain documentation of reviews in accordance with PCI DSS Requirement 10.7.</td><td>□</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td></td><td><strong>Identify the documentation from the reviews</strong> examined for this testing procedure.</td><td colspan="4"><em>&lt;Report Findings Here&gt;</em></td></tr>
</table>

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 2.5.6.a Examine documentation from reviews and interview personnel to verify: • Remote access privileges are reviewed at least quarterly by an authorized individual, and • Documentation of reviews is retained in accordance with PCI DSS Requirement 10.7.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.5.6.b Examine remote access configurations and interview personnel to verify that only individuals with a confirmed business need have remote access.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the system component(s) examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** configurations confirm that only individuals with a confirmed business need have remote access.				
	<Report Findings Here>				
TSP 2.5.7 All non-console administrative access, and all remote access to systems in the TDE must use multi-factor authentication.		□	□	□	□
TSP 2.5.7.a Examine remote access configurations and interview personnel to verify that all non-console administrative access, and all remote access to systems in the TDE requires multi-factor authentication.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the system component(s) examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** configurations confirm that multi-factor authentication is required for all non-console administrative access to systems in the TDE.				
	<Report Findings Here>				
	For each system component, **describe how** configurations confirm that multi-factor authentication is required for all remote access to systems in the TDE.				

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
	<Report Findings Here>				
TSP 2.5.7.b Observe access processes for non-console administrative access and remote access to the TDE to verify multi-factor authentication is used.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how multi-factor authentication is used for non-console administrative access to the TDE.				
	<Report Findings Here>				
	Describe how multi-factor authentication is used for remote access to the TDE.				
	<Report Findings Here>				
TSP 2.5.8 All non-console administrative access, and all remote access to systems in the TDE must occur over a communication channel that uses strong cryptography for authentication and transmission, and that meets the requirements in TSP 2.6.		□	□	□	□
TSP 2.5.8.a Review usage policies to verify they require use of a secure communication channel for all non-console administrative access, and all remote access to the TDE.	**Identify the usage policies** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.5.8.b Examine remote access configurations to verify that use of secure communication technologies, as described in TSP 2.6, is enforced for all non-console administrative access and all remote access connections.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how remote access configurations confirm that that use of secure communication technologies, as described in TSP 2.6, is enforced for all non-console administrative access and all remote access connections.				
	<Report Findings Here>				
TSP 2.6 Access to HSMs					

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 2.6.1 Logical access to HSMs must be either at the HSM console or via an HSM non-console access solution that has been evaluated by an independent laboratory to comply with the following sections of ISO 13491-2:2005(E): • Annex A – Section A.2.2 Logical security characteristics, • Annex D – Section D.2: Logical security characteristics, • Annex E – Section E.2.1: Physical security characteristics, and Section E.2.2 Logical security characteristics • Annex F – Section F.2.1: Physical security characteristics, and Section F.2.2 Logical security characteristics, and • If digital signature functionality is provided: Annex G – Section G.2.1 General considerations, and Section G.2.2 Device management for digital signature verification		□	□	□	□
TSP 2.6.1.a Examine systems configurations and observe non-console access by authorized personnel to verify that logical access to HSMs is permitted only from the HSM console itself or via a validated HSM non-console access solution.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how system configurations ensure that logical access to HSMs is permitted only from the HSM console itself or via a validated HSM non-console access solution.				
	<Report Findings Here>				
	Describe how logical access to HSMs is permitted only from the HSM console itself or via a validated HSM non-console access solution.				
	<Report Findings Here>				
TSP 2.6.1.b If a non-console access solution is used, examine documentation (such as lab certification letters, solution technical documentation, or vendor attestation) to verify that the HSM non-console access solution has been evaluated by an independent laboratory to comply with the defined sections of ISO 13491-2:2005(E). ***Note:*** *An independent laboratory is one that is organizationally independent of the non-console management solution vendor, and is*	**Indicate whether** a non-console access is used. **(yes/no)** *If "no," mark the remainder of 2.6.1.b as "Not Applicable."* *If "yes," complete the following:*	*<Report Findings Here>*			
	Identify the documentation (such as lab certification letters, solution technical documentation, or vendor attestation) examined for this testing procedure.	*<Report Findings Here>*			

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
not otherwise subject to any commercial, financial, or other commitment that might influence their evaluation of the vendor's product.	**Provide the name of the assessor** who attests that the HSM non-console access solution has been evaluated by an independent laboratory to comply with the defined sections of ISO 13491-2:2005(E).	*<Report Findings Here>*			
TSP 2.6.2 All non-console access to HSMs within the TDE must originate from the TDE or another CDE within the TSP.		□	□	□	□
TSP 2.6.2 Examine network and system configuration settings to verify that non-console access to HSMs within the TDE is only permitted from systems located in the TDE or another CDE within the TSP.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** network and system configuration settings confirm that non-console access to HSMs within the TDE is only permitted from systems located in the TDE or another CDE within the TSP.				
	<Report Findings Here>				
TSP 2.6.3 Devices with non-console access to HSMs in the TDE must be secured as follows: ***Note:*** *The term "devices" in these requirements refers to the endpoint device (for example, a PC, laptop, terminal, or secure cryptographic device) that an individual is using to access the HSM via a non-console connection.*					
TSP 2.6.3.1 Devices must be located in a designated secure area or room that is monitored at all times.		□	□	□	□
TSP 2.6.3.1.a Review policies and procedures and interview personnel to verify that devices with non-console access to HSMs must be located in a designated secure area or room that is monitored at all times while in use.	**Identify the policies and procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.6.3.1.b Observe locations of devices with non-console access to HSMs and verify they are located in a designated secure area or room that is monitored at all times while in use.	**Provide the name of the assessor** who attests that devices with non-console access to HSMs are located in a designated secure area or room that is monitored at all times while in use.	*<Report Findings Here>*			
TSP 2.6.3.2 Devices that are dedicated to managing HSM functions must be disconnected from all networks and secured in a locked room/rack/cabinet/drawer/safe when not in use.		□	□	□	□

TSP 2. Secure TDE Systems and Network					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 2.6.3.2.a If dedicated devices are used for non-console access to HSMs: Review policies and procedures and interview personnel to verify that devices with non-console access to HSMs must be disconnected from all networks and secured in a locked room/rack/cabinet/drawer/safe when not in use.	**Indicate whether** dedicated devices are used for non-console access to HSMs. **(yes/no)** *If "no," mark the remainder of 2.6.3.2.a as "Not Applicable."* **If "yes," complete the following:**	*<Report Findings Here>*			
	Identify the policies and procedures reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.6.3.2.b Observe locations of dedicated devices and verify they are disconnected from all networks and secured in a locked room/rack/cabinet/drawer/safe when not in use.	**Provide the name of the assessor** who attests that dedicated devices are disconnected from all networks and secured in a locked room/rack/cabinet/drawer/safe when not in use.	*<Report Findings Here>*			
TSP 2.6.3.3 Physical access to devices with non-console access must be restricted to authorized personnel and managed under dual control.		□	□	□	□
TSP 2.6.3.3.a Review policies and procedures and interview personnel to verify that physical access to devices with non-console access to HSMs must be restricted to authorized personnel and managed under dual control.	**Identify the policies and procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 2. Secure TDE Systems and Network					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 2.6.3.3.b Observe locations of devices with non-console access to HSMs and verify that physical access to the devices is restricted to authorized personnel and managed under dual control.	**Describe how** physical access to the devices with non-console access to HSMs is restricted to authorized personnel and managed under dual control.				
	<Report Findings Here>				
TSP 2.6.3.4 Authentication mechanisms (e.g., smart cards, dongles etc.) for devices with non-console access must be physically secured when not in use.		□	□	□	□
TSP 2.6.3.4.a Review policies and procedures and interview personnel to verify that authentication mechanisms for devices with non-console access to HSMs must be physically secured when not in use.	**Identify the policies and procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.6.3.4.b Observe authentication mechanisms for devices with non-console access to HSMs and verify they are physically secured when not in use.	**Describe how** authentication mechanisms for devices with non-console access to HSMs are physically secured when not in use.				
	<Report Findings Here>				
TSP 2.6.3.5 Operation of a device with non-console access requires dual control and multi-factor authentication.		□	□	□	□
TSP 2.6.3.5.a Review policies and procedures and interview personnel to verify that operation of devices with non-console access to HSMs requires dual control and multi-factor authentication.	**Identify the policies and procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.6.3.5.b Observe usage of devices with non-console access to HSMs and verify that dual control and multi-factor authentication is required.	**Describe how** dual control and multi-factor authentication is required for devices with non-console access to HSMs.				
	<Report Findings Here>				
TSP 2.6.3.6 Devices must only have applications and software installed as necessary to support / perform the functions for which it requires access to the HSM (e.g., HSM configuration).		□	□	□	□
TSP 2.6.3.6.a Review system configuration standards and interview personnel to verify that necessary applications and software are	**Identify the system configuration standards** reviewed for this testing procedure.	*<Report Findings Here>*			

TSP 2. Secure TDE Systems and Network					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
defined and documented for devices with non-console access to HSMs.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.6.3.6.b Examine device configurations to verify that only the applications and software defined as necessary for the device to perform non-console access functions is installed.	**Identify the devices** examined for this testing procedure.	*<Report Findings Here>*			
	For each device, **describe how** device configurations confirm that only the applications and software defined as necessary for the device to perform non-console access functions is installed.				
	<Report Findings Here>				
TSP 2.6.3.7 Devices must be verified as having up to date security configurations (e.g., security patches, anti-virus software etc. as applicable for the type/function of device) prior to being granted access		□	□	□	□
TSP 2.6.3.7.a Observe processes and interview personnel to verify that devices are verified as having up to date security configurations (e.g., security patches, anti-virus software etc. as applicable for the type/function of device) prior to being granted access.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe the processes observed to confirm that devices have up to date security configurations (e.g., security patches, anti-virus software etc. as applicable for the type/function of device) prior to being granted access.				
	<Report Findings Here>				
TSP 2.6.3.8 Devices must not be connected to other networks whilst connected to the HSM.		□	□	□	□
TSP 2.6.3.8.a Review policies and procedures and interview personnel to verify that devices must not have any other active network connections whilst connected to the HSM.	**Identify the policies and procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.6.3.8.b Examine device configurations and observe connection processes to verify that no other connections are active on the device during non-console access to the HSM.	**Identify the devices** examined for this testing procedure.	*<Report Findings Here>*			
	For each device, **describe how** device configurations ensure that no other connections are active on the device during non-console access to the HSM.				

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
	<Report Findings Here>				
	Describe how no other connections are active on the device during non-console access to the HSM.				
	<Report Findings Here>				
TSP 2.6.3.9 Devices must be cryptographically authenticated prior to the connection being granted access to HSM functions.		□	□	□	□
TSP 2.6.3.9.a Review policies and procedures and interview personnel to verify that devices must be cryptographically authenticated prior to being granted access to the HSM.	**Identify the policies and procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.6.3.9.b Examine device configurations and observe connection processes to verify that devices are cryptographically authenticated prior to being granted access to the HSM.	**Identify the devices** examined for this testing procedure.	*<Report Findings Here>*			
	For each device, **describe how** configurations ensure that devices are cryptographically authenticated prior to being granted access to the HSM.				
	<Report Findings Here>				
	Describe how devices are cryptographically authenticated prior to being granted access to the HSM.				
	<Report Findings Here>				
TSP 2.6.4 Non-console access procedures must be designed such that there are no means available for "man-in-the-middle" attacks.		□	□	□	□
TSP 2.6.4 Examine non-console access configurations and observe connection processes to verify there are no means available for "man-in-the-middle" attacks.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** non-console access configurations confirm that there are no means available for "man-in-the-middle" attacks.				

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings		Summary of Assessment Findings (check one)			
			In Place	In Place w/ CCW	N/A	Not in Place
	<Report Findings Here>					
	Describe how there are no means available for "man-in-the-middle" attacks.					
	<Report Findings Here>					
TSP 2.6.5 System implementations must be designed and implemented to prevent replay attacks.			□	□	□	□
TSP 2.6.5 Examine device configurations and observe connection processes to verify controls are implemented to prevent replay attacks.	**Identify the devices** examined for this testing procedure.	*<Report Findings Here>*				
	For each device, **describe how** the configurations confirm that controls are implemented to prevent replay attacks.					
	<Report Findings Here>					
	Describe how replay attacks were prevented during the connection processes.					
	<Report Findings Here>					
TSP 2.6.6 The loading and exporting of clear-text cryptographic keys, key components and/or key shares to/from the HSM is not permitted over a non-console connection.			□	□	□	□
TSP 2.6.6.a Review policies and procedures and interview personnel to verify that the loading and exporting of clear-text cryptographic keys, key components and/or key shares to/from the HSM is not permitted over a non-console connection.	**Identify the policies and procedures** reviewed for this testing procedure.	*<Report Findings Here>*				
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*				
TSP 2.6.6.b Examine device configurations to verify that neither loading nor exporting of cryptographic keys, key components and/or key shares to/from the HSM is performed over a non-console connection.	**Identify the devices** examined for this testing procedure.	*<Report Findings Here>*				
	For each device, **describe how** the configurations confirm that neither loading nor exporting of cryptographic keys, key components and/or key shares to/from the HSM is performed over a non-console connection.					
	<Report Findings Here>					

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 2.6.7 Non-console access activities must adhere to all other HSM and key-management requirements—for example, commands resulting in an encryption or decryption operation must be authorized under dual control.		□	□	□	□
TSP 2.6.7.a Review policies and procedures and interview personnel to verify that all procedural and logical controls required for HSM and key-management functions must be adhered to during non-console access connections.	**Identify the policies and procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.6.7.b Examine device configurations and observe connection processes to verify that all procedural and logical controls required for HSM and key-management functions are adhered to during non-console access connections.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** the device configurations confirm that all procedural and logical controls required for HSM and key-management functions are adhered to during non-console access connections.				
	<Report Findings Here>				
	Describe how all procedural and logical controls required for HSM and key-management functions are adhered to during non-console access connections.				
	<Report Findings Here>				
TSP 2.6.8 All non-console access to HSMs in the TDE must occur over a communication channel that meets the requirements in TSP 2.7.		□	□	□	□
TSP 2.6.8 Examine HSM non-console access configurations to verify that the requirements in TSP 2.7 are enforced for all non-console connections.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how HSM non-console access configurations confirm that the requirements in TSP 2.7 are enforced for all non-console connections.				
	<Report Findings Here>				
TSP 2.7 Strong Cryptography for Non-Console and Remote Access					
TSP 2.7.1 All communications must use strong cryptography for authentication and transmission.		□	□	□	□

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 2.7.1 Examine system configuration settings to verify that the strong cryptography is used for authentication and transmission.	**Describe how** system configuration settings confirm that the strong cryptography is used for authentication and transmission.				
	<Report Findings Here>				
TSP 2.7.2 Mechanisms (e.g., digital signatures, checksums) must exist to detect unauthorized changes to configuration and change-control settings.		□	□	□	□
TSP 2.7.2.a Examine system configuration settings to verify that mechanisms are enabled to detect unauthorized changes to configuration and change-control settings.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** system configuration settings confirm that mechanisms are enabled to detect unauthorized changes to configuration and change-control settings.				
	<Report Findings Here>				
TSP 2.7.2.b Examine logs and records of testing to verify the mechanism is tested at least annually to confirm it is working as intended.	**Identify the logs** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the records of testing examined for this testing procedure.	*<Report Findings Here>*			
TSP 2.7.2.c Examine audit logs and alerts, and interview responsible personnel to verify that alerts are investigated.	**Identify the audit logs** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the alerts examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.7.3 Multi-factor authentication must be used for all connections		□	□	□	□
TSP 2.7.3 Examine system configurations and verify multi-factor authentication is required.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
	For each system component, **describe how** system configurations confirm that multi-factor authentication is required.				
	<Report Findings Here>				
TSP 2.7.4 Access must be declined after three consecutive unsuccessful access attempts.		□	□	□	□
TSP 2.7.4.a Inspect configuration settings to verify that authentication parameters are set to lockout user accounts after not more than three unsuccessful access attempts.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** configuration settings confirm that authentication parameters are set to lockout user accounts after not more than three unsuccessful access attempts.				
	<Report Findings Here>				
TSP 2.7.4.b Review audit logs to verify that access is declined after not more than three consecutive unsuccessful access attempts.	**Identify the audit logs** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.7.5 Access counters must only be reset by an authorized individual (e.g., security administrator) after user identification has been validated.		□	□	□	□
TSP 2.7.5.a Inspect configuration settings to verify that access counters can only be reset by authorized individuals.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** configuration settings confirm that access counters can only be reset by authorized individuals.				
	<Report Findings Here>				
TSP 2.7.5.b Review user IDs authorized with reset privileges and interview personnel to verify that authority for resets is appropriately assigned.	**Identify the User IDs authorized with reset privileges** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 2.7.5.c Interview personnel and review documented procedures for resetting access counters to verify user validation by another authorized individual is required prior to reset of the access counter.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.7.6 Access must be logged, and the log must be reviewed at least weekly for suspicious activity.		□	□	□	□
TSP 2.7.6.a Examine system configurations and audit logs to verify that access is logged.	**Identify the audit logs** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the system configurations examined for this testing procedure.	*<Report Findings Here>*			
TSP 2.7.6.b Review documented procedures and interview personnel to verify access logs are reviewed at least weekly to identify suspicious activity.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.7.7 Connections using Internet Protocol Security (IPSec) must meet the following: i. Tunnel mode must be used except where communication is host-to-host. ii. Aggressive mode must not be used for tunnel establishment. iii. The device authentication method must use certificates obtained from a trusted Certificate Authority (CA). iv. Encapsulating Security Payload (ESP) must be used to provide data confidentiality and authentication. v. The Perfect Forward Secrecy (PFS) option of Internet Key Exchange (IKE) must be used to protect against session key compromise. ***Note:*** *If an internal CA is used for VPN certificates, it must be verified as meeting industry standards (for example, via independent audit to TS101456).*		□	□	□	□

TSP 2. Secure TDE Systems and Network					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 2.7.7 For all connections using IPSec, examine VPN system documentation and configuration settings to verify that the following security features are fully documented and implemented: i. Tunnel mode is used except where communication is host-to-host. ii. Aggressive mode is not used for tunnel establishment. iii. The device authentication method uses certificates obtained from a trusted Certificate Authority (CA). iv. Encapsulating Security Payload (ESP) is used to provide data confidentiality and authentication. v. The Perfect Forward Secrecy (PFS) option of Internet Key Exchange (IKE) is used to protect against session key compromise.	**Indicate whether** IPSec connections are used. **(yes/no)** *If "no," mark the remainder of TSP 2.7.7 as "Not Applicable."* *If "yes," complete the following:*	*<Report Findings Here>*			
	Identify the VPN system documentation examined for this testing procedure.	*<Report Findings Here>*			
	Identify the system component(s) examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** configuration settings confirm that the following security features are fully documented and implemented:				
	i. Tunnel mode is used except where communication is host-to-host.				
	<Report Findings Here>				
	ii. Aggressive mode is not used for tunnel establishment.				
	<Report Findings Here>				
	iii. The device authentication method uses certificates obtained from a trusted Certificate Authority.				
	<Report Findings Here>				
	iv. Encapsulating Security Payload (ESP) is used to provide data confidentiality and authentication.				
	<Report Findings Here>				
	v. The Perfect Forward Secrecy (PFS) option of Internet Key Exchange (IKE) is used to protect against session key compromise.				
	<Report Findings Here>				

TSP 2. Secure TDE Systems and Network

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 2.8 Wireless Networks					
TSP 2.8.1 The TDE must not use or be connected to any wireless network or system. ***Note****: Where there is a legitimate, documented business reason, it is permissible for a device with TDE access to have wireless capability, on condition that the wireless capability is disabled prior to and for the duration of TDE access.*		□	□	□	□
TSP 2.8.1.a Examine firewall and router configurations to verify the TDE does not use or connect to any wireless network.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** the firewall and router configurations confirm that the TDE does not use or connect to any wireless network.				
	<Report Findings Here>				
TSP 2.8.1.b For devices with access to the TDE, examine documentation and system configurations to verify that *either*: • Devices have no wireless capability, or • If there is a documented business need for the device to also have wireless capability, policies and procedures are implemented to disable wireless prior to and for the duration of TDE access.	**Identify the document(s)** examined for this testing procedure.	*<Report Findings Here>*			
	Identify devices with access to the TDE.	*<Report Findings Here>*			
	For each device with access to the TDE, **describe how** system configurations confirm that either: • Devices have no wireless capability, or • If there is a documented business need for the device to also have wireless capability, policies and procedures are implemented to disable wireless prior to and for the duration of TDE access.				
	<Report Findings Here>				
TSP 2.8.1.c For any devices with wireless capability, interview device users and examine audit logs to verify that wireless capability is disabled prior to and for the duration of TDE access.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the system component(s) examined for this testing procedure.	*<Report Findings Here>*			

TSP 2. Secure TDE Systems and Network					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
	For each system component, **describe how** audit logs show that wireless capability is disabled prior to and for the duration of TDE access.				
	<Report Findings Here>				
TSP 2.8.2 To prevent the introduction of wireless devices, random scans of the TDE must be conducted at least monthly using a scanning device that is capable of detecting rogue and hidden wireless networks.		□	□	□	□
TSP 2.8.2.a Review results of scans and interview personnel to verify that random scans to detect wireless devices are conducted at least monthly.	**Identify the results of scans** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 2.8.2.b Review process documentation and examine the capabilities of the scanning method used to verify the scans are capable of detecting rogue and hidden wireless networks.	**Identify the process documentation** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the scanning method used.	*<Report Findings Here>*			
	Describe how the scanning method used is capable of detecting rogue and hidden wireless networks.				
	<Report Findings Here>				

TSP 3. Protect and manage cryptographic keys

These requirements apply to all cryptographic keys used for tokenization processes in the TDE, including:

- Keys used to encrypt/decrypt PAN and PAN-to-Payment Token mapping references
- Keys used to protect Payment Token functions in the TDE
- Keys used for domain restriction validation, such as the cryptogram validation
- Keys used to protect Payment Token Data during storage, processing, and transmission

The requirements in this section build PCI DSS Requirement 3. When applying PCI DSS Requirement 3 to the TDE, the following principles apply:

- Where PCI DSS Requirement 3 specifically mentions PAN or CHD, the requirement also applies to Payment Tokens within the TDE. For example, PAN and Payment Tokens must be masked when displayed such that only personnel with a legitimate business need can see the full PAN/Payment Token (PCI DSS Requirement 3.3), and rendered unreadable wherever they are stored (PCI DSS requirement 3.4).
- The key-management requirements in this section are in addition to those in PCI DSS Requirements 3.5 – 3.6.

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.1 General Principles					
TSP 3.1.1 All TDE key-management activity must be performed using a HSM that is either: • FIPS 140-2 Level 3 (overall) or higher certified, or • PCI PTS HSM approved.		□	□	□	□
TSP 3.1.1.a Interview responsible personnel to verify that all key-management activities are performed within a HSM.	**Identify the responsible personnel interviewed for this testing procedure.**	*<Report Findings Here>*			
TSP 3.1.1.b For all HSMs used in the TDE, examine approval documentation (e.g., FIPS certification or PTS approval) and review the list of approved devices to verify that all HSMs used are either:	**Identify the approval documentation** (e.g., FIPS certification or PTS approval) reviewed for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
• Listed on the NIST Cryptographic Module Validation Program (CMVP) list, with a valid listing number, and approved to FIPS 140-2 Level 3 (overall), or higher. Refer to http://csrc.nist.gov. • Listed on the PCI SSC website, with a valid PCI SSC listing number, as an Approved PCI PTS Device under the approval class "HSM."	**Identify the HSMs** used in the TDE.	*<Report Findings Here>*			
	For each HSM in the TDE, **describe how** the HSMs used 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 (overall), or higher. Refer to http://csrc.nist.gov. • Listed on the PCI SSC website, with a valid PCI SSC listing number, as an Approved PCI PTS Device under the approval class "HSM."				
	<Report Findings Here>				
TSP 3.1.2 A documented description of the cryptographic architecture must exist that includes: • Details of all keys used by each HSM • Description of the key usage for each key		□	□	□	□
TSP 3.1.2 Interview responsible personnel and review documentation to verify that a document exists to describe the cryptographic architecture, including details of all keys used by each HSM and a description of usage for each key.	**Identify the documentation** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.1.3 Where clear-text key components or shares pass through a PC or other equipment, the equipment must never be connected to any network and must be powered down when not in use. Devices used for the generation/transmission of clear-text key components or shares must be powered off when not in use and not connected to any network.		□	□	□	□

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 3.1.3 Examine documented procedures for all key-handling methods. Verify procedures require that devices that handle clear-text key components are - Powered off when not in use - Not connected to any network	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.1.4 All cryptographic keys used for tokenization operations must use algorithms and key sizes in accordance with *Annex A* of this document.		□	□	□	□
TSP 3.1.4.a Examine documented key-management policies and procedures to verify that all cryptographic keys use algorithms and key sizes that are in accordance with *Annex A.*	**Identify the key management policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.1.4.b Observe key-management operations and devices to verify that all cryptographic algorithms and key sizes are in accordance with *Annex A.*	**Describe how** all cryptographic algorithms and key sizes are in accordance with *Annex A.*				
	<Report Findings Here>				
	Describe how all cryptographic algorithms and key sizes are in accordance with *Annex A.*				
	<Report Findings Here>				
TSP 3.1.5 All key-encrypting keys (KEKs) used to transmit or convey other cryptographic keys must be at least as strong as the key being transmitted or conveyed.		□	□	□	□
TSP 3.1.5.a Examine documented key-management policies and procedures to verify that all key-encrypting keys (KEKs) used to transmit or convey other cryptographic keys are at least as strong as the key being transmitted or conveyed.	**Identify the key management policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.1.5.b Observe key-management operations and devices to verify that all key-encrypting keys (KEKs) used to transmit or	**Describe how** all key-encrypting keys (KEKs) used to transmit or convey other cryptographic keys are at least as strong as the key being transmitted or conveyed.				

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
convey other cryptographic keys are at least as strong as the key being transmitted or conveyed.	*<Report Findings Here>*				
	Describe how all key-encrypting keys (KEKs) used to transmit or convey other cryptographic keys are at least as strong as the key being transmitted or conveyed.				
	<Report Findings Here>				
TSP 3.1.6 Cryptographic keys must not be embedded (hard-coded) into software.		□	□	□	□
TSP 3.1.6.a Review policies and procedures and interview personnel to verify that the embedding of cryptographic keys into software (for example, in shell scripts, command files, communication scripts, software code etc.) is strictly prohibited.	**Identify the policies and procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.1.6.b Inspect software configuration (for example, shell scripts, command files, communication scripts, software code etc.) to verify that cryptographic keys are not embedded.	**Identify the software configuration(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each, **describe how** the software configurations (for example, shell scripts, command files, communication scripts, software code etc.) confirm that cryptographic keys are not embedded.				
	<Report Findings Here>				
TSP 3.1.7 Key-management activities must be performed by TSP or issuer personnel or an authorized third party. If any key-management activity is outsourced to a third party, the third party must meet all applicable requirements in this document.		□	□	□	□
TSP 3.1.7.a Examine documented key-management policies and procedures and interview responsible personnel to verify that all functions are performed by TSP or issuer personnel, or an authorized third party.	**Identify the documented key management policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.1.7.b If key-management activities are outsourced to a third party, review the third party's PCI Attestation of Compliance to verify they are in compliance with all applicable requirements in this document.	**Indicate whether** key-management activities are outsourced to a third party. **(yes/no)** *If "no," mark the remainder of 3.1.7.b as "Not Applicable."* *If "yes," complete the following:*	*<Report Findings Here>*			
	Identify the third party's PCI Attestation of Compliance reviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how the third party is compliant with all applicable requirements in this document.				
	<Report Findings Here>				
TSP 3.1.8 Key-management activities must only be performed by fully trained and authorized personnel.		□	□	□	□
TSP 3.1.8.a Examine documented procedures and processes to verify that only authorized personnel have the ability to perform key-management activities.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how only authorized personnel have the ability to perform key-management activities.				
	<Report Findings Here>				
TSP 3.1.8.b Interview responsible personnel and observe HSM system configurations and processes to verify that only authorized users have the ability to access keys.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the HSM(s) examined for this testing procedure.	*<Report Findings Here>*			
	For each HSM, **describe how** the system configurations confirm that only authorized users have the ability to access keys.				

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
	<Report Findings Here>				
TSP 3.1.8.c Interview responsible personnel to ensure they have undergone relevant training for the key-management functions they perform.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.1.9 Audit trails must be maintained for all key-management activities and all activities involving clear-text key components. The audit log must include: • Unique identification of the individual that performed each function • Date and time • Function being performed • Purpose • Success or Failure of activity		□	□	□	□
TSP 3.1.9.a Examine policies and processes to verify that all key-management activities and all activities involving clear-text key components must be logged.	**Identify the policies** examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.1.9.b Through interviews and observation of audit logs, verify that all key-management activities and all activities involving clear-text key components are logged, and the logs include: • Unique identification of the individual that performed each function • Date and time • Function being performed • Purpose • Success or Failure of activity	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the audit logs examined for this testing procedure.	*<Report Findings Here>*			
	Describe how the audit logs include all key-management activities and all activities involving clear-text key components to include:				
	• Unique identification of the individual that performed each function				

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
	<Report Findings Here>				
	• Date and time				
	<Report Findings Here>				
	• Function being performed				
	<Report Findings Here>				
	• Purpose				
	<Report Findings Here>				
	• Success or Failure of activity				
	<Report Findings Here>				
TSP 3.2 Symmetric and Asymmetric Keys					
TSP 3.2.1 Symmetric keys and private keys must exist only in the following forms: i. As clear-text inside the protected memory of a secure cryptographic device ii. As a cryptogram iii. As two or more full-length components (where each component must be the same length as the final key) or as part of an "m of n" sharing scheme where the value of "m" is at least 2.		□	□	□	□
TSP 3.2.1 Examine documented procedures and system configurations to verify symmetric keys and private keys exist only in the following forms: i. As clear-text inside the protected memory of a secure cryptographic device ii. As a cryptogram iii. As two or more full-length components (where each component must be the same length as the final key) or as part of an "m of n" sharing scheme where the value of "m" is at least 2.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the system component(s) examined for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
	For each system component, **describe how** system configurations confirm that symmetric keys and private keys exist only in the following forms: i. As clear-text inside the protected memory of a secure cryptographic device ii. As a cryptogram iii. As two or more full-length components (where each component must be the same length as the final key) or as part of an "m of n" sharing scheme where the value of "m" is at least 2.				
	<Report Findings Here>				
TSP 3.2.2 Management of key components and key sharing schemes must ensure the following conditions are met: i. The components or shares must be managed using the principles of dual control and split knowledge. ii. No single person shall be able to access or use all components or a quorum of shares of a single secret or private cryptographic key. iii. Effective implementation of these principles must enforce the existence of physical barriers beyond procedural controls to prevent any one individual from gaining access to key components or shares sufficient to form the actual key.		□	□	□	□
TSP 3.2.2.a If symmetric keys or private keys exist as components or key shares, examine documented procedures and interview personnel to verify that: i. Components and shares are managed using the principles of dual control and split knowledge. ii. No single person is able to access or use all components or a quorum of shares of a single secret or private cryptographic key.	**Indicate whether** symmetric keys or private keys exist as components or key shares. **(yes/no)** *If "no," mark the remainder of TSP 3.2.2.a as "Not Applicable."* *If "yes," complete the following:*	*<Report Findings Here>*			
	Identify the documented procedures examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor’s Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.2.2.b Observe implemented physical and logical controls to verify these principles are enforced by the existence of physical barriers beyond procedural controls to prevent any one individual from gaining access to key components or shares sufficient to form the actual key.	**Describe how** physical and logical controls are enforced by the existence of physical barriers beyond procedural controls to prevent any one individual from gaining access to key components or shares sufficient to form the actual key.				
	<Report Findings Here>				

TSP 3. Protect and manage cryptographic keys					
		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.2.3 Public keys must have their authenticity and integrity ensured. In order to ensure authenticity and integrity, a public key must either be encrypted, or if in clear-text form, must exist only in one of the following forms: • Within a certificate created by a trusted Certificate Authority (CA), • Within a PKCS#10, • Within an SCD, or • With a MAC (message authentication code) created using the algorithm defined in ISO 16609. ***Note:*** *If an internal CA is used, it must be verified as meeting industry standards (for example, via independent audit to TS101456).*		□	□	□	□
TSP 3.2.3.a Examine documented procedures for public keys to verify that public keys must exist only in one of the following forms: • Within a certificate created by a trusted CA • Within a PKCS#10, • Within an SCD, or • Using a MAC (message authentication code) created using the algorithm defined in ISO 16609.	**Identify the documented procedures** for public keys examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.2.3.b Observe key-management processes and interview responsible personnel to verify that the implemented method(s) ensures the authenticity and integrity of public keys.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how the implemented method(s) ensures the authenticity and integrity of public keys.				
	<Report Findings Here>				
TSP 3.3 Key-Management Security Administration ***Note:*** *These requirements relate to the procedures and activities for managing keys and key sets*					

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.3.1 Procedures must be defined for the transfer of key-management roles between individuals.		□	□	□	□
TSP 3.3.1.a Examine documented procedures to verify that procedures for transferring key-management roles between individuals are defined**.**	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.3.1.b Interview responsible personnel in applicable key-management roles to verify they are aware of and are following the documented procedures.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.3.2 All access to physical equipment associated with key-management activity, such as HSMs or personal computers, must be managed following the principle of dual control, such that no single person is able to access or perform key-management functions.		□	□	□	□
TSP 3.3.2.a Examine documented procedures to verify that access to physical equipment associated with key-management activity is managed such that no single person is able to access or perform key-management functions.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.3.2 b Interview personnel and observe the process of accessing physical equipment to verify that dual control is required to access or perform key-management functions.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how dual control is required to access or perform key-management functions.				
	<Report Findings Here>				
TSP 3.3.3 Key Managers must be designated and managed as follows.					

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.3.3.1 There must be a nominated Key Manager approved by the CISO (or equivalent), with overall responsibility for all activities relating to key management. The Key Manager must: • Have a nominated deputy. • Be responsible for ensuring that all key-management activity is fully documented. • Be responsible for ensuring that all key-management activity is carried out in accordance with the documented procedures. • In collaboration with the personnel department, vet all key custodians to ensure their suitability for the role.		□	□	□	□
TSP 3.3.3.1.a Examine documentation to verify the Key Manager is approved by CISO (or equivalent), with overall responsibility for all activities relating to key management.	**Identify the documentation** examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.3.3.1.b Examine documentation and interview Key Manager to verify that the Key Manager: • Has a nominated deputy. • Is responsible for ensuring that all key-management activity is fully documented. • Is responsible for ensuring that all key-management activity is carried out in accordance with the documented procedures. • In collaboration with the personnel department, vets all key custodians to ensure their suitability for the role.	**Identify the documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.3.3.2 Incident response procedures, including notification to the Key Manager, must be initiated immediately upon any security breach or loss of integrity relating to a cryptographic key or key-management activities.		□	□	□	□
TSP 3.3.3.2 Examine documented incident response procedures to verify processes are in place to notify the Key Manager of any security breach or loss of integrity relating to a cryptographic key or key-management activities.	**Identify the documented incident response procedures** examined for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 3.3.3.3 The Key Manager must be responsible for ensuring that: i. All key custodians have been trained with regard to their responsibilities, and this forms part of their annual security training. ii. Each custodian signs a statement, or is legally bonded, acknowledging that they understand their responsibilities. iii. Key custodians who form the necessary threshold to create a key must not report directly to the same manager. If the Key Manager is also a key custodian, other key custodians must not report to the Key Manager if, in conjunction with the Key Manager, that would form a threshold to create a key.		□	□	□	□
TSP 3.3.3.3.a Examine documentation and interview Key Manager to verify that the Key Manager is aware of their responsibility to ensure: i. All key custodians are trained with regard to their responsibilities as part of their annual security training. ii. Each custodian signs a statement, or is legally bonded, acknowledging that they understand their responsibilities. iii. Key custodians who form the necessary threshold to create a key do not report directly to the same manager. If the Key Manager is also a key custodian, other key custodians do not report to the Key Manager if, in conjunction with the Key Manager, that would form a threshold to create a key.	**Identify the documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the Key Manager interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.3.3.3.b Examine roles and responsibilities and organization chart to ensure that key custodians responsible for creating keys do not report to the same manager.	**Identify the roles and responsibilities** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the organization chart examined for this testing procedure.	*<Report Findings Here>*			
	Describe how key custodians responsible for creating keys do not report to the same manager.				
	<Report Findings Here>				
TSP 3.3.3.4 The Key Manager must not have the right to override operations of the key custodians or perform activities for other key custodians.		□	□	□	□

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.3.3.4 Examine documentation and interview responsible personnel to verify that Key Managers do not have the right to override operations of the key custodians or perform activities for other key custodians.	**Identify the documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.3.4 Key custodians and custodian back-ups must be designated and managed as follows.					
TSP 3.3.4.1 A designated key custodian(s) and back-up custodian must be assigned for each key component, with the fewest number of custodians assigned as necessary to enable effective key management. Back-up custodians must only be designated for a single primary key custodian.		□	□	□	□
TSP 3.3.4.1 Examine the list of key custodians to ensure that: • Each key component has a primary and a back-up custodian. • The fewest number of custodians are assigned as necessary to enable effective key management. • Back-up custodians are designated for a single primary key custodian.	**Identify the list of key custodians** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how the list of key custodians shows that:				
	• Each key component has a primary and a back-up custodian.				
	<Report Findings Here>				
	• The fewest number of custodians are assigned as necessary to enable effective key management.				
	<Report Findings Here>				
	• Back-up custodians are designated for a single primary key custodian.				
	<Report Findings Here>				
TSP 3.3.4.2 The roles and responsibilities of key custodians must be fully documented at a level sufficient to allow performance of required activities on a step-by-step basis.		□	□	□	□
TSP 3.3.4.2.a Examine documentation to verify that roles and responsibilities of key custodians are fully documented at a level sufficient to allow performance of required activities on a step-by-step basis.	**Identify the documentation** examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.3.4.2.b Interview key custodian personnel to verify the documented roles and responsibilities allow performance of required activities on a step-by-step basis.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.3.4.3 The suitability of key custodian personnel (primary and back-up) must be reviewed on an annual basis.		□	□	□	□
TSP 3.3.4.3 Examine documentation and interview responsible personnel to verify that primary and back-up key custodians are reviewed annually for suitability to the role.	**Identify the documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.3.4.4 Key custodians and their back-ups must be employees of the TSP or applicable TSP customer (e.g., the Issuer for whom the TSP is managing payment tokens), or an authorized third party. If any key-management activity is outsourced to a third party, the third party must meet all applicable requirements in this document.		□	□	□	□
TSP 3.3.4.4.a Examine documentation and interview responsible personnel to verify that key custodians and their back-ups are employees of the TSP or applicable TSP customer (e.g., the Issuer for whom the TSP is managing Payment Tokens), or an authorized third party.	**Identify the documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.3.4.4.b If any key-management activity is outsourced to a third party, examine documentation and interview responsible personnel to verify the third party meets all applicable requirements in this document.	**Indicate whether** any key management activity is outsourced to a third party. **(yes/no)** *If "no," mark the remainder of TSP 3.3.4.4.b as "Not Applicable."* If "yes," complete the following:	*<Report Findings Here>*			
	Identify the documentation examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.3.4.5 Key custodians must be provided with a list of responsibilities and sign a statement acknowledging their responsibilities for safeguarding key components, shares, or other keying materials entrusted to them.		□	□	□	□
TSP 3.3.4.5.a. Examine documentation and interview responsible personnel to verify that key Custodians are provided with a list of	**Identify the documentation** examined for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
responsibilities for safeguarding key components, shares, or other keying materials entrusted to them.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.3.4.5.b Examine signed statements or other legally binding documentation signed by key custodians to verify they acknowledge understanding of their responsibilities.	**Identify the signed statements or other legally binding documentation** examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.3.5 PINs and pass-phrases used with key-management devices must be managed as follows: • If PINs or pass-phrases are stored the PIN or pass-phrase must be stored securely. • Only those person(s) who need access to a device must have access to the PIN or pass-phrase for that device. • There must be a defined policy regarding the PINs and pass-phrases needed to access key-management devices. This policy must include the length and character-mix of such PINs and pass-phrases, and the frequency of change.		□	□	□	□
TSP 3.3.5.a Examine location where the PIN or pass-phrase is stored and ensure it is stored securely.	**Describe how** the location where the PIN or pass phrase is stored is secure.				
	<Report Findings Here>				
TSP 3.3.5.b Examine access controls and interview personnel to verify that person(s) with access to the PIN or pass-phrase have a business need to access the applicable key-management devices.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the access controls examined for this testing procedure.	*<Report Findings Here>*			
	Describe how the access controls examined confirm that person(s) with access to the PIN or pass-phrase have a business need to access the applicable key-management devices.				
	<Report Findings Here>				
TSP 3.3.5.c Examine policy regarding using PINs and pass-phrases to access key-management devices. Verify that the policy includes the length and character-mix of such PINs and pass-phrases, and the frequency of change.	**Identify the policy regarding using PINs and pass phrases to access key-management devices** examined for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.4 Key Generation					
TSP 3.4.1 Keys and key components must be generated using a random or pseudo-random process (as described in ISO 9564-1 and ISO 11568-5) that is capable of satisfying the statistical tests of National Institute of Standards and Technology (NIST) SP 800-22 or equivalent.		□	□	□	□
TSP 3.4.1 Examine key-management documentation and interview personnel to verify that keys and key components are generated using a random or pseudo-random process described in ISO 9564-1 and ISO 11568-5 that is capable of satisfying the statistical tests of NIST SP 800-22 or equivalent.	**Identify the key management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.4.2 Key generation must take place in a secure cryptographic device (e.g., hardware security module (HSM)) that has achieved PCI approval or FIPS 140-2 Level 3 or higher certification for physical security.		□	□	□	□
TSP 3.4.2 Examine key-management documentation and interview personnel to verify that • Key generation takes place in an secure cryptographic device (e.g., HSM)), • The HSM has achieved PCI approval or FIPS 140-2 Level 3 certification for physical security	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.4.3 During key-generation operation, the HSM must utilize a secure algorithm that complies with Annex A of this document.		□	□	□	□
TSP 3.4.3 Examine key-management documentation and interview personnel to verify that during key-generation the HSM utilizes a secure algorithm that complies with Annex A of this document.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.4.4 Cables must be inspected prior to key-management activity to ensure disclosure of a clear-text key or key component or share is not possible.		□	□	□	□

TSP 3. Protect and manage cryptographic keys					
		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.4.4 Examine key-management documentation and observe personnel performing inspection of cables to verify that procedures are in place to inspect cables prior to key-management activity, to ensure disclosure of a clear-text key or key component is not possible.	**Identify the key management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how personnel inspect cables prior to key-management activity, to ensure disclosure of a clear-text key or key component is not possible.				
	<Report Findings Here>				
TSP 3.4.5 Use the principles of split knowledge and dual control during the generation of any cryptographic keys in component or share form.		□	□	□	□
TSP 3.4.5 Examine key-management documentation and interview personnel to verify that split knowledge and dual control is required during the generation of any cryptographic keys in component or share form.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.4.6 Key components, if printed, must be created in such a way that the key component cannot be observed during the process by anyone other than the authorized key custodian. Additionally, the key components cannot be observed on final documents without evidence of tampering.		□	□	□	□
TSP 3.4.6 Examine key-management documentation and interview personnel to verify that any printed key components • Are created in such a way that they cannot be observed in the creation process by anyone other than the authorized key custodian, and • Cannot be observed on final documents without evidence of tampering.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.4.7 Immediately destroy any residue from the printing or generation process that might disclose a component so that an unauthorized person cannot obtain it.		□	□	□	□
TSP 3.4.7 Examine key-management documentation and interview personnel to verify that any residue from the printing or generation process is immediately destroyed.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.4.8 Ensure that a generated key is not at any time observable or otherwise accessible in clear-text to any person during the generation process.		□	□	□	□
TSP 3.4.8 Examine key-management documentation and interview personnel to verify that any generation of keys is not observable or otherwise accessible in clear-text to any other person during the generation process.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.4.9 Key components or shares must be placed in pre-serialized, tamper-evident envelopes when not in use by the authorized key custodian.		□	□	□	□
TSP 3.4.9.a Examine key-management documentation and interview personnel to verify that key components or shares are placed in pre-serialized, tamper-evident envelopes when not in use by the authorized key custodian.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.4.9.b Observe locations of key components or shares not in use by the authorized key custodian to verify they are contained in pre-serialized, tamper-evident envelopes.	**Describe how** key components or shares not in use by the authorized key custodian are contained in pre-serialized, tamper-evident envelopes.				
	<Report Findings Here>				
TSP 3.4.10 Generation of asymmetric keys must meet the following conditions: • The generation of asymmetric key pairs must ensure the secrecy of the private key and the integrity of the public key. • Creation and management of asymmetric keys must be in compliance with the payment system requirements for obtaining the issuer certificate.		□	□	□	□

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 3.4.10 Examine key-management documentation and interview personnel to verify: • The generation of asymmetric key pairs ensures the secrecy of the private key and the integrity of the public key. • Their creation and management are in compliance with the payment system requirements for obtaining the issuer certificate.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.5 Key Distribution					
TSP 3.5.1 Keys must be distributed only in their allowable forms.		□	□	□	□
TSP 3.5.1 Examine key-management documentation and interview personnel to verify that keys are distributed only in their allowable forms in accordance with TSP 3.3.2.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.5.2 When transmitted electronically, keys and key components or shares must be encrypted prior to transmission following all key-management requirements.		□	□	□	□
TSP 3.5.2 Examine key-management documentation and interview personnel to verify that keys and key components or shares are encrypted prior to electronic transmission.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.5.3 Ensure that private or secret key components or shares and keying data that are sent as clear-text meet the following requirements: i. Use different communication channels such as different courier services. It is not sufficient to send key components or shares for a specific key on different days using the same communication channel. ii. A two-part form that identifies the sender and the materials sent must accompany the keying data. iii. The form must be signed by the sender and require that the recipient return one part of the form to the originator. iv. Key components or shares must be placed in pre-serialized, tamper-evident envelopes for shipment.		□	□	□	□
TSP 3.5.3.a Examine key-management documentation and interview personnel to verify that any private or secret key components or shares and keying data sent as clear-text: • Use different communication channels such as different courier services and not the same courier in different days, • Are accompanied by a two-part form that identifies the sender and the materials sent, and is signed by the sender, • Are accompanied by instructions for the form to be signed by the recipient and to return one part of the form to the sender, and • Are placed in pre-serialized, tamper-evident packaging.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.5.3.b Obtain a sample of packages received by the TSP containing private or secret key components or shares and keying data and verify that they meet the conditions in 3.5.3.a above or are rejected.	**Identify the sample of** packages examined for this testing procedure.	*<Report Findings Here>*			
	For each item in the sample, **describe how** the packages meet the conditions below or are rejected.				
	• Use different communication channels such as different courier services and not the same courier in different days,				
	<Report Findings Here>				
	• Are accompanied by a two-part form that identifies the sender and the materials sent, and is signed by the sender,				
	<Report Findings Here>				

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
	• Are accompanied by instructions for the form to be signed by the recipient and to return one part of the form to the sender, and				
	<Report Findings Here>				
	• Are placed in pre-serialized, tamper-evident packaging.				
	<Report Findings Here>				
TSP 3.5.4 Key components or shares must only be received by the authorized custodian, who must: i. Inspect and ensure that no one has tampered with the shipping package. If there are any signs of tampering, the key must be regarded as compromised and the vendor's key compromise procedures document must be followed. ii. Verify the contents of the package with the attached two-part form. iii. Return one part of the form to the sender of the component or share, acknowledging receipt. iv. Securely store the component or share according to the TSP's key storage policy.		□	□	□	□
TSP 3.5.4.a Examine key-management documentation and interview personnel to verify that the authorized custodian • Is the only personnel that can receive key components or shares, • Inspects the key components or shares for tampering with the shipping package upon receipt, • Documents the key components or shares as compromised if evidence of tampering of the shipping package is detected, • Verifies the contents of the package with the attached two-part form, • Returns one part of the form to the sender of the key component or share to acknowledge receipt, and • Securely stores the key component or share in accordance with the TSP's key storage policy.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.5.4.b Observe the authorized custodian perform the items in 3.5.4.a above to verify all steps are followed.	**Describe how** all steps below are followed:				
	• Is the only personnel that can receive key components or shares,	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
	- Inspects the key components or shares for tampering with the shipping package upon receipt,	*<Report Findings Here>*			
	- Documents the key components or shares as compromised if evidence of tampering of the shipping package is detected,	*<Report Findings Here>*			
	- Verifies the contents of the package with the attached two-part form,	*<Report Findings Here>*			
	- Returns one part of the form to the sender of the key component or share to acknowledge receipt, and	*<Report Findings Here>*			
	- Securely stores the key component or share in accordance with the TSP's key storage policy.	*<Report Findings Here>*			
TSP 3.5.5 Before the TSP accepts a certificate, they must ensure that they know its origin, and prearranged methods to validate the certificate status must exist and must be used. This includes the valid period of usage and revocation status, if available.		□	□	□	□
TSP 3.5.5.a Examine key-management documentation and interview personnel to verify that a prearranged method to validate certificate status is in place and includes the valid period of usage and revocation status, if available.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.5.5.b Examine key-management documentation and interview personnel to verify that a prearranged method to validate certificate status is in place and includes the valid period of usage and revocation status, if available.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 3.6 Key Loading **Note:** These requirements relate to the loading of keys and clear-text cryptographic key components/shares into HSMs.					
TSP 3.6.1 Any hardware used in the key loading function must be dedicated, controlled, and maintained in a secure environment under dual control.		□	□	□	□
TSP 3.6.1.a Examine key-management documentation and interview personnel to verify that any hardware used in the key loading function is dedicated, controlled, and maintained in a secure environment under dual control.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.6.1.b Observe any hardware used in the key loading function to verify it is dedicated, controlled, and maintained in a secure environment and under dual control.	**Describe how** all hardware used in the key loading function is dedicated, controlled, and maintained in a secure environment and under dual control.				
	<Report Findings Here>				
TSP 3.6.2 Prior to loading keys (or components/shares), the target cryptographic devices, cabling, and paper components must be inspected for any signs of tampering that might disclose the value of the transferred key (or components/shares).		□	□	□	□
TSP 3.6.2.a Examine key-management documentation and interview personnel to verify that the target cryptographic devices, cabling and its paper components are inspected for any signs of tampering prior to key loading.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.6.2.b Observe personnel performing physical inspections of the target cryptographic devices, cabling and its paper components to verify processes are followed to detect signs of tampering prior to key loading.	**Describe how** processes are followed to detect signs of tampering prior to key loading.				
	<Report Findings Here>				
TSP 3.6.3 Any physical media (e.g., an integrated circuit card or dongle), programmable read-only memory (PROM), physical keys, and other key/key component/key share-holding mechanisms used for loading keys, key components, or shares must only be in the physical possession of the designated custodian (or their back-up), and only for the minimum practical time.		□	□	□	□

TSP 3. Protect and manage cryptographic keys					
		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.6.3 Examine key-management documentation and interview personnel to verify that all key/key component/key share-holding mechanisms used for loading keys, key components, or shares are: • In the physical possession of the designated custodian or their back-up, and • Only for the minimum practical time.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.6.4 In relation to key transfer devices: i. Any device used to transfer keys between the cryptographic device that generated the key(s) and the cryptographic devices that will use those key(s), must itself be a secure cryptographic device. ii. After loading a key or key components into the target device, the key transfer device must not retain any residual information that might disclose the value of the transferred keying material.		□	□	□	□
TSP 3.6.4 Examine key-management documentation and interview personnel to verify that: • Any key transfer devices used to transfer keys between the cryptographic device that generated the key(s) and the cryptographic device that will use those key(s) are secure cryptographic devices, and • Key transfer devices do not retain any residual information that might disclose the value of the transferred keying materials after they have loaded a key or key components to any target device.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.6.5 All key loading activities must be under the control of the Key Manager.		□	□	□	□
TSP 3.6.5.a Examine key-management documentation and interview personnel to verify that all key loading activities are performed under the control of the Key Manager.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how all key loading activities are under control of the Key Manager.				

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 3.6.5.b Observe key loading activities to verify that all such activities are under control of the Key Manager.	*<Report Findings Here>*				
TSP 3.6.6 Any physical media (e.g., an integrated circuit card or dongle), programmable read-only memory (PROM), physical keys, and other key/key component/key share-holding mechanisms used in loading keys in a secure environment must be managed under dual control.		□	□	□	□
TSP 3.6.6.a Examine key-management documentation and interview personnel to verify that all key/key component/key share-holding device used for key loading are managed under dual control.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.6.6.b Observe personnel performing key loading to verify that all key/key component/key share-holding mechanisms are handled under dual control.	**Describe how** all key/key component/key share-holding mechanisms are handled under dual control.				
	<Report Findings Here>				
TSP 3.6.7 Make certain that the key-loading process does not disclose any portion of a key component/share to an unauthorized individual.		□	□	□	□
TSP 3.6.7 Examine key-management documentation and interview personnel to verify that the key-loading process does not disclose any portion of a key component/share to an unauthorized individual.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.6.8 If the key component/share is in human-readable form, ensure that it is only visible at one point in time to the key custodian and only for the duration of time required to load the key.		□	□	□	□
TSP 3.6.8 Examine key-management documentation and interview personnel to verify that any key component/share that is human-readable is only visible • At one point in time to the key custodian, and • For the duration of time required to load the key.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys

		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.6.9 In the loading of keys or key components/shares, incorporate a validation mechanism to ensure the authenticity of the keys and ascertain that they have not been tampered with, substituted, or compromised. If check values for key and key components are used for this purpose, they must not be the full length of the key or its components. Validation must be performed under dual control. The outcome of the process (success or otherwise) must be reported to the Key Manager.		□	□	□	□
TSP 3.6.9.a Examine key-management documentation and interview personnel to verify that for all keys or key components/shares loaded: • A validation mechanism is in place to ensure authenticity of the keys and key components, and provide assurance that the keys and key components have not been tampered with, substituted or compromised, • If check values are used, they are not the full length of the key or key components/shares. • The validation process is performed under dual control, and • The outcome of the validation process is reported to the Key Manager.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.6.9.b Observe personnel performing validation processes to verify that they are conducted under dual control and the outcomes are reported to the Key Manager.	**Describe how** validation processes are conducted under dual control.				
	<Report Findings Here>				
	Describe how the outcomes for validation processes are reported to the Key Manager.				
	<Report Findings Here>				

TSP 3. Protect and manage cryptographic keys					
		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.6.10 Once a key or its components/shares have been loaded and validated as operational, either: i. Securely destroy or delete it from the key-loading materials as defined in TSP 3.11, "Key Destruction"; or ii. Securely store it according to these requirements if preserving the keys or components/shares for future loading.		□	□	□	□
TSP 3.6.10.a Examine key-management documentation and interview personnel to verify that once a key and/or its components/shares have been loaded and validated as operational, the key and/or its components/shares are either: • Securely destroyed or deleted from the key-loading materials, or • If the keys or its components/shares are to be used for future loading, they are securely stored in accordance with requirements in this document.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.6.10.b Observe personnel performing process to verify that either secure destruction or deletion, or secure storage of the key and/or its components/shares is performed.	**Describe how** either activity below is performed once a key and/or its components/shares have been loaded and validated as operational, the key and/or its components/shares are either:				
	• Securely destroyed or deleted, **or**	*<Report Findings Here>*			
	• If the keys or its components/shares are to be used for future loading, they are securely stored in accordance with requirements in this document.	*<Report Findings Here>*			
TSP 3.7 Key Component Storage **Note:** These requirements relate to the secure storage of clear-text key components or shares.					
TSP 3.7.1 Key components/shares must be stored in pre-serialized, tamper-evident envelopes in separate, secure locations (such as safes). These envelopes must not be removable without detection.		□	□	□	□
TSP 3.7.1.a Examine key-management documentation and interview personnel to verify:	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
• Key components/shares are stored in pre-serialized, tamper-evident envelopes, and • The envelopes are stored in secure locations (such as safes), and • Removal of the envelopes from their secure location is detectable.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.7.1.b Observe the envelopes used to verify that they are pre-serialized and tamper-evident.	**Describe how** the envelopes are:				
	• Pre-serialized	*<Report Findings Here>*			
	• Tamper-evident	*<Report Findings Here>*			
TSP 3.7.1.c Observe storage locations to verify the envelopes are stored in separate, secure locations and cannot be removed without detection.	**Describe how** the envelopes are stored in separate, secure locations and cannot be removed without detection.				
	<Report Findings Here>				
TSP 3.7.2 An inventory of the contents of key storage safes must be maintained and audited at least quarterly.		□	□	□	□
TSP 3.7.2.a Examine key-management documentation and interview personnel to verify that • An inventory of the contents of key storage safes is maintained, and • The inventory is audited at least quarterly.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.7.2.b Examine inventory and audit documentation to verify inventory is complete and audits are performed at least quarterly.	**Identify the inventory documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the audit documentation examined for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.7.3 Where a secret or private key component/share is stored on a physical media (e.g., an integrated circuit card or dongle) and an access code (e.g., a personal identification number (PIN)) or similar access-control mechanism is used to access that media, only the key custodian (or designated back-up) for the key component/share stored on the media must be allowed possession of both the media and its corresponding access code.		□	□	□	□
TSP 3.7.3 Where a secret or private key component/share is stored on a physical media, examine key-management documentation and interview personnel to verify that the key custodian (or designated back-up) is the only person allowed possession of both the media and its corresponding access code.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.7.4 Access logs to key component/share storage must include: • Date and time (in/out) • Names and signatures of the key custodians involved • Purpose of access • Serial number of envelope (in/out)		□	□	□	□
TSP 3.7.4.a Examine key-management documentation and interview personnel to verify that access logs are maintained.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.7.4.b Examine access logs to key component/share storage and verify that they contain: • Date and time (in/out) • Names and signatures of the key custodians involved • Purpose of access • Serial number of envelope (in/out)	**Identify the access logs** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how access logs to key components/share storage contain:				
	• Date and time (in/out)				
	<Report Findings Here>				
	• Names and signatures of the key custodians involved				

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
	<Report Findings Here>				
	- Purpose of access				
	<Report Findings Here>				
	- Serial number of envelope (in/out)				
	<Report Findings Here>				
TSP 3.7.5 Access and destruction logs for master keys must be retained for at least six months after all keys protected by those master keys are no longer in circulation.		□	□	□	□
TSP 3.7.5 Examine key-management documentation and interview personnel to verify that logs for access and destruction of master keys are retained for at least six months after all keys protected by those master keys are retired and no longer in circulation.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8 Key Usage					

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 3.8.1 Each key must be used for only one purpose and not shared between payment systems, issuers or cryptographic zones, including but not limited to: • Private keys shall be used only to create digital signatures OR to perform decryption operations. Private keys shall never be used to encrypt data or other keys. • Public keys shall be used only to verify digital signatures OR perform encryption operations. Public keys shall never be used to generate signatures. • Key-encrypting keys must never be used as working keys (session keys) and vice versa.		□	□	□	□
TSP 3.8.1.a Examine key-management documentation (e.g., the cryptographic key inventory) and interview personnel to verify that cryptographic keys: • Are defined for one, specific purpose, and • Are not shared between payment systems, issuers or cryptographic zones	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.1.b Examine key-management documentation and interview personnel to verify that • Private keys are only used to **create** digital signatures OR to perform **de**cryption operations. • Private keys are never used to encrypt data or other keys. • Public keys are only used to **verify** digital signatures OR perform encryption operations. • Public keys are never used to generate signatures. • Key-encrypting keys are never used as working keys (session keys) and vice versa.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.2 Transport keys used to encrypt other keys for conveyance (e.g., KEK, ZCMK) must be unique per established key zone. These keys must only be shared between the two communicating entities and must not be shared with any third organization.		□	□	□	□
	Identify the documented procedures examined for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 3.8.2 Examine documented procedures and interview key custodians and key-management supervisory personnel to verify that transport keys are: • Unique per established key zone • Only shared between the two communicating entities	**Identify the key custodians and key-management supervisory personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.3 The HSM must enforce a separation of keys to prevent keys from being used for purposes other than those for which they were intended.		□	□	□	□
TSP 3.8.3a Examine key-management documentation and interview personnel to verify that cryptographic keys are only used for the one, specific purpose for which they were defined.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.3b Observe HSM settings and configurations to verify they enforce a separation of keys.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** HSM settings and configurations enforce a separation of keys.				
	<Report Findings Here>				
TSP 3.8.4 Where an issuer provides a key with a defined expiry date, the TSP must not use the key beyond the issuer-specified expiry date.		□	□	□	□
TSP 3.8.4a Examine documented key-management policies and procedures and interview personnel to verify that issuer-provided keys with a defined expiry date are not used after the issuer-specified expiry date.	**Identify the key-management policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.4b Observe issuer keys currently in use to verify they are within the issuer-specified expiry date.	**Describe how** the issuer keys currently in use are within the issuer specified expiry date.				
	<Report Findings Here>				

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.8.5 All other keys generated by or on behalf of the TSP (not Issuer-provided keys) must have a defined cryptoperiod and be used only for the designated cryptoperiod of that key. If there is a defined need to extend the life of a key beyond its designated life span, there must be a formal risk assessment and sign off by the CISO (or equivalent) prior to the extension. The duration of the extension must be clearly defined and documented in the key inventory.		□	□	□	□
TSP 3.8.5a Examine documented key-management policies and procedures and interview personnel to verify: • All TSP keys have a defined cryptoperiod based on a formal risk assessment and industry guidance • Keys are not used beyond their defined cryptoperiod. • Key cryptoperiods are not extended without a formal risk assessment and sign off by CISO (or equivalent) prior to the extension, with the duration of the extension documented in the key inventory.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.5.b Observe keys currently in use to verify they have not exceeded their defined cryptoperiod.	**Describe how** the keys currently in use have not exceeded their defined cryptoperiod.				
	<Report Findings Here>				

TSP 3. Protect and manage cryptographic keys					
		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.8.6 Production keys must be separated from other keys as follows: i. Prohibit any keys from being shared or substituted between production and test systems. ii. Prohibit keys used for pilots (i.e., limited production—for example, via time, capabilities or volume) from being used for full product rollout unless the keys were managed to the same level of security compliance as required for production. iii. Ensure that any keys used for prototyping (i.e., using cards for proof of concept or process where production keys are not used) are not used in production.		□	□	□	□
TSP 3.8.6.a Examine key-management documentation and interview personnel to verify: • Cryptographic keys are never shared or substituted between production and test/development systems. • Keys used for pilots are not used for full product rollout unless the keys were managed to the same level of security compliance as required for production. • Keys used for prototyping are not used in production.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.6.b Observe processes for generating and loading keys into production systems to verify they have no association with test or development keys.	**Describe** test or development keys have no association with processes for generating and loading keys into production systems.				
	<Report Findings Here>				
TSP 3.8.6.c Observe processes for generating and loading keys into test systems to verify they have no association with production keys.	**Describe how** production keys have no association with generating and loading keys into test systems.				
	<Report Findings Here>				
TSP 3.8.6.d Compare check, hash, cryptogram, or fingerprint values for production and test keys against higher-level keys (MFKs, KEKs shared with other network nodes, and BDKs) to verify that production keys have different values from test keys.	**Describe how** production keys have different values from test keys.				
	<Report Findings Here>				
TSP 3.8.7 The life of key-encrypting keys (KEKs) must be shorter than the time required to conduct an exhaustive search of the key space. Only algorithms and key lengths stipulated in Normative Annex A of this document shall be allowed.		□	□	□	□

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.8.7.a Examine documented procedures and interview personal to verify procedures require that the life of key-encrypting keys (KEKs) is shorter than the time required to conduct an exhaustive search of the key space.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.7.b Observe key-encrypting keys to verify they have a life shorter than the time required to conduct an exhaustive search of the key space.	**Describe how** key encrypting keys have a life shorter than the time required to conduct an exhaustive search of the key space.				
	<Report Findings Here>				
TSP 3.8.7.c Examine documented procedures and interview personal to verify procedures require that only the algorithms and key lengths stipulated in Normative Annex A of this document are used.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.7.d Observe key-encrypting keys to verify that only algorithms and key lengths stipulated in Normative Annex A of this document are used.	**Describe how** only algorithms and key lengths stipulated in Normative Annex A of this document are used for key-encrypting keys.				
	<Report Findings Here>				
TSP 3.8.8 Ensure that private and secret keys exist in the minimum number of locations consistent with effective system operation.		□	□	□	□
TSP 3.8.8 Examine documented procedures to verify that private and secret keys only exist in the minimum number of locations consistent with effective system operation.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.9 Key variants must not be used except within the device with the original key.		□	□	□	□
TSP 3.8.9.a Examine documented procedures for generating all types of keys and verify the procedures ensure that only unique keys, or sets of keys, are used, and any key variants exist only within the device with the original key.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.8.9.b Interview personnel and observe key-generation processes to verify that only unique keys or sets of keys are generated for use outside of the original device.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.10 An inventory of keys under TSP management must be maintained to determine when a key is no longer required, including: • Key label/name • Effective date • Expiration date (if applicable) • Key purpose/type • Key length		□	□	□	□
TSP 3.8.10.a Review documentation of key inventory control and monitoring procedures. Verify all keys are identified and accounted for in the inventory.	**Identify the key inventory control documentation** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the monitoring procedures reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.10.b Review key inventory records to verify the following details are included: • Key label/name • Effective date • Expiration date (if applicable) • Key purpose/type • Key length	**Identify the key inventory records** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.10.c Interview personnel to verify that key-inventory procedures are known and followed.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.11 All derivation keys must be unique per issuer.		□	□	□	□

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 3.8.11 Examine key-management documentation and interview personnel to verify that all derivation keys are unique per issuer.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.8.12 Integrated Chip (IC) keys must be unique per IC.		□	□	□	□
TSP 3.8.12 Examine key-management documentation and interview personnel to verify that all IC keys are unique per IC.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.9 Key Back-up/Recovery **Note:** It is not a requirement to have back-up copies of key components, shares, or keys. However, if back-up copies are used, these requirements must be met.					
TSP 3.9.1 Ensure that key back-up and recovery are part of the business recovery/resumption plans of the organization.		□	□	□	□
TSP 3.9.1 Examine documented procedures and interview personal to verify that key back-up and recovery are part of the business recovery/resumption plans of the organization.	**Identify the key-management documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.9.2 Require a minimum of two authorized individuals to enable the recovery of keys.		□	□	□	□
TSP 3.9.2.a Review documented recovery procedures to verify that recovery of keys requires dual control.	**Identify the documented recovery procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.9.2.b Interview appropriate personnel.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 3.9.3 All relevant policies and procedures that apply to production keys must also apply to back-up keys.		□	□	□	□
TSP 3.9.3 Interview personnel and examine documented procedures and back-up records to determine whether any back-up copies of keys or their components exist. Perform the following: • Observe back-up processes to verify back-up copies of secret and/or private keys are maintained in accordance with the same requirements as are followed for the production keys. • Verify through examination of documented procedures and interviews of personnel that back-ups 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	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the back-up records examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.9.4 The loading of back-up keys into a failed device must be prohibited until the reason for that failure has been ascertained and the problem has been corrected.		□	□	□	□
TSP 3.9.4 Examine documented procedures and interview personal to verify the procedures ensure that the loading of back-up keys into failed devices is not permitted until after the reason for that failure has been ascertained and the problem has been corrected.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.9.5 The back-up of keys must conform to the organization's Information Security Policy.		□	□	□	□
TSP 3.9.5 Examine documented procedures and interview personal to verify that the back-up of keys conforms to the organization's Information Security Policy.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.9.6 All access to back-up storage locations must be witnessed and logged under dual control.		□	□	□	□

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.9.6 Examine documented procedures and interview personal to verify: • All back-up storage locations can only be accessed and used under dual control. • Access to all back-up storage locations is witnessed and logged under dual-control.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.10 Key Destruction **Note:** These requirements relate to the destruction of keys, components, and shares.					
TSP 3.10.1 Immediately destroy key components/shares that are no longer required after successful loading and validation as operational.		□	□	□	□
TSP 33.10.1.a Examine documented procedures and interview personnel to verify processes are in place for destroying keys and their components/shares after successful loading and validation.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.10.1.b Examine key-history logs and key-destruction logs to verify that all key components/shares have been destroyed immediately upon completion of loading.	**Identify the key-history logs** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the key-destruction logs examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.10.1.c Review storage locations for key components/shares that have been loaded to verify they are no longer present.	**Describe how** key components/shares that have been loaded are no longer present. *<Report Findings Here>*				
TSP 3.10.2 When a cryptographic device (e.g., HSM) is decommissioned, any data stored and any resident cryptographic keys must be deleted or otherwise destroyed.		□	□	□	□
TSP 3.10.2.a Interview personnel and observe demonstration of processes for removing HSMs from service to verify that all	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
keying material is rendered irrecoverable (for example, zeroized), or that devices are physically destroyed under dual-control to prevent the disclosure of any sensitive data or keys.	**Describe how** all keying material is rendered irrecoverable (for example, zeroized), or that devices are physically destroyed under dual-control to prevent the disclosure of any sensitive data or keys.				
	<Report Findings Here>				
TSP 3.10.2.b Interview personnel and observe processes for removing HSMs from service to verify that tests and inspections of devices are performed to confirm that keys have been rendered irrecoverable or the devices are physically destroyed.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how tests and inspections of devices are performed to confirm that keys have been rendered irrecoverable or the devices are physically destroyed.				
	<Report Findings Here>				
TSP 3.10.3 Securely destroy all copies of keys that are no longer required.		□	□	□	□
TSP 3.10.3.a Examine documented procedures and interview personnel to verify processes are in place for destroying all copies (including back-ups) of keys that are no longer required.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.10.3.b Examine key-history logs and key-destruction logs to verify that all copies of keys have been destroyed once the key is no longer required.	**Identify the key-history logs** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the key-destruction logs examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.10.4 All key destruction must be logged and the log retained for verification.		□	□	□	□
TSP 3.10.4 Examine system configurations and audit trails to verify that all key destruction operations are logged.	**Identify the audit trails** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how audit trails show that all key destruction operations are logged.				
	<Report Findings Here>				

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
	Identify the system component(s) examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** system configurations confirm that all key destruction operations are logged.				
	<Report Findings Here>				
TSP 3.10.5 Destroy keys and key components/shares so that it is impossible to recover them by physical or electronic means.		□	□	□	□
TSP 3.10.5.a Examine documented procedures for destroying keys and key components/shares and confirm they are sufficient to ensure that no part of the key or component can be recovered.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.10.5.b Observe key-destruction processes to verify that no part of the key or component can be recovered.	**Describe how** no part of the key or component can be recovered.				
	<Report Findings Here>				
TSP 3.10.6 If a key that resides inside a HSM cannot be destroyed, the device itself must be destroyed in a manner that ensures it is irrecoverable.		□	□	□	□
TSP 3.10.6 Review documented procedures for removing HSMs from service and interview personnel to verify if any key within the HSM cannot be destroyed, the device itself is destroyed in a manner that ensures it is irrecoverable.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.10.7 Destroy all hard-copy key components/shares maintained on paper by cross-shredding, pulping, or burning. Strip shredding is not sufficient.		□	□	□	□
TSP 3.10.7.a Review documented procedures and interview personnel to verify all hard-copy key components/shares maintained on paper are destroyed by cross-shredding, pulping, or burning.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the documented procedures reviewed for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 3.10.7.b Review documented procedures and interview personnel to verify that strip shredding is not used to destroy hard-copy key components/shares.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.10.8 Electronically-stored keys must either be overwritten with random data a minimum of three times or destroyed by smashing so they cannot be reassembled.		□	□	□	□
TSP 3.10.8 Review documented procedures and interview personnel to verify that keys stored on electronic media are: • Overwritten with random data a minimum of three times, *and/or* • Destroyed by smashing so they cannot be reassembled.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.10.9 Destroy all key components under dual control with appropriate key-destruction affidavits signed by the applicable key custodian.		□	□	□	□
TSP 3.10.9.a Review documented procedures for destroying keys to verify that dual control is implemented for all key-destruction processes.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.10.9.b Interview personnel and observe demonstration of processes for removing keys from service to verify that dual control is implemented.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how dual control is implemented.				
	<Report Findings Here>				
TSP 3.10.9.c Inspect key-destruction logs and verify that the key-custodian signs an affidavit as a witness to the key destruction process.	**Identify the key-destruction logs** inspected for this testing procedure.	*<Report Findings Here>*			
TSP 3.10.10 A person who is not a key custodian for any part of that key must witness the destruction and also sign the key-destruction affidavits, which are kept indefinitely.		□	□	□	□
TSP 3.10.10.a Observe the key-destruction process and verify that it is witnessed by a person who is not a key custodian for any component of that key.	**Describe how** the key destruction process is witnessed by a person who is not a key custodian for any component of that key.				
	<Report Findings Here>				

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 3.10.10.b Inspect key-destruction logs and verify that a witness who is not a key custodian for any component of the key signs an affidavit as a witness to the key destruction process.	**Identify the key-destruction logs** inspected for this testing procedure.	*<Report Findings Here>*			
TSP 3.11 Key-Management Audit Trail					
TSP 3.11.1 Key-management logs must contain, at a minimum, for each recorded activity: • The date and time of the activity took place • The action taken (e.g., key generation, key distribution, key destruction) • Name and signature of the person performing the action (may be more than one name and signature if split responsibility is involved) • Countersignature of the Key Manager or CISO (or equivalent)		□	□	□	□
TSP 3.11.1 Review key-management logs to verify the following is recorded for each activity: • The date and time of the activity took place • The action taken (e.g., key generation, key distribution, key destruction) • Name and signature of the person performing the action (may be more than one name and signature if split responsibility is involved) • Countersignature of the Key Manager or CISO (or equivalent)	**Identify the key-management logs** reviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how the following is recorded in the key-management logs reviewed for each activity:				
	• The date and time of the activity took place	*<Report Findings Here>*			
	• The action taken (e.g., key generation, key distribution, key destruction)	*<Report Findings Here>*			
	• Name and signature of the person performing the action (may be more than one name and signature if split responsibility is involved)	*<Report Findings Here>*			
	• Countersignature of the Key Manager or CISO (or equivalent)	*<Report Findings Here>*			
TSP 3.11.2 Key-management logs must be retained for at least the life span of the key(s) to which they relate.		□	□	□	□
TSP 3.11.2.a Review documented procedures and interview personnel to verify procedures require key-management logs	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
must be retained for the life span of the key(s) to which they relate.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.11.2.b Examine key-management logs for different types of keys and verify logs are retained for the life span of the key(s) to which they relate.	**Identify the key-management logs** examined for this testing procedure.	*<Report Findings Here>*			
TSP 3.11.3 The TSP must prohibit access to key-management logs by any personnel outside of the Key Manager or authorized individuals.		□	□	□	□
TSP 3.11.3.a Review documented procedures and interview personnel to ensure access to key-management logs is only permitted for the Key Manager or authorized individuals.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.11.3.b Verify through observation that access to key-management logs is only permitted to authorized individuals.	**Describe how** access to key-management logs is only permitted to authorized individuals.				
	<Report Findings Here>				
TSP 3.11.4 Access to any capability to reset the sequence number generator in the HSM must be restricted.		□	□	□	□
TSP 3.11.4.a Review documented procedures and interview personnel to ensure procedures restrict access to any capability to reset the sequence number generator in the HSM.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.11.4.b Verify through access control list review or other processes that only authorized personnel have access to the sequence number generator.	**Describe how** access control list review or other processes confirm that only authorized personnel have access to the sequence number generator.				
	<Report Findings Here>				
TSP 3.11.5 The CISO (or equivalent) or an authorized individual must investigate all audit log validation failures.		□	□	□	□
	Identify the documented procedures reviewed for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.11.5 Review documented procedures and interview personnel to verify the CISO (or equivalent) investigates all audit log validation failures.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.11.6 The unauthorized deletion of any audit trail must be prevented		□	□	□	□
TSP 3.11.6.a Review documented procedures to verify controls are defined for protecting audit trails from unauthorized deletion.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.11.6.b Examine system configurations to verify controls are implemented to prevent unauthorized deletion of audit trails.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** controls are implemented in the system configurations to prevent unauthorized deletion of audit trails.				
	<Report Findings Here>				
TSP 3.12 Key Compromise **Note:** These requirements relate to procedures for dealing with any known or suspected key compromise. Unless otherwise stated, the following applies to TSP-owned keys.					
TSP 3.12.1 The TSP must define procedures that include the following: • Who is to be notified in the event of a key compromise. At a minimum, this must include the CISO or equivalent, Key Manager, and Security Manager. • The actions to be taken to protect and/or recover system software and/or hardware, symmetric and asymmetric keys, previously generated signatures, and encrypted data. • An investigation into the cause of the compromise, including a documented analysis of how and why the event occurred and the damages suffered. • The removal from operational use of all compromised keys within a predefined time frame and a means of migrating to new key(s). • Where keys are issuer-owned, the issuer must be notified immediately for further instruction.		□	□	□	□

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 3.12.1.a Review documented procedures for key compromise and verify they include: • Identification of individuals to be notified, including the CISO (or equivalent), Key Manager and Security Manager. • Identify the minimum actions to be taken to protect and/or recover system software and/or hardware, symmetric and asymmetric keys, previously generated signatures, and encrypted data. • Requirement for an investigation to be performed to identify the cause of the compromise, including an analysis of how/why the event occurred and identification of damages suffered. • Time frame within which all compromised keys must be removed from operational use. • Methods for migrating to new keys. • Where applicable, immediately notifying the issuer about compromised keys.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.12.1.b Verify through interviews that applicable personnel are aware of procedures to be followed in the event of a key compromise.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.12.2 A replacement key must not be a variant of the compromised key.		□	□	□	□
TSP 3.12.2 Review documented procedures to ensure replacement keys are not created from a variant of the compromise key.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.12.3 Where a key compromise is suspected but not yet proven, the Key Manager must have the ability to activate emergency key replacement procedures.		□	□	□	□
TSP 3.12.3.a Review documented procedures to verify the Key Manager has authority to activate emergency key replacement procedures.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.12.3.b Interview Key Manager to verify he/she is aware of their responsibility and understand the procedures to activate emergency key replacement procedures.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.12.4 In the event of known or suspected key compromise, all instances of the key must be immediately revoked pending the outcome of the investigation. Known compromised keys must be replaced.		□	□	□	□
TSP 3.12.4.a Review documented procedures to verify they require that all instances of a key suspected of being compromised must be immediately revoked pending the outcome of the investigation.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.12.4.b Verify through interviews that procedures are understood and communicated to affected personnel.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.12.5 All keys that are encrypted with a key that has been revoked must also be revoked.		□	□	□	□
TSP 3.12.5 Review documented procedures to verify that all keys encrypted with a key that has been revoked are also revoked.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.12.6 In the event that a KEK has been compromised, all keys encrypted with the KEK must be replaced.		□	□	□	□
TSP 3.12.6 Review documented procedures to verify that if a KEK is compromised, the KEK and all keys encrypted with that KEK are replaced.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.12.7 In the event that a MDK has been compromised, all keys derived from that master key must be replaced.		□	□	□	□
TSP 3.12.7 Review documented procedures to verify that if a MDK is compromised, the MDK and all and and all keys derived from that MDK are replaced.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.12.8 The CISO or equivalent must be notified within 24 hours of a known or suspected compromise.		□	□	□	□
TSP 3.12.8 Review documented procedures to verify steps include notification of the CISO or equivalent within 24 hours of a known or suspected compromise.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.12.9 Data items that have been signed using a key that has been revoked (e.g., a public-key certificate) must be withdrawn as soon as practically possible and replaced once a new key is in place.		□	□	□	□
TSP 3.12.9 Review documented procedures and interview personnel to verify data items that have been signed with a key	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
that has been revoked are withdrawn as soon as possible and replaced.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.13 Key-Management Security Hardware					
TSP 3.13.1 When in its normal operational state: • All of the HSM's tamper-detection mechanisms must be activated. • All physical keys must be removed. • All unnecessary externally attached devices must be removed (such as an operator terminal).		□	□	□	□
TSP 3.13.1.a Review documented procedures and interview personnel to verify the following is required whenever the HSM is in its normal operational state: • All of the HSM's tamper-resistant mechanisms must be activated. • All physical keys must be removed. • All unnecessary externally attached devices must be removed (such as an operator terminal).	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.13.1.b Observe HSMs in normal operational state to verify they are configured according to the documented procedures, and that: • All of the HSM's tamper-resistant mechanisms are activated. • All physical keys are removed. • All unnecessary externally attached devices are removed (such as an operator terminal).	**Identify the HSM(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each device, **describe how** the HSMs in normal operational state are configured according to the documented procedures, and that:				
	• All of the HSM's tamper-resistant mechanisms are activated.	*<Report Findings Here>*			
	• All physical keys are removed.	*<Report Findings Here>*			
	• All unnecessary externally attached devices are removed (such as an operator terminal).	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys

		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.13.2 HSMs must be brought into service only if there is assurance that the equipment has not been subject to unauthorized modification, substitution, or tampering. This requires physical protection of the device up to the point of key insertion or inspection.		□	□	□	□
TSP 3.13.2.a Review documented procedures to verify that HSMs are not brought into service unless there is assurance that the HSM has not been substituted or subjected to unauthorized modifications or tampering.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.13.2.b Observe processes and interview personnel to verify that HSMs are physically protected up to the point of key insertion or inspection, to provide assurance that the HSM has not been substituted or subjected to unauthorized modifications or tampering.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how HSMs are physically protected up to the point of key insertion or inspection, to provide assurance that the HSM has not been substituted or subjected to unauthorized modifications or tampering.				
	<Report Findings Here>				
TSP 3.13.3 The process for the installation and commissioning of the HSM must be documented and logged. Logs must be retained for a minimum of six months after the life of the HSM and any keys generated or protected by the HSM.		□	□	□	□
TSP 3.13.3.a Review documented procedures and interview personnel to verify: • Processes for installation and commissioning of HSMs must be documented and logged. • Logs must be retained for at least six months after the life of the HSM and keys generated or protected by the HSM.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.13.3.b Observe processes and examine logs for HSM installation to verify: • Processes for installation and commissioning of HSMs are documented and logged • Logs are retained for at least six months after the life of the HSM and any keys generated or protected by the HSM	**Identify the logs for HSM installation** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how:				
	• Processes for installation and commissioning of HSMs are documented and logged	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
	• Logs are retained for at least six months after the life of HSM and any keys generated or protected by the HSM	*<Report Findings Here>*			
TSP 3.13.4 When a HSM is removed from service permanently or for repair, all operational keys must be deleted from the device prior to its removal.		□	□	□	□
TSP 3.13.4.a Review documented procedures for removing HSMs from service and interview personnel to verify that all operational keys are deleted from the device (for example, zeroized) prior to its removal from service.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.13.4.b Observe demonstration of processes for removing HSMs from service to verify all operational keys are deleted from the device.	**Describe how** all operational keys are deleted from the device.				
	<Report Findings Here>				
TSP 3.13.5 The removal process for the repair or decommissioning of the HSM must be documented and logged. Logs must be retained for a minimum of six months after the life of the HSM and any keys generated or protected by the HSM.		□	□	□	□
TSP 3.13.5.a Review documented procedures and interview personnel to verify: • Processes for removal of an HSM for repair or decommissioning must be documented and logged. • Logs must be retained for at least six months after the life of the HSM and keys generated or protected by the HSM.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 3.13.5.b Observe processes and examine logs for HSM removal to verify: • Processes for removal of an HSM for repair or decommissioning are documented and logged. • Logs are retained for at least six months after the life of HSM and any keys generated or protected by the HSM.	**Identify the logs for HSM removal** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how:				
	• Processes for removal of an HSM for repair or decommissioning are documented and logged.	*<Report Findings Here>*			
	• Logs are retained for at least six months after the life of the HSM and any keys generated or protected by the HSM.	*<Report Findings Here>*			

TSP 3. Protect and manage cryptographic keys					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 3.13.6 The HSM must be under physical dual control at all times it is accessed or is in any privileged mode.		□	□	□	□
TSP 3.13.6 Review documented procedures and interview personnel to verify that HSMs must be under physical dual control at all times when accessed or when in any privileged mode.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 4. Restrict access to TDE by business need to know

The requirements in this section build on PCI DSS Requirement 7.

TSP 4. Restrict access to TDE by business need to know					
		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 4.1 Control and Manage Logical Access to TDE					
TSP 4.1.1 Access to clear-text cardholder data, Payment Tokens, and Payment Token Data in the TDE must be restricted to only those with a legitimate business reason to access the data.		□	□	□	□
TSP 4.1.1.a Interview personnel and examine documentation (i.e., data flow diagrams, system configurations), to identify where clear-text cardholder data, Payment Tokens and Payment Token Data resides in the TDE.	**Identify the documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 4.1.1.b Interview responsible personnel and examine documentation to verify that job functions/roles with a legitimate business reason to access this data are identified.	**Identify the documented** procedures reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 4.1.1.c Review access control lists protecting the identified resources and verify that only personnel/roles with a legitimate business reason have access to the data and privileges are assigned appropriately.	**Identify the access control lists** reviewed for this testing procedure.	*<Report Findings Here>*			
	Provide the name of the assessor who attests that only personnel/roles with a legitimate business reason have access to the data and privileges are assigned appropriately	*<Report Findings Here>*			

TSP 4. Restrict access to TDE by business need to know

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 4.1.2 Review user accounts and access privileges to in-scope system components at least every six months to ensure user accounts and access remain both authorized and appropriate based on job function.		□	□	□	□
TSP 4.1.2 Interview responsible personnel and examine supporting documentation to verify: • User accounts and access privileges are reviewed at least every six months. • Reviews confirm that access is appropriate based on job function, and that all access is authorized.	**Identify the supporting documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 5. Identify and authenticate all access to TDE systems

The requirements in this section build on PCI DSS Requirement 8.

TSP 5. Identify and authenticate all access to TDE systems					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 5.1 Administrative Access					
TSP 5.1.1 Require multi-factor authentication for all administrative access into and within the TDE. ***Note:*** *Multi-factor authentication only needs to be performed upon initial authentication to a particular system component within the TDE (e.g., multi-factor authentication is not required at both the system- and application-level for that system component).*		☐	☐	☐	☐
TSP 5.1.1.a Interview personnel and examine supporting documentation to verify that multi-factor authentication is required for all administrative access into and within the TDE.	**Identify the supporting documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 5.1.1.b Examine system configurations and observe administrative access to systems in the TDE to verify multi-factor authentication is required for all administrative access.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** system configurations ensure that multi-factor authentication is required for all administrative access to systems in the TDE.				
	<Report Findings Here>				
	Describe how multi-factor authentication is required for all administrative access to systems in the TDE.				
	<Report Findings Here>				

TSP 5. Identify and authenticate all access to TDE systems

Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 5.2 Password Management					
TSP 5.2.1 "First use" passwords must expire if not used within 24 hours of distribution.		□	□	□	□
TSP 5.2.1 Examine password procedures and observe processes to verify that first-time passwords are set to expire if not used within 24 hours.	**Identify the password procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how first time passwords are set to expire if not used within 24 hours.				
	<Report Findings Here>				
TSP 5.2.2 Passwords used to access TDE systems must meet at least the following complexity and strength: • A minimum length of at least seven characters. • Consist of a combination of at least three of the following: – Upper-case letters – Lower-case letters – Numbers – Special characters		□	□	□	□
TSP 5.2.2 Examine system configuration settings to verify that password parameters are set to require at least the following strength/complexity: • A minimum length of at least seven characters. • Consist of a combination of at least three of the following: – Upper-case letters – Lower-case letters – Numbers	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** system configuration settings ensure that password parameters are set to require at least the following strength/complexity:				
	• A minimum length of at least seven characters.				
	<Report Findings Here>				

TSP 5. Identify and authenticate all access to TDE systems

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
– Special characters	• Consist of a combination of at least three of the following: – Upper-case letters – Lower-case letters – Numbers – Special characters				
	<Report Findings Here>				
TSP 5.2.3 Passwords must not be displayed during entry.		□	□	□	□
TSP 5.2.3 Examine authentication procedures for entering a password and verify the password is not displayed as it is entered.	**Describe how** the password is not displayed as it is entered.				
	<Report Findings Here>				
TSP 5.2.4 Passwords must have a maximum life not to exceed 90 days and a minimum life of at least one day.		□	□	□	□
TSP 5.2.4 Examine system configuration settings to verify that user password parameters are set to have a maximum life of not more than 90 days and a minimum life of at least one day.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	For each system component, **describe how** system configuration settings ensure that password parameters are set to have a maximum life of not more than 90 days and a minimum life of at least one day.				
	<Report Findings Here>				
TSP 5.3 Account Locking					
TSP 5.3.1 Locked accounts must only be unlocked: • By an authorized individual (e.g., security administrator), and/or • Using an automated password reset mechanism using challenge questions with answers that only the individual user would know. These questions must be designed such that the answers are not information that is available elsewhere in the organization, such as in the Human Resources department.		□	□	□	□

TSP 5. Identify and authenticate all access to TDE systems

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 5.3.1.a Examine documented procedures to verify that accounts can only be unlocked by either the security administrator or other authorized individual, or via an automated password reset mechanism.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 5.3.1.b If a security administrator can unlock accounts: Interview administrators and observe a demonstration of processes to verify that an account is unlocked only after the identity of the user is verified.	**Indicate whether** a security administrator can unlock accounts. **(yes/no)** *If "no," mark 5.3.1.b as "Not Applicable."*	*<Report Findings Here>*			
	If "yes":				
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how the account is unlocked only after the identity of the user is verified.				
	<Report Findings Here>				
TSP 5.3.1.c If accounts can be unlocked via an automated reset mechanism: Observe the mechanism including the challenge/response criteria, to verify the questions are designed such that answers do not comprise information that is used or available elsewhere in the organization.	**Indicate whether** accounts can be unlocked via an automated reset mechanism. **(yes/no)** *If "no," mark 5.3.1.c as "Not Applicable."*	*<Report Findings Here>*			
	If "yes":				
	Describe the automated mechanism in place.	*<Report Findings Here>*			
	Describe how the questions are designed such that answers do not comprise information that is used or available elsewhere in the organization.				

TSP 5. Identify and authenticate all access to TDE systems

Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
	<Report Findings Here>				

TSP 6. Restrict physical access to the TDE

For TSPs, any physical access to data or systems that house cardholder data, Payment Tokens, and/or Payment Token Data should be strictly controlled and monitored. The requirements in this section build on PCI DSS Requirement 9.

TSP 6. Restrict physical access to the TDE					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 6.1 Physical Perimeter and Facility Security					
TSP 6.1.1 The physical perimeter of the TSP facility must be monitored by closed-circuit television (CCTV) with clear line of sight to all entrances/exits.		□	□	□	□
TSP 6.1.1 Observe CCTV images from the CCTV control room to verify the physical perimeter of the TSP facility is monitored and that CCTV has a clear line of sight to all entrances/ exits.	**Provide the name of the assessor** who attests that the physical perimeter of the TSP facility is monitored and that CCTV has a clear line of sight to all entrances/ exits.	*<Report Findings Here>*			
TSP 6.1.2 The exterior walls, roofs, and floors of facilities that house the TSP must be constructed of solid materials such as reinforced concrete, concrete block, brick, stone, or metal, and situated on a solid foundation.		□	□	□	□
TSP 6.1.2 Verify through observation and documentation that exterior walls, roof, and floors of the TSP facility are constructed of solid materials.	**Identify the documentation** reviewed for this testing procedure.	*<Report Findings Here>*			
	Provide the name of the assessor who attests that exterior walls, roof, and floors of the TSP facility are constructed of solid materials.	*<Report Findings Here>*			
TSP 6.1.3 All external doors to the facility must be kept locked or otherwise controlled at all times, equipped with intrusion detection systems and monitored by CCTV cameras. In a multi-tenant building, all entry/exit points to TSP space must be controlled at all times, equipped with intrusion detection systems and monitored by CCTV cameras.		□	□	□	□

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 6.1.3.a Examine policies and procedures and interview personnel to verify that external doors to the facility must be locked or otherwise controlled at all times.	**Identify the policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 6.1.3.b Observe external doors to the facility (or entry/exit points in a multi-tenant building) to verify doors are locked or otherwise controlled by intrusion detection systems and monitored by CCTV at all times.	**Describe how** external doors to the facility (or entry/exit points in a multi-tenant building) doors are locked or otherwise controlled by intrusion detection systems and monitored by CCTV at all times.				
	<Report Findings Here>				
TSP 6.1.4 In a multi-tenant building, the physical environment where the TDE is housed must be isolated from public access (including other tenants) by floor-to-ceiling, wall-to-wall construction or other controls (e.g., intrusion detection system). Construction must prevent access via raised floors and dropped ceilings.		□	□	□	□
TSP 6.1.4 If the TDE is located in a multi-tenant building: Observe the physical environment where the TDE is housed and verify: • The TDE is isolated from public access and other tenants by floor-to-ceiling, wall-to-wall construction. • The construction prevents access via raised floors and dropped ceilings or controls.	**Indicate whether** the TDE is located in a multi-tenant building. **(yes/no)** *If "no," mark 6.1.4 as "Not Applicable."*	*<Report Findings Here>*			
	If "yes":				
	Describe how:				
	• The TDE is isolated from public access and other tenants by floor-to-ceiling, wall-to-wall construction.				
	<Report Findings Here>				
	• The construction prevents access via raised floors and dropped ceilings or controls.				
	<Report Findings Here>				

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 6.1.5 Emergency exit doors must only be capable of being opened from inside the building or from the entity's floor space in a multi-tenant building. These doors shall not be used for any other purpose. Such doors must: • Be equipped with alarm sensors and contact monitored 24 hours a day. • Be fitted with a local audible alarm that sounds when the door is opened. • Display clearly marked "Emergency Exit" or "Exit" signage.		□	□	□	□
TSP 6.1.5.a Examine policies and procedures and interview personnel to verify emergency exit doors can only be opened from the inside of the building, or from the entity's floor space in multi-tenant building, and are not allowed to be used for any other purpose.	**Identify the policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 6.1.5.b Examine security system configurations and emergency exit doors to verify: • Doors are equipped with alarm sensors and contact monitored 24 hours a day. • Doors are fitted with a local audible alarm that sounds when the door is opened. • Doors display clearly marked "Emergency Exit" or "Exit" signage.	**Provide the name of the assessor** who attests that: • Doors are equipped with alarm sensors and contact monitored 24 hours a day. • Doors are fitted with a local audible alarm that sounds when the door is opened. • Doors display clearly marked "Emergency Exit" or "Exit" signage.	*<Report Findings Here>*			
TSP 6.2 Data Center and TDE Security ***Note:*** *These requirements can be met by applying controls across a number of levels—for example, door entry controls may be applied at room level for each TDE or data center, or at an outer level that must be passed through to access the TDE and data center, or a combination of both. Some controls may also be applied at rack level—for example, where the TDE is in a secured rack in a larger data center. However the requirements are implemented, they must ensure that access to the TDE is controlled and monitored as defined in these requirements.*					
TSP 6.2.1. All access to the TDE must be approved by the Security Manager (see TSP 8).		□	□	□	□
TSP 6.2.1 Examine access control lists for entry to the TDE, and interview Security Manager to verify that all	**Identify the Security Manager** interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
personnel permitted to access the TDE are approved by Security Manager.	**Identify the access control lists** reviewed for this testing procedure.	*<Report Findings Here>*			
	Provide the name of the assessor who attests that all personnel permitted to access the TDE are approved by Security Manager.	*<Report Findings Here>*			
TSP 6.2.2 TSP data centers must be equipped with a positively controlled single entry portal (e.g., mantrap).		□	□	□	□
TSP 6.2.2 Observe all data center entry points to verify that a single entry portal (e.g., mantrap) is installed that: • Requires positive authentication prior to granting entry • Grants entry to a single person for each positive authentication	**Provide the name of the assessor** who attests that a single entry portal (e.g., mantrap) is installed that: • Requires positive authentication prior to granting entry • Grants entry to a single person for each positive authentication	*<Report Findings Here>*			
TSP 6.2.3 CCTV cameras must be located at all entrances and emergency exit points.		□	□	□	□
TSP 6.2.3 Observe all entrances and emergency exit points to verify presence of CCTV cameras.	**Provide the name of the assessor** who attests that CCTV cameras are present at all entrances and emergency exit points.	*<Report Findings Here>*			
TSP 6.2.4 Doors into the TDE must be fitted with an electronic access control system (e.g., card reader, biometric scanner) to control physical access. The access control systems must record all entry and exit activities.		□	□	□	□
TSP 6.2.4.a Observe all entrances into the TDE to verify doors are fitted with an electronic access control system to control physical access.	**Describe how** the doors to all entrances into the TDE are fitted with an electronic access control system to control physical access.				
	<Report Findings Here>				
TSP 6.2.4.b Examine audit logs and/or other access records to verify the access control system records all entry and exit activities.	**Identify the audit logs and/or other access records** examined for this testing procedure.	*<Report Findings Here>*			

<table>
<tr><th colspan="6">*TSP 6. Restrict physical access to the TDE*</th></tr>
<tr><th rowspan="2">Requirements and Testing Procedures</th><th rowspan="2">Reporting Instructions & Assessor's Findings</th><th colspan="4">Summary of Assessment Findings
(check one)</th></tr>
<tr><th>In Place</th><th>In Place w/ CCW</th><th>N/A</th><th>Not in Place</th></tr>
<tr><td rowspan="2"></td><td colspan="5">**Describe how** the access control system records all entry and exit activities in the audit logs and/or other access control records.</td></tr>
<tr><td colspan="5">*<Report Findings Here>*</td></tr>
<tr><td colspan="2">**TSP 6.2.5** Multi-factor authentication is required for entry to the TDE and telecommunications rooms.</td><td>□</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td rowspan="2">**TSP 6.2.5** Examine access controls and observe access events to verify multi-factor authentication is required for entry to:
• The TDE, and
• Telecommunications rooms</td><td>**Identify the multi-factor authentication method** used.</td><td colspan="4">*<Report Findings Here>*</td></tr>
<tr><td>**Provide the name of the assessor who attests that:**
• The TDE, and
• Telecommunications rooms</td><td colspan="4">*<Report Findings Here>*</td></tr>
<tr><td colspan="2">**TSP 6.2.6** All individuals must be individually identified and authenticated before being granted access to the TDE. Entry controls must prevent piggy-backing by granting access to a single person at a time, with each person being identified and authenticated before access is granted.</td><td>□</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td rowspan="3">**TSP 6.2.6** Observe personnel entering the TDE to verify that the implemented mechanisms:
• Require individuals to be individually identified and authenticated before being granted access to the TDE.
• Grant access to a single person at a time, with each person being identified and authenticated before access is granted.</td><td colspan="5">**Describe how** the implemented mechanisms:</td></tr>
<tr><td>• Require individuals to be individually identified and authenticated before being granted access to the TDE.</td><td colspan="4">*<Report Findings Here>*</td></tr>
<tr><td>• Grant access to a single person at a time, with each person being identified and authenticated before access is granted.</td><td colspan="4">*<Report Findings Here>*</td></tr>
<tr><td colspan="2">**TSP 6.2.7** A physical intrusion-detection system that is connected to the alarm system must be in place for the TDE.</td><td>□</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td rowspan="2">**TSP 6.2.7** Interview personnel and observe intrusion-detection system settings to verify that a physical intrusion-detection system is in place and connected to the alarm system.</td><td>**Identify the responsible personnel** interviewed for this testing procedure.</td><td colspan="4">*<Report Findings Here>*</td></tr>
<tr><td>**Identify the system component(s)** observed for this testing procedure.</td><td colspan="4">*<Report Findings Here>*</td></tr>
</table>

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
	Describe how the intrusion detection system settings confirm that a physical intrusion-detection system is in place and connected to the alarm system.				
	<Report Findings Here>				
TSP 6.2.8 HSMs must be stored in a dedicated area(s) (e.g., secure room, cabinet, or cage) that is physically separate from non-TDE systems.		□	□	□	□
TSP 6.2.8 Examine TDE device inventory and observe physical locations of TDE HSMs to verify they are located in a dedicated area(s) that is physically separate from non-TDE systems.	**Identify the TDE device inventory** examined.	*<Report Findings Here>*			
	Describe how TDE HSMs are located in a dedicated area(s) that is physically separate from non-TDE systems.				
	<Report Findings Here>				
TSP 6.2.9 The physical connection points leading into the TDE network must be controlled at all times.		□	□	□	□
TSP 6.2.9 Observe physical connection points leading into the TDE network to verify they are controlled at all times.	**Provide the name of the assessor** who attests that physical connection points leading into the TDE network are controlled at all times.	*<Report Findings Here>*			
TSP 6.2.10 Conduit openings for utilities or ductwork passing through TSP floor space from public or shared access, and/or from TSP floor space into the TDE, must be sized to prevent surreptitious or forced entry into the TDE. Intrusion detection devices and/or security meshing may be used.		□	□	□	□
TSP 6.2.10 Observe conduit openings passing through TSP floor space from public or shared access, and/or from TSP floor space into the TDE. For all conduit openings, verify that one or more of the following controls is in place to prevent personnel from using the conduit as an entry mechanism: • The conduit opening is sized to prevent personnel from accessing the TDE via the conduit, and/or • Intrusion detection devices and/or security meshing are in place.	**Provide the name of the assessor** who attests that, for all conduit openings, one or more of the following controls is in place to prevent personnel from using the conduit as an entry mechanism: • The conduit opening is sized to prevent personnel from accessing the TDE via the conduit, and/or • Intrusion detection devices and/or security meshing are in place.	*<Report Findings Here>*			

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 6.3 Closed-Circuit Television (CCTV)					
TSP 6.3.1 The CCTV must be able to capture identifiable images of individuals entering or leaving the TDE at all times. All CCTV cameras must be tested and monitors checked at least monthly to confirm clarity of images, and a record of such testing retained for a minimum of two years.		□	□	□	□
TSP 6.3.1.a Observe CCTV footage from different times of day (including night time) to verify that identifiable images of individuals entering or leaving the TDE are captured at all times. Records of such testing are retained for a minimum of two years.	**Provide the name of the assessor** who attests that identifiable images of individuals entering or leaving the TDE are captured at all times and that records of such testing are retained for a minimum of two years.	*<Report Findings Here>*			
TSP 6.3.1.b Interview security personnel and examine records to verify that: • Cameras are tested and monitors checked at least monthly to confirm clarity of images. • Records of such testing are retained for a minimum of two years.	**Identify the records** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 6.3.2 Facilities must be equipped with an interior emergency lighting system that activates when the main lighting fails. When activated, this system should provide adequate lighting for all areas monitored by CCTV surveillance cameras, or the facility should have appropriate low light level cameras.		□	□	□	□
TSP 6.3.2 Examine CCTV camera settings, lighting at CCTV locations and lighting control settings to verify that either: • An emergency lighting system activates when the main lighting fails, and the emergency lighting provides adequate lighting for all areas monitored by CCTV cameras, or • The facility uses low-light level CCTV cameras that don't require additional lighting to monitor and capture images.	**Provide the name of the assessor** who attests that either: • An emergency lighting system activates when the main lighting fails, and the emergency lighting provides adequate lighting for all areas monitored by CCTV cameras, or • The facility uses low-light level CCTV cameras that don't require additional lighting to monitor and capture images.	*<Report Findings Here>*			

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 6.3.3 CCTV cameras must monitor all access to the TDE 24 hours a day, 7 days a week: - Blind spots must not exist. - Cameras within the TDE must monitor the room whenever the TDE is occupied.		□	□	□	□
TSP 6.3.3.a Examine CCTV camera locations and captured images to verify that cameras monitor all access to the TDE 24/7, and there are no blind spots.	**Provide the name of the assessor** who attests that: - There are no blind spots in the CCTV camera locations. - Cameras monitor all access to the TDE 24/7.	*<Report Findings Here>*			
TSP 6.3.3.b Examine CCTV camera settings and captured images from within the TDE to verify that the TDE is monitored whenever it is occupied.	**Provide the name of the assessor** who attests that the TDE is monitored whenever it is occupied.	*<Report Findings Here>*			
TSP 6.3.4 CCTV cameras must be connected at all times to: - Monitors located in a dedicated control room - An alarm system that will generate an alarm if the CCTV is disrupted - An active image-recording device - A back-up electrical power source capable of maintaining the system for a minimum of two hours.		□	□	□	□
TSP 6.3.4 Examine CCTV control settings and interview personnel to verify that CCTV cameras are connected at all times to: - Monitors located in a dedicated control room - An alarm system that will generate an alarm if the CCTV is disrupted - An active image-recording device - A back-up electrical power source capable of maintaining the system for a minimum of two hours.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how CCTV control settings ensure that cameras are connected at all times to:				
	- Monitors located in a dedicated control room	*<Report Findings Here>*			
	- An alarm system that will generate an alarm if the CCTV is disrupted	*<Report Findings Here>*			
	- An active image-recording device	*<Report Findings Here>*			

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
	• A back-up electrical power source capable of maintaining the system for a minimum of two hours.	*<Report Findings Here>*			
TSP 6.3.5 CCTV equipment must record at a minimum of four frames per second and be able to record events during dark periods—for example, through the use of infrared CCTV cameras or automatic activation of floodlights upon any detected activity.		□	□	□	□
TSP 6.3.5 Examine camera settings and documentation to verify that camera recordings provide a minimum of • One (1) picture frame per second continuous and three (3) picture frames on motion, • One (1) LUX minimum continuous lighting at locations covered by cameras.	**Identify the documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how camera settings ensure that camera recordings provide a minimum of:				
	• One (1) picture frame per second continuous and three (3) picture frames on motion,	*<Report Findings Here>*			
	• One (1) LUX minimum continuous lighting at locations covered by cameras.	*<Report Findings Here>*			
TSP 6.3.6 CCTV recordings must be time-stamped with date and time, and CCTV clocks synchronized with the electronic access control and intrusion-detection systems. CCTV clocks must be checked weekly to verify synchronization.		□	□	□	□
TSP 6.3.6.a Examine CCTV recordings to verify they are time-stamped with date and time.	**Describe how** CCTV recordings are time stamped with date and time.				
	<Report Findings Here>				
TSP 6.3.6.b Examine documented procedures to verify that mechanisms are defined for synchronizing the time and date stamps of the CCTV cameras, access control and intrusion-detection systems.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 6.3.6.c Examine system configurations for CCTV cameras, access control and intrusion-detection systems to verify that clocks are synchronized.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how system configurations confirm that clocks are synchronized for the following:				
	• CCTV cameras	*<Report Findings Here>*			

TSP 6. Restrict physical access to the TDE					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
	• Access control systems	*<Report Findings Here>*			
	• Intrusion detection systems	*<Report Findings Here>*			
TSP 6.3.6.d Examine access logs and recordings from the CCTV camera, access control and intrusion-detection systems to verify time and date stamps are synchronized.	**Provide the name of the assessor** who attests that time and date stamps are synchronized.	*<Report Findings Here>*			
TSP 6.3.6.e Examine documented procedures and interview personnel to verify that CCTV clocks are checked weekly to verify synchronization.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 6.3.7 CCTV servers and recording storage must be located within a secure area separate to the TDE.		□	□	□	□
TSP 6.3.7.a Observe the location of the CCTV server and storage systems to verify they are located in a secure area that is separate from the TDE.	**Describe how** the following are located in a secure area that is separate from the TDE.				
	• CCTV server	*<Report Findings Here>*			
	• Storage systems	*<Report Findings Here>*			
TSP 6.3.7.b Examine access-control lists for the CCTV server/storage area and for the TDE to identify all personnel with access to each area. Compare access lists to verify that personnel with access to the TDE do not have access to the CCTV server/storage area.	**Provide the name of the assessor** who attests that personnel with access to the TDE to not have access to the CCTV server/storage area.	*<Report Findings Here>*			
TSP 6.3.8 CCTV recordings for the TDE area must be retained for a minimum of 90 days.		□	□	□	□
TSP 6.3.8.a Examine system configurations, storage capacities, and media rotation schedules to verify that systems and processes are in place to retain at least 90 days of images for the TDE area.	**Describe how** systems and processes are in place for the following to ensure that at least 90 days of images are retained for the TDE area:				
	• System configurations	*<Report Findings Here>*			
	• Storage capacities	*<Report Findings Here>*			
	• Media rotation schedules	*<Report Findings Here>*			

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 6.3.8.b Examine recordings captured over the most recent 90-day period to verify that recordings for the TDE area are retained for at least 90 days.	**Describe how** recordings captured over the most recent 90-day period for the TDE are retained for at least 90 days.				
	<Report Findings Here>				
TSP 6.4 Access Control Systems					
TSP 6.4.1 Access control systems must be in place to control all access events.		☐	☐	☐	☐
TSP 6.4.1 Examine access control system configuration and access logs to verify systems control all access events.	**Identify the access control system** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the access control logs examined for this testing procedure.	*<Report Findings Here>*			
	Describe how access control system configurations confirm that all access events are controlled by systems.				
	<Report Findings Here>				
	Describe how access logs show that all access events are controlled by systems.				
	<Report Findings Here>				
TSP 6.4.2 The access-control system must grant access to personnel only during authorized working hours, and only to those areas required by the individual's job functions.		☐	☐	☐	☐
TSP 6.4.2 Examine access control system configuration and access control lists. Interview responsible personnel to verify that the permitted access is only as needed for each individual's authorized working hours and only to the areas required by the individual's job functions.	**Provide the name of the assessor** who attests that the permitted access is only as needed for each individual's authorized working hours and only to the areas required by the individual's job functions.	*<Report Findings Here>*			
TSP 6.4.3 Access control system servers and control panels must be located within a secure area separate to the TDE, and be connected to a back-up electrical power source capable of maintaining the system for a minimum of two hours.		☐	☐	☐	☐

<table>
<tr><th colspan="6"><i>TSP 6. Restrict physical access to the TDE</i></th></tr>
<tr><th rowspan="2">Requirements and Testing Procedures</th><th rowspan="2">Reporting Instructions & Assessor’s Findings</th><th colspan="4">Summary of Assessment Findings
(check one)</th></tr>
<tr><th>In Place</th><th>In Place w/ CCW</th><th>N/A</th><th>Not in Place</th></tr>
<tr><td rowspan="2"><b>TSP 6.4.3.a</b> Observe the location of the access control system servers and control panels to verify they are located in a secure area that is separate from the TDE.</td><td colspan="5"><b>Describe how</b> access control system servers and control panels are located in a secure area that is separate from the TDE.</td></tr>
<tr><td colspan="5"><i><Report Findings Here></i></td></tr>
<tr><td rowspan="3"><b>TSP 6.4.3.b</b> Examine access-control lists for the access-control server area and for the TDE to identify all personnel with access to each area. Compare access lists to verify that personnel with access to the TDE do not have access to the access-control server area.</td><td><b>Identify the access-control list</b> examined for this testing procedure.</td><td colspan="4"><i><Report Findings Here></i></td></tr>
<tr><td colspan="5"><b>Describe how</b> personnel with access to the TDE to not have access to the access-control server area.</td></tr>
<tr><td colspan="5"><i><Report Findings Here></i></td></tr>
<tr><td rowspan="3"><b>TSP 6.4.3.c</b> Examine system configurations to verify that access control system servers and control panels are connected to a back-up electrical power source capable of maintaining the system for a minimum of two hours.</td><td><b>Identify the system component(s)</b> examined for this testing procedure.</td><td colspan="4"><i><Report Findings Here></i></td></tr>
<tr><td colspan="5"><b>Describe how</b> system configurations confirm that the access control system servers and control panels are connected to a back-up electrical power source capable of maintaining the system for a minimum of two hours.</td></tr>
<tr><td colspan="5"><i><Report Findings Here></i></td></tr>
<tr><td colspan="2"><b>TSP 6.4.4</b> The access control system must provide an audit trail of all access attempts to the TDE. Audit logs must include:
• Time and date of access request
• Identification of individual requesting access
• Location
• Whether access was granted or denied</td><td>□</td><td>□</td><td>□</td><td>□</td></tr>
<tr><td rowspan="3"><b>TSP 6.4.4.a</b> Examine access control system configuration to verify that audit trails are enabled and configured to log all access attempts to the TDE.</td><td><b>Identify the system component(s)</b> examined for this testing procedure.</td><td colspan="4"><i><Report Findings Here></i></td></tr>
<tr><td colspan="5"><b>Describe how</b> access control system configurations confirm that audit trails are enabled and configured to log all access attempts to the TDE.</td></tr>
<tr><td colspan="5"><i><Report Findings Here></i></td></tr>
</table>

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 6.4.4.b Observe audit logs for the access control system to verify that an audit trail exists for all TDE access points, and includes the following detail: • Time and date of access request • Identification of individual requesting access • Location • Whether access was granted or denied	**Identify the audit logs** observed for this testing procedure.	*<Report Findings Here>*			
	Describe how audit logs for the access control system contain an audit trail for all TDE access points that includes:				
	• Time and date of access request	*<Report Findings Here>*			
	• Identification of individual requesting access	*<Report Findings Here>*			
	• Location	*<Report Findings Here>*			
	• Whether access was granted or denied	*<Report Findings Here>*			
TSP 6.4.5 Access logs to the TDE must be reviewed at least monthly by the assigned Security Manager (see TSP 8), resulting in a documented validation report.		□	□	□	□
TSP 6.4.5 Examine documented validation reports and interview the TDE owner to verify that access logs to the TDE are reviewed and validated at least monthly.	**Identify the documented validation reports** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how the validation reports show that access logs to the TDE are reviewed and validated at least monthly.				
	<Report Findings Here>				
TSP 6.4.6 Records generated by the electronic access control system must be retained for a minimum of one year.		□	□	□	□
TSP 6.4.6 Examine audit logs to verify that records generated by the electronic access control system are retained for a minimum of one year.	**Identify the audit logs** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how audit logs show that records generated by the electronic access control system are retained for a minimum of one year.				

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
	<Report Findings Here>				
TSP 6.4.7 The access control system must be tested at least once each calendar quarter and a documented report kept for at least three years.		□	□	□	□
TSP 6.4.7 Examine testing report documentation to verify that: • The electronic access control system is tested at least once each calendar quarter, and • Documented reports are kept for at least three years	**Identify the testing report documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how the testing report documentation shows that:				
	• The electronic access control system is tested at least once each calendar quarter, and	*<Report Findings Here>*			
	• Documented reports are kept for at least three years	*<Report Findings Here>*			
TSP 6.5 Alarms					
TSP 6.5.1 The access control system must provide an audible alarm (local sounder) and an auditable record of door conditions. For the TDE, an alarm event should activate if a controlled door or gate is left open for more than 30 seconds.		□	□	□	□
TSP 6.5.1.a Examine access control system configuration to verify it provides an audible alarm and an auditable record of door conditions.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how the access control system configurations confirm that it provides an audible alarm and an auditable record of door conditions.				
	<Report Findings Here>				
TSP 6.5.1.b Examine audit logs from the access control system to verify the door conditions are recorded.	**Describe how** door conditions are recorded in the audit logs from the access control system.				
	<Report Findings Here>				
TSP 6.5.1.c Examine TDE entry mechanisms to verify that an audible alarm is configured to sound if the entrance remains open for more than 30 seconds	**Describe how** the TDE entry mechanisms are configured to sound an audible alarm if the entrance remains open for more than 30 seconds.				
	<Report Findings Here>				

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 6.5.1.d Observe authorized personnel entering the TDE and request the door or gate is held open. Verify that an audible alarm sounds if the TDE entrance remains open for more than 30 seconds.	**Describe how** an audible alarm sounds if the TDE entrance remains open for more than 30 seconds.				
	<Report Findings Here>				
TSP 6.5.2 Alarm conditions must transmit to a staffed, central monitoring location for assessment and response. ***Note:*** *For multi-tenant buildings, an outsourced monitoring location or an auto-dialer that rings a designated TSP staff member may monitor output from the electronic intrusion detection system.*		□	□	□	□
TSP 6.5.2 Examine alarm system configuration to verify that alarm conditions are transmitted to a staffed, central monitoring location for assessment and response.	**Describe how** the alarm system configurations confirm that alarm conditions are transmitted to a staffed, central monitoring location for assessment and response.				
	<Report Findings Here>				
TSP 6.5.3 Alarm response must require the physical inspection of the alarm site within a reasonable, defined time by a security officer, local law enforcement personnel or designated TSP personnel.		□	□	□	□
TSP 6.5.3.a Review documented procedures to verify they: • Require that an alarm response is required that includes the physical inspection of the alarm site within a reasonable, defined time. • Identify personnel authorized to perform the physical inspection—i.e., security officers, local law enforcement personnel or designated TSP personnel.	**Identify the documented procedures** reviewed for this testing procedure.	*<Report Findings Here>*			
TSP 6.5.3.b Examine records of previous alarm events and interview response personnel to verify that: • A physical inspection of the alarm site occurred within a reasonable time.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the records of previous alarm events examined for this testing procedure.	*<Report Findings Here>*			
	Describe how the records of previous alarm events show that:				

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
• The physical inspection was performed by authorized personnel—i.e., a security officer, local law enforcement personnel or designated TSP personnel.	• A physical inspection of the alarm site occurred within a reasonable time.	*<Report Findings Here>*			
	• The physical inspection was performed by authorized personnel—i.e., a security officer, local law enforcement personnel or designated TSP personnel.	*<Report Findings Here>*			
TSP 6.5.4 All alarm conditions, response, and outcome must be documented and maintained for a minimum of one year.		□	□	□	□
TSP 6.5.4 Examine audit logs and response reports to verify alarm conditions, response, and outcome are retained for a minimum of one year.	**Identify the audit logs** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the response reports examined for this testing procedure.	*<Report Findings Here>*			
TSP 6.6 Personnel Security					
TSP 6.6.1 All individuals—including employees, visitors, and third parties—who require access to the TDE must obtain an approved photo identification badge. Badges must be worn and visible at all times.		□	□	□	□
TSP 6.6.1.a Examine documented procedures to verify that use of approved photo identification badge is required, and that what constitutes an approved photo identification badge is clearly defined.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 6.6.1.b Observe individuals gaining access to the TDE to verify that: • An approved photo identification badge is required for all entry. • The photo identification badges are in accordance with the TSP's documented requirements.	**Describe how** the following is in place for individuals gaining access to the TDE:				
	• An approved photo identification badge is required for all entry.	*<Report Findings Here>*			
	• The photo identification badges are in accordance with the TSP's documented requirements.	*<Report Findings Here>*			
	Describe how badges are worn and visible at all times for:				
	• Individuals entering the TDE	*<Report Findings Here>*			

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 6.6.1.c Observe individuals entering and within the TDE to verify that badges are worn and visible at all times.	- Individuals within the TDE	*<Report Findings Here>*			
TSP 6.6.2 ID badges must not disclose the corporate name or location of the facility to which they permit access.		□	□	□	□
TSP 6.6.2 Observe ID badges in use to verify that badges do not disclose the corporate name or location of the TSP facility to which they permit access.	**Describe how** the badges in use do not disclose the corporate name or location of the TSP facility to which they permit access.				
	<Report Findings Here>				
TSP 6.6.3 All TSP personnel with access to the TDE must undergo a security background check as defined in PCI DSS Requirement 12.7.		□	□	□	□
TSP 6.6.3 Obtain a list of TSP personnel with access to the TDE, interview Human Resource department management to verify that background checks are conducted (within the constraints of local laws) for all TSP personnel with access to the TDE.	**Identify the Human Resources personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the documented list of TSP personnel with access to the TDE examined for this testing procedure.	*<Report Findings Here>*			
TSP 6.6.4 All visitors and third parties must either be escorted at all times within TDE, or have undergone a background check as defined in PCI DSS Requirement 12.7 prior to being granted access.		□	□	□	□
TSP 6.6.4.a Examine documented procedures to verify that all visitors and third parties must either be escorted at all times within TDE, or undergo a background check as defined in PCI DSS Requirement 12.7 prior to being granted access.	**Identify the documented procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 6.6.4.b Observe visitors and third party individuals granted access to the TDE, and interview authorizing personnel and/or Human Resource department management to verify that all such individuals are either escorted at all times within the TDE, or had undergone a background check prior to being granted access.	**Identify the authorizing and/or Human Resources personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how visitors and third party personnel are either escorted at all times within TDE, or had undergone a background check prior to being granted access.				
	<Report Findings Here>				

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 6.6.5 Access policies and procedures must be communicated and acknowledged by personnel with access to the TDE. Policies must include: • All personnel are responsible for securing their ID badge from loss or theft. It is not permitted to share or loan ID badges or access cards to another person. • If an individual determines his/her ID badge has been lost or misplaced, they must notify the TSP badge administrator immediately. • Upon notification of a lost or misplaced badge, access to the badge must be immediately revoked and/or the badge disabled.		□	□	□	□
TSP 6.6.5.a Examine access policies and procedures to verify they require: • All personnel are responsible for securing their ID badge from loss or theft. It is not permitted to share or loan ID badges or access cards to another person. • If an individual determines his/her ID badge has been lost or misplaced, they must notify the TSP badge administrator immediately. • Upon notification of a lost or misplaced badge, access to the badge must be immediately revoked and/or the badge disabled.	**Identify the access policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 6.6.5.b Interview personnel with access to the TDE and examine documented acknowledgments to verify that the access policies and procedures have been communicated and acknowledged.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 6.7 Physical Locks and Keys					
TSP 6.7.1 When manually keyed locksets are used to provide override capability of the electronic access control system, the keys must be designed under a master keying system.		□	□	□	□

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 6.7.1 If manually keyed locksets are used to provide override capability of the electronic access control system, interview the Security Manager to verify that the keys are designed under a master keying system.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 6.7.2 Facility master keys that can override an access-controlled door may only be provided to the Security Manager, or their designated equivalent.		□	□	□	□
TSP 6.7.2 Examine key-issuance logs and interview the Security Manager to verify that facility master keys that can override an access-controlled door are only provided to the Security Manager or their designated equivalent.	**Identify the key-issuance logs** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the Security Manager interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how the key-issuance logs show that facility master keys that can override an access-controlled door are only provided to the Security Manager or their designated equivalent.				
	<Report Findings Here>				
TSP 6.7.3 The number of facility master keys must be kept to the essential minimum as defined by business needs. Unissued keys must be stored in locked security containers at all times, and inventoried at least monthly by the physical key custodian.		□	□	□	□
TSP 6.7.3.a Examine key-issuance logs and interview the Security Manager to verify that the number of facility master keys is kept to the essential minimum as defined by business needs.	**Identify the key-issuance logs** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how the key issuance logs show that the number of facility master keys is kept to the essential minimum as defined by business needs.				
	<Report Findings Here>				
TSP 6.7.3.b Examine physical key storage locations to verify that unissued keys are stored in locked security containers at all times.	**Describe how** unissued keys are stored in locked security containers at all times.				
	<Report Findings Here>				

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 6.7.3.c Examine key inventory records and interview the physical key custodian to verify that physical keys are inventoried at least monthly.	**Identify the key inventory records** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 6.7.4 Each key must be identified by a unique code to identify the key and the individual to whom it is issued. Keys must not carry any markings or tags that identify the facility or door which it opens.		□	□	□	□
TSP 6.7.4.a Examine physical keys and key inventory to verify that: • Each key is identified by a unique code. • Keys do not carry any markings or tags that identify the facility or door that it opens.	**Provide the name of the assessor** who attests that: • Each key is identified by a unique code. • Keys do not carry any markings or tags that identify the facility or door that it opens.	*<Report Findings Here>*			
TSP 6.7.5 The designated physical key custodian must manage and maintain an auditable record of key issuance. A log of key issuance must be maintained for a minimum of one year and contain at least the following information: • Key-identification number • Date and time the key is issued (transfer of responsibility) • Name and signature of the employee issuing the key • Name and signature of the authorized recipient of the key • Date and time the key is returned (transfer of responsibility) • Name and signature of the authorized individual returning the key		□	□	□	□
	Identify the key issuance logs examined for this testing procedure.	*<Report Findings Here>*			

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 6.7.5.a Examine key-issuance logs to verify that a log of key issuance is maintained that contains at least the following information: • Key-identification number • Date and time the key is issued (transfer of responsibility) • Name and signature of the employee issuing the key • Name and signature of the authorized recipient • Date and time the key is returned (transfer of responsibility) • Name and signature of the authorized individual returning the key					
TSP 6.7.5.b Interview the physical key custodian and examine key-issuance logs to verify that the log is maintained for a minimum of one year.	**Identify the physical key custodian** interviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the key issuance logs examined for this testing procedure.	*<Report Findings Here>*			
	Describe how key issuance logs are maintained for a minimum of one year.				
	<Report Findings Here>				
TSP 6.7.6 Personnel who are issued keys must sign a consent form indicating they received such keys and that they will ensure that the key(s) entrusted to them cannot be accessed by unauthorized individuals.		□	□	□	□
TSP 6.7.6.a Examine consent forms to verify they require personnel issued with keys to acknowledge receipt of the key(s), and that they will ensure that the key(s) entrusted to them cannot be accessed by unauthorized individuals.	**Identify the consent forms** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the signed consent forms examined for this testing procedure.	*<Report Findings Here>*			

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 6.7.6.b Examine signed consent forms and key-issuance logs to verify that personnel currently issued with keys have signed the consent form.	**Identify the key-issuance logs** examined for this testing procedure.	*<Report Findings Here>*			
TSP 6.7.6.c Interview personnel issued with keys to verify they understand their responsibility to ensure that the key(s) entrusted to them cannot be accessed by unauthorized individuals.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 6.7.7 Physical keys may not be transferred or loaned to another individual by the assignee. If there is a need to transfer custodianship, the defined transfer process must be followed (see TSP 6.7.5).		□	□	□	□
TSP 6.7.7 Interview personnel issued with keys to verify they do not transfer or loan keys to another individual.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 6.7.8 Use of a physical key to override an electronic access-controlled system must result in an alarm condition that is validated by another individual.		□	□	□	□
TSP 6.7.8.a Examine alarm system configuration to verify that use of a physical key to override an electronic access-controlled system results in an alarm condition.	**Identify the system component(s)** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how the alarm system configuration confirms that use of a physical key to override an electronic access-controlled system results in an alarm condition.				
	<Report Findings Here>				
TSP 6.7.8.b Examine policies and procedures to verify that such alarm conditions are validated by another individual.	**Identify the policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 6.8 Media Handling and Destruction					
TSP 6.8.1 All TDE removable media must be stored within the TDE or in the custody of an authorized individual.		□	□	□	□
TSP 6.8.1 Observe media storage in the TDE and interview personnel to verify that removable media is	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
either stored within the TDE or in the custody of an authorized individual.	**Describe how** the removable media is either stored within the TDE or in the custody of an authorized individual.				
	<Report Findings Here>				
TSP 6.8.2 A log must be maintained when media is removed from or returned to its storage location, or transferred to the custody of another individual. The log must contain: • Unique media identifier • Date and time media moved or transferred • Name and signature of current custodian or storage location • Name and signature of recipient custodian or storage location • Reason for transfer		□	□	□	□
TSP 6.8.2.a Examine TDE media logs and interview personnel to verify that a record is maintained of all media removed from or returned to its storage location in the TDE, or transferred to the custody of another individual.	**Identify the TDE media logs** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 6. Restrict physical access to the TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 6.8.2.b Examine TDE media logs to verify the log contains: • Unique media identifier • Date and time media moved or transferred • Name and signature of current custodian or storage location • Name and signature of recipient custodian or storage location • Reason for transfer	**Provide the name of the assessor** who attests that TDE media logs contain the following: • Unique media identifier • Date and time media moved or transferred • Name and signature of current custodian or storage location • Name and signature of recipient custodian or storage location • Reason for transfer	**<Report Findings Here>**			
TSP 6.8.3 The destruction of media containing CHD, Payment Tokens and/or Payment Token Data must be performed according to industry standards under dual control. A log must be maintained and signed confirming the destruction process.		□	□	□	□
TSP 6.8.3.a Examine media destruction procedures and interview personnel to verify that media containing CHD Payment Tokens and/or Payment Token Data is destroyed according to industry standards, and under dual control.	**Identify the media destruction procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 6.8.3.b Examine media destruction records to verify that a log is maintained and signed to confirm the destruction process.	**Identify the media destruction records** examined for this testing procedure.	*<Report Findings Here>*			
	Describe how media destruction records show that a log is maintained and signed to confirm the destruction process.				
	<Report Findings Here>				

TSP 7. Monitor all access to TDE

The requirements in this section build on PCI DSS Requirement 10.

TSP 7. Monitor all access to TDE

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 7.1 Identify and respond to suspicious events					
TSP 7.1.1 Implement a methodology for the timely identification of attack patterns and undesirable behavior across systems—for example, using coordinated manual reviews and/or centrally-managed or automated log correlation tools—to include at least the following: • Identification of anomalies or suspicious activity as they occur • Issuance of timely alerts upon detection of suspicious activity or anomaly to responsible personnel • Response to alerts in accordance with documented response procedures		□	□	□	□
TSP 7.1.1.a Review documentation and interview personnel to verify a methodology is defined and implemented to identify attack patterns and undesirable behavior across systems in a timely manner, and includes the following: • Identification of anomalies or suspicious activity as they occur • Issuance of timely alerts to responsible personnel • Response to alerts in accordance with documented response procedures	**Identify the documentation** reviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 7.1.1.b Examine incident response procedures and interview responsible personnel to verify that: • On-call personnel receive timely alerts. • Alerts are responded to per documented response procedures.	**Identify the incident response procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			

TSP 8. Maintain an Information Security Policy

The requirements in this section build on PCI DSS Requirement 12.

TSP 8. Maintain an Information Security Policy					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 8.1 Security Roles and Responsibilities					
TSP 8.1.1 Assign to an individual the following responsibilities: • A senior-level executive within the organization responsible for establishing and maintaining programs to ensure information assets are adequately protected. This role is referred to as Chief Information Security Officer (CISO), or equivalent. • A manager designated with the overall responsibility for physical security for the TDE. This role is referred to as Security Manager.		□	□	□	□
TSP 8.1.1.a Interview personnel and examine documentation to verify a senior manager has been identified as being responsible for the TSP Information Security Management.	**Identify the documentation** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 8.1.1.b Interview personnel and review biographical information to verify identified individual has IT security knowledge.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the biographical information examined for this testing procedure.	*<Report Findings Here>*			
TSP 8.1.1.c Interview personnel and examine documentation to identify manager with overall security responsibilities of the facility and for the TDE.	**Identify the documentation** examined for this testing procedure.	*<Report Findings Here>*			

TSP 8. Maintain an Information Security Policy

Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 8.2 Implement a PCI DSS compliance program					
TSP 8.2.1 Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program • Providing updates to executive management and board of directors on PCI DSS compliance initiatives and issues, including remediation activities, at least annually		□	□	□	□
TSP 8.2.1.a Examine documentation to verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance.	**Identify the documentation** examined for this testing procedure.	*<Report Findings Here>*			
TSP 8.2.1.b Examine the company's PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized.	**Identify the company's PCI DSS charter** examined for this testing procedure.	*<Report Findings Here>*			
TSP 8.2.1.c Examine executive management and board of directors meeting minutes and/or presentations to ensure PCI DSS compliance initiatives and remediation activities are communicated at least annually.	**Identify the executive management and board of directors meeting minutes and/or presentations** examined for this testing procedure.	*<Report Findings Here>*			

TSP 8. Maintain an Information Security Policy

		Summary of Assessment Findings (check one)			
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**In Place**	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 8.2.2 A formal PCI DSS compliance program must be in place to include: • Definition of activities for maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities • Annual PCI DSS assessment processes • Processes for the continuous validation of PCI DSS requirements (for example: daily, weekly, quarterly, etc. as applicable per requirement) • A process for performing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions		□	□	□	□
TSP 8.2.2.a Examine information security policies and procedures to verify that processes are specifically defined for the following: • Maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities • Annual PCI DSS assessment(s) • Continuous validation of PCI DSS requirements • Business-impact analysis to determine potential PCI DSS impacts for strategic business decisions	**Identify the information security policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 8.2.2.b Interview personnel and observe compliance activities to verify that the defined processes are implemented for the following: • Maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities • Annual PCI DSS assessment(s) • Continuous validation of PCI DSS requirements • Business-impact analysis to determine potential PCI DSS impacts for strategic business decisions	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how defined processes are implemented for the following:				
	• Maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities	*<Report Findings Here>*			
	• Annual PCI DSS assessment(s)	*<Report Findings Here>*			

TSP 8. Maintain an Information Security Policy

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
	• Continuous validation of PCI DSS requirements	*<Report Findings Here>*			
	• Business-impact analysis to determine potential PCI DSS impacts for strategic business decisions	*<Report Findings Here>*			
TSP 8.2.3 PCI DSS compliance roles and responsibilities must be specifically defined and formally assigned to one or more personnel, including at least the following: • Managing PCI DSS business-as-usual activities • Managing annual PCI DSS assessments • Managing continuous validation of PCI DSS requirements (for example: daily, weekly, quarterly, etc. as applicable per requirement) • Managing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions		□	□	□	□
TSP 8.2.3.a Examine information security policies and procedures and interview personnel to verify that roles and responsibilities are clearly defined and that duties are assigned to include at least the following: • Managing PCI DSS business-as-usual activities • Managing annual PCI DSS assessments • Managing continuous validation of PCI DSS requirements (for example: daily, weekly, quarterly, etc. as applicable per requirement) • Managing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions	**Identify the information security policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 8.2.3.b Interview responsible personnel and verify they are familiar with and performing their designated PCI DSS compliance responsibilities.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 8.2.4 Provide up-to-date PCI DSS and/or information security training at least annually to personnel with PCI DSS compliance responsibilities.		□	□	□	□

TSP 8. Maintain an Information Security Policy

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 8.2.4.a Examine information security policies and procedures to verify that PCI DSS and/or information security training is required at least annually for each role with PCI DSS compliance responsibilities.	**Identify the information security policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 8.2.4.b Interview personnel and examine certificates of attendance or other records to verify that personnel with PCI DSS compliance responsibility receive up-to-date PCI DSS and/or similar information security training at least annually.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the certificates of attendance or other records examined for this testing procedure.	*<Report Findings Here>*			
	Describe how personnel with PCI DSS compliance responsibility receive up-to-date PCI DSS and/or similar information security training at least annually.				
	<Report Findings Here>				
TSP 8.3 Validate PCI DSS is incorporated into business-as-usual (BAU) activities					
TSP 8.3.1 Implement a process to immediately detect and alert on critical security control failures. Examples of critical security controls include, but are not limited to: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)		□	□	□	□
TSP 8.3.1.a Examine documented policies and procedures to verify that processes are defined to immediately detect and alert on critical security control failures.	**Identify the documented policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			

TSP 8. Maintain an Information Security Policy					
Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
TSP 8.3.1.b Examine detection and alerting processes and interview personnel to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Describe how processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.				
	<Report Findings Here>				
TSP 8.3.1.1 Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls		□	□	□	□
TSP 8.3.1.1.a Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure, and include: • Restoring security functions	**Identify the documented policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			

TSP 8. Maintain an Information Security Policy

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
• Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 8.3.1.1.b Examine records to verify that security control failures are documented to include: • Identification of cause(s) of the failure, including root cause • Duration (date and time start and end) of the security failure • Details of the remediation required to address the root cause	**Identify the records** examined for this testing procedure.	*<Report Findings Here>*			
TSP 8.3.2 Review hardware and software technologies at least annually to confirm whether they continue to meet the organization's PCI DSS requirements. (For example, a review of technologies that are no longer supported by the vendor and/or no longer meet the security needs of the organization.) The process includes a plan for remediating technologies that no longer meet the organization's PCI DSS requirements, up to and including replacement of the technology, as appropriate.		□	□	□	□
TSP 8.3.2.a Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to review hardware and software technologies to confirm whether they continue to meet the organization's PCI DSS requirements.	**Identify the documented policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
	Identify the responsible personnel interviewed for this testing procedure.	*<Report Findings Here>*			
TSP 8.3.2.b Review the results of the recent reviews to verify reviews are performed at least annually.	**Identify the results of recent reviews** reviewed for this testing procedure.	*<Report Findings Here>*			

TSP 8. Maintain an Information Security Policy

Requirements and Testing Procedures	**Reporting Instructions & Assessor's Findings**	**Summary of Assessment Findings** (check one)			
		In Place	**In Place w/ CCW**	**N/A**	**Not in Place**
	Describe how the reviews are performed at least annually.				
	<Report Findings Here>				
TSP 8.3.2.c For any technologies that have been determined to no longer meet the organization's PCI DSS requirements, verify a plan is in place to remediate the technology.	**Indicate whether** there are any technologies that have been determined to no longer meet the organization's PCI DSS requirements**. (yes/no)** *If "no," mark the remainder of 8.3.2.c as "Not Applicable."* *If "yes," complete the following:*	*<Report Findings Here>*			
	Describe the plan verified to be in place to remediate the technology.				
	<Report Findings Here>				

TSP 8. Maintain an Information Security Policy

Requirements and Testing Procedures	Reporting Instructions & Assessor's Findings	Summary of Assessment Findings (check one)			
		In Place	In Place w/ CCW	N/A	Not in Place
TSP 8.3.3 Perform reviews at least quarterly to verify BAU activities are being followed. Reviews must be performed by personnel assigned to the PCI DSS compliance program (as identified in TSP 8.2.3), and include the following: • Confirmation that all BAU activities are being performed • Confirmation that personnel are following security policies and operational procedures (for example, daily log reviews, firewall rule-set reviews, configuration standards for new systems, etc.) • Documenting how the reviews were completed, including how all BAU activities were verified as being in place. • Collection of documented evidence as required for the annual PCI DSS assessment • Review and sign-off on results by personnel assigned responsibility for the PCI DSS compliance program • Retention of records and documentation for at least 12 months, covering all BAU activities		□	□	□	□
TSP 8.3.3.a Examine policies and procedures to verify that processes are defined for reviewing and verifying BAU activities. Verify the procedures include: • Confirming that all BAU activities are being performed • Confirming that personnel are following security policies and operational procedures (for example, daily log reviews, firewall rule-set reviews, configuration standards for new systems, etc.) • Documenting how the reviews were completed, including how all BAU activities were verified as being in place • Collecting documented evidence as required for the annual PCI DSS assessment • Reviewing and signing off on results by executive management assigned responsibility for PCI DSS governance • Retaining records and documentation for at least 12 months, covering all BAU activities	**Identify the policies and procedures** examined for this testing procedure.	*<Report Findings Here>*			
TSP 8.3.3.b Interview responsible personnel and examine records of reviews to verify that: • Reviews are performed by personnel assigned to the PCI DSS compliance program • Reviews are performed at least quarterly	**Identify the responsible personnel** interviewed for this testing procedure.	*<Report Findings Here>*			
	Identify the records of reviews examined for this testing procedure.	*<Report Findings Here>*			

Annex A: Minimum Key Sizes and Equivalent Key Strengths for Approved Algorithms

Cryptographic Algorithms

The following are the minimum key sizes and parameters for the algorithm(s) in question that should be used in connection with key transport, exchange, or establishment, and for data protection:

Algorithm	TDEA	AES	RSA	Elliptic Curve	DSA/D-H
Minimum key size in number of bits:	168	128	3072	256	3072/256

Key-encipherment keys should be at least of equal or greater strength than any key it is protecting. This applies to any key-encipherment key used for the protection of secret or private keys that are stored, or for keys used to encrypt any secret or private keys for loading or transport. The following algorithms and bits of security are considered equivalent for this purpose:

Bits of Security	Key Lengths			
	Symmetric key algorithms	RSA	Elliptic Curve	D-H
112	3TDEA [168-bit key]	2048	224-225	2048/224
128	AES-128	3072	256-383	3072/256
192	AES-192	7680	384-511	7680/384
256	AES-256	15360	512+	15360/512

3TDEA refers to three-key triple DEA keys exclusive of parity bits. The RSA key size refers to the size of the modulus. The Elliptic Curve key size refers to the minimum order of the base point on the elliptic curve; this order should be slightly smaller than the field size. The DSA key sizes refer to the size of the modulus and the minimum size of a large subgroup.

For implementations using Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH):

- **DH implementations** – Entities should securely generate and distribute the system-wide parameters: generator *g,* prime number *p,* and parameter *q,* the large prime factor of (*p* - 1). Parameter *p* should be at least 3072 bits long, and parameter *q* should be at least 256 bits long. Each entity should generate a private key *x* and a public key *y* using the domain parameters (*p, q, g*).
- **ECDH implementations** – Entities should securely generate and distribute the system-wide parameters. Entities may generate the elliptic curve domain parameters or use a recommended curve (See *FIPS186-4*). The elliptic curve specified by the domain parameters should be at least as secure as P-256 (or P-384). Each entity should generate a private key *d* and a public key *Q* using the specified elliptic curve domain parameters. (See *FIPS186-4* for methods of generating *d* and *Q*).
- Each private key should be statistically unique, unpredictable, and created using an approved random number generator as described below.
- Entities should authenticate the DH or ECDH public keys using DSA, ECDSA, a certificate, or a symmetric MAC (see *ISO 16609 – Banking –Requirements for message authentication using symmetric techniques*)*.* One of the following should be used: MAC algorithm 1 using padding method 3, MAC algorithm 5 using padding method 4.

Note that TDEA should not be used.

Secure Hash Algorithms

Current popular hashes produce hash values of length n = 128 (MD4 and MD5) and n = 160 (SHA-1), and therefore can provide no more than 64 or 80 bits of security, respectively, against collision attacks. To avoid introducing security weakness via any hash function used, the hash function should provide at least as many bits of security as does the cryptographic algorithm used, and in no case less than 128-bits. Standardized hash algorithms and associated effective bits of security are listed below.

Bits of Security	Hash Algorithm
128	SHA-256
128	SHA3-256 (SHA-3 family, a.k.a., Keccak)
192	SHA3-384
256	SHA-512
256	SHA3-512

Random Number Generators

The proper generation of random number is essential to the effective security for cryptographic key generation. Where deterministic random number generators are used, the requirements of *NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators* apply, except for the Dual_EC_DRBG algorithm, which should not be used.

The number of bits of entropy should be equal to or greater than the required number of bits of security.