Payment Card Industry (PCI)
Token Service Providers

Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens)

Version 1.0

December 2015

Table of Contents

Introduction

The purpose of this document is to define physical and logical security requirements and assessment procedures for Token Service Providers that generate and issue EMV Payment Tokens, as defined under the *EMV® Payment Tokenisation Specification Technical Framework*[1]. The *EMV® Payment Tokenisation Specification Technical Framework* defines Token Service Providers as:

> An entity that provides a Token Service comprised of the Token Vault and related processing. The Token Service Provider will have the ability to set aside licensed ISO BINS as Token BINs to issue Payment Tokens for the PANs that are submitted according to this specification.

In their capacity as the authorized party for issuance of Payment Tokens, Token Service Providers are responsible for a number of discrete functions, which are defined in the *EMV® Payment Tokenisation Specification Technical Framework.* For a detailed description of the Payment Token ecosystem, terminology definitions, key responsibilities, and controls specific to each entity within the ecosystem, refer to the *EMV® Payment Tokenisation Specification Technical Framework.*

This document does not address how a Token Service Provider would meet the requirements in the *EMV® Payment Tokenisation Specification Technical Framework*. Rather, this document defines the security controls needed to protect environments where the tokenization services occur.

Entities designated as a Token Service Provider under the *EMV Payment Tokenisation Specification* may be subject to these requirements. To determine if an entity is required to meet these requirements, confirm with the payment brand for which the services are provided.

These requirements cover EMV Payment Tokens, not acquiring tokens or other types of tokens. While organizations may choose to use this framework to assess other token deployments, it is not required that these requirements be applied to those implementations.

These requirements are not intended for merchants or any other entity that is not a Token Service Provider as described above.

[1] www.emvco.com

Terminology

To assist with understanding the applicability of these requirements, this document introduces the following terms:

- **Payment Token** – A surrogate value for a PAN that meets the EMVCo definition of Payment Token, as defined in the *EMV® Payment Tokenisation Specification Technical Framework.*
- **Payment Token Data** – Covers a number of discrete data elements, including the Payment Token and related data as defined in the *EMV® Payment Tokenisation Specification Technical Framework,* which include the Payment Token Expiry Date, Payment Token Requestor ID, Payment Token Assurance Level and Payment Token Assurance Data.
- **TSP** – Acronym for entities designated as a Token Service Provider under the *EMV® Payment Tokenisation Specification Technical Framework*.
- **TDE** – Acronym for token data environment. The TDE is a dedicated, secure area within which the TSP performs tokenization services in accordance with the *EMV® Payment Tokenisation Specification Technical Framework,* and as described below.

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

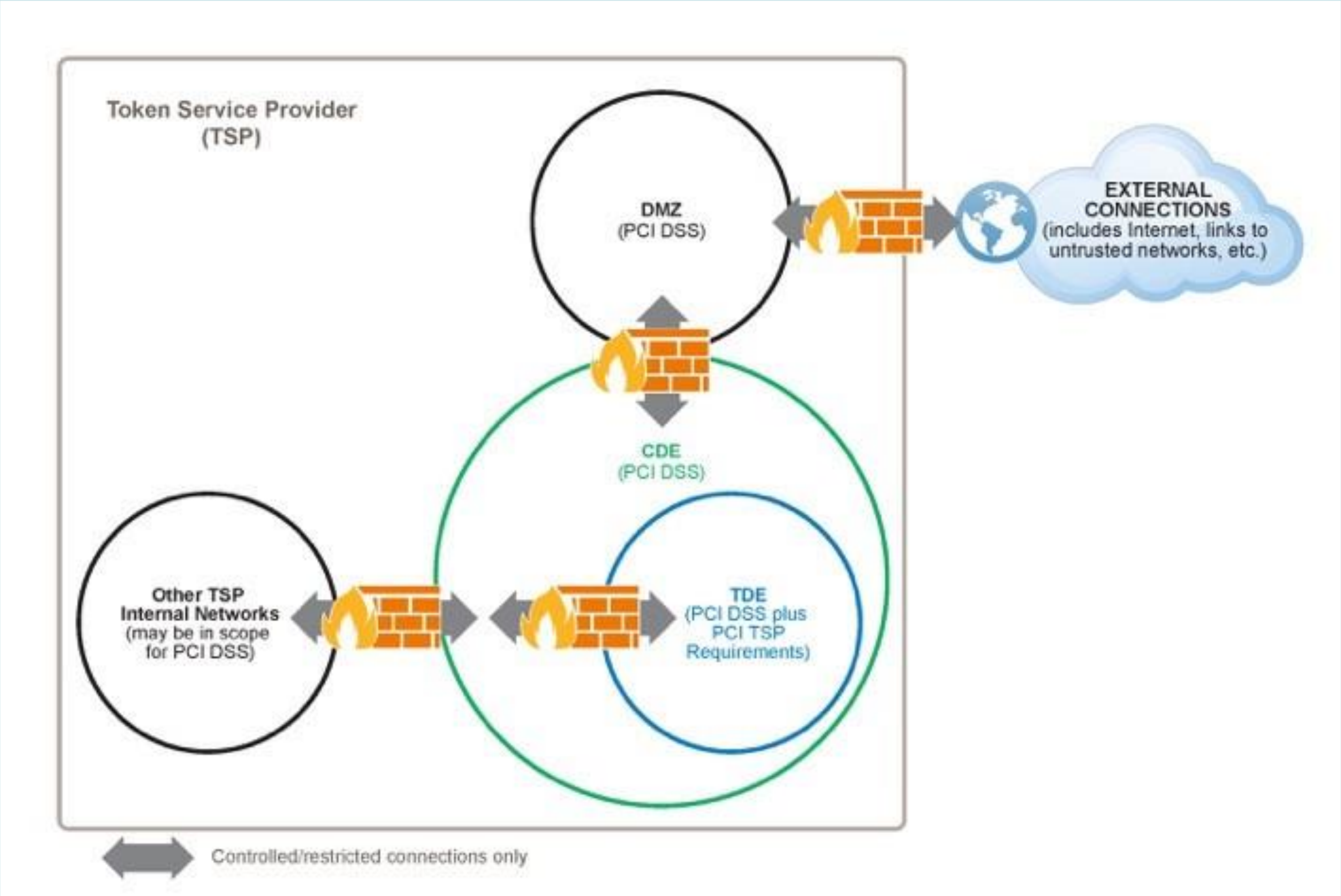
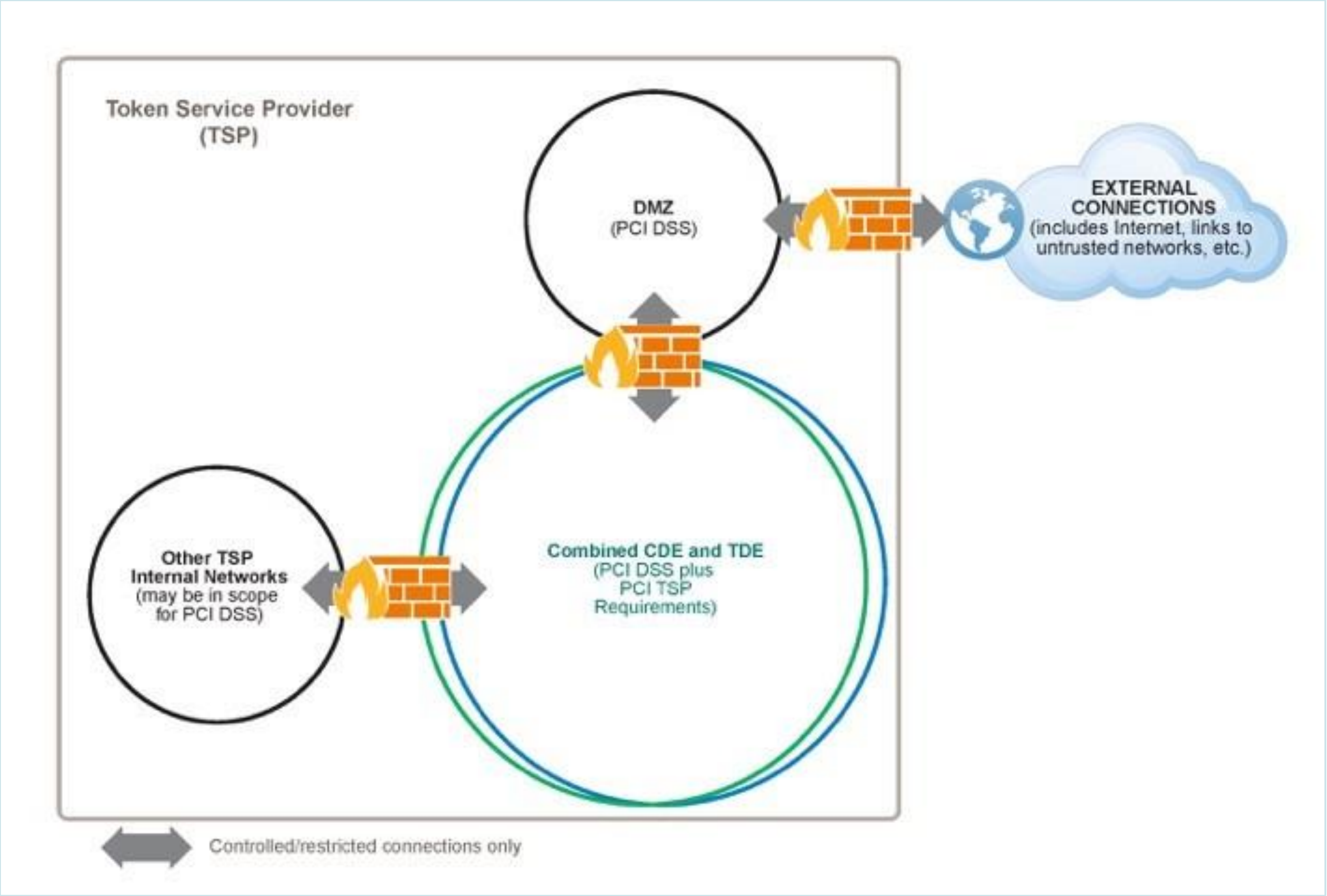

Token Service Provider (TSP)
DMZ (PCI DSS)
EXTERNAL CONNECTIONS (includes Internet, links to untrusted networks, etc.)
CDE (PCI DSS)
Other TSP Internal Networks (may be in scope for PCI DSS)
TDE (PCI DSS plus PCI TSP Requirements)
Controlled/restricted connections only

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.

PCI DSS Requirement	Additional Applicability for TSPs
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
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.

Summary of Additional TSP Requirements

For TSPs, the requirements in this document apply in addition to PCI DSS Requirements 1–12. These additional requirements are organized into the following control areas:

TSP 1 *– Document and validate PCI DSS scope*

TSP 2 *– Secure TDE Systems and Network*

TSP 3 *– Protect and manage cryptographic keys*

TSP 4 *– Restrict access to TDE by business need to know*

TSP 5 *– Identify and authenticate all access to TDE systems*

TSP 6 *– Restrict physical access to the TDE*

TSP 7 *– Monitor all access to TDE*

TSP 8 *– Maintain an Information Security Policy*

Additional Requirements for Token Service Providers

TSP 1. Document and validate PCI DSS scope

Requirements	Testing Procedures	Guidance
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	Accurate scoping of the environment ensures that applicable security controls are applied appropriately. Validation of scope for PCI DSS and these TSP Requirements should be performed as frequently as possible to ensure scope remains up to date and aligned with changing business objectives.
	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.	
TSP 1.1.2 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).	**TSP 1.1.2** 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.	Changes to systems or networks can have significant impact to scope. For example, firewall rule changes can bring whole network segments into scope, or new systems may be added to the CDE and/or TDE that have to be appropriately protected. Processes to determine the potential impact that changes to systems and networks may have on an entity's scope may be performed as part of a dedicated PCI compliance program, or may fall under an entity's over-arching compliance and/or governance program.

Requirements	Testing Procedures	Guidance
TSP 1.1.2.1 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.	**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.	It is important to have processes to analyze all changes made to ensure that all appropriate controls are applied to any systems or networks added to the in-scope environment due to a change. Building this validation into a change management process helps ensure that device inventories and configuration standards are kept up to date, and security controls are applied where needed. A change-management process should include supporting evidence that all requirements are implemented or preserved through the iterative process.
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.	An organization's structure and management define the requirements and protocol for effective and secure operations. Changes to this structure could have negative effects to existing controls and frameworks by reallocating or removing resources that once supported security controls or inheriting new responsibilities that may not have established controls in place. Therefore, it is important to revisit scope and controls for PCI DSS and these TSP Requirements when there are changes to ensure controls are in place and active.

Requirements	Testing Procedures	Guidance
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 1.1.4** 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.	If segmentation is used to isolate in-scope networks from out-of-scope networks, those segmentation controls must be verified using penetration testing to confirm they continue to operate as intended and effectively. Penetration-testing techniques should follow the existing penetration methodology as specified in PCI DSS Requirement 11. For additional information on effective penetration testing, refer to the PCI SSC's information supplement on *Penetration Testing Guidance*.
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	Mechanisms to detect and prevent unauthorized loss of clear-text PAN and Payment Tokens via unauthorized channels may include appropriate tools—such as data loss prevention (DLP) solutions—and/or manual processes and procedures. Coverage of the mechanisms should include, but not be limited to, e-mails, downloads to removable media, and output to printers. Use of these mechanisms allows an organization to detect and prevent situations where an unauthorized connection is being used to capture data. The exfiltration of Payment Tokens and other Payment Token Data via an unauthorized channel could be an indication that the tokenization service has been compromised.
	TSP 1.1.5.b Examine audit logs and alerts, and interview responsible personnel to verify that alerts are investigated.	

Requirements	Testing Procedures	Guidance
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	Attempts to remove clear-text PAN and/or Payment Tokens via an unauthorized channel, method, or process may indicate malicious intent to steal data, or be the actions of an authorized employee who is unaware of or simply not following the proper methods. Timely investigation of these occurrences can identify where remediation needs to be applied and provides valuable information to help understand where the threats are coming from. The result of such an investigation also helps determine whether a security compromise has occurred, and thus whether the organization's incident response procedures (per PCI DSS Requirement 12.10) need to be initiated.
	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.	

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.

Requirements	Testing Procedures	Guidance
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.	Performing non-tokenization functions or services on systems that also perform tokenization services can introduce additional risk to the tokenization services. For example, access to non-tokenization services increases the potential for unnecessary or unauthorized access to tokenization services running on the same system. The presence of non-tokenization functions may also introduce additional security weaknesses to the systems performing tokenization functions. Where the TSP has a business or technical justification for performing other functions on a TDE system—for example, authorization and transaction processing—the functions being performed must be managed in accordance with these TSP Requirements. Security functions for tokenization services, such as audit logging and monitoring controls, are considered to be supporting tokenization services.

Requirements	Testing Procedures	Guidance
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.	Defining a dedicated TDE and separating it from all non-TDE networks reduces the risk of a vulnerability being introduced to the TDE from another area of the TSP's network, such as back office (e.g., accounting, human resources, etc.) areas and any part of the TSP's network with internet connectivity. Systems within the TDE should be limited to those necessary for performing or supporting tokenization services—for example, systems that need to interact with the Token Vault in order to process token transactions. Systems that are not required for tokenization services should only be in the TDE if the TSP has a legitimate business or technical reason—for example, system interoperability or operational performance of transaction processing. All systems in the TDE, including any that are not dedicated to TDE services, are subject to the requirements in this document.
	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.	
	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.	
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.	Maintaining a documented architecture of the TDE includes identification and definition of all APIs exposed to networks other than the TDE. It's important that all exposed APIs are periodically reviewed and tested to ensure that they are functioning as intended. Use of industry best practices and guidance are recommended—for example, the OWASP REST (REpresentational State Transfer) Security Cheat Sheet provides best practices for REST-based services.
	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.	

Requirements	Testing Procedures	Guidance
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	Allowing virtual systems, such as virtual machines (VMs) and hypervisors, to span both TDE and non-TDE networks provides opportunities for malicious users to bypass network controls in order to gain access to TDE systems. Note that this requirement does not apply to virtual network components such as VRFs (Virtual Routing and Forwarding devices), and VDCs (Virtual Data Centers).
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 2.3.1.a** Review change control documentation to verify there is a process for backing up network devices prior to any changes of those devices.	Without properly documented and implemented change controls, security features on network devices could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced. Backing up network device data (such as configuration and database files, rule sets, router configuration tables etc.) prior to making changes to the device allows for the device to be restored back to its previous state in the event the change causes a failure or adversely affects device security.
	TSP 2.3.1.b Review procedures for back-ups and managing back-up media to verify media is securely stored and managed.	
TSP 2.4 Firewalls ***Note:*** *These requirements apply to firewalls protecting the TDE.*		
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.	If not protected from unauthorized access, firewall configuration documentation could be used by malicious individuals to identify gaps in firewall rule sets and gain entry to the TDE.

Requirements	Testing Procedures	Guidance
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, and verify that no connections are permitted between that system and any system outside the TDE.	Removing all unnecessary connectivity between TDE systems and non-TDE systems helps to minimize opportunities for attackers to leverage open connections in order to gain access to a TDE system.
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.	Any software that is not required to perform necessary firewall functions should be disabled or removed to reduce the risk of the device being compromised through software loaded on the firewall.
	TSP 2.4.3.b Examine firewall documentation and configurations to verify that all software not required for firewall functionality is deleted or disabled.	
2.4.4 Source routing must be disabled on firewalls.	**TSP 2.4.4** Examine firewall configurations to verify that source routing is disabled.	Source routing is a common attack vector used to identify communication routes between systems, which is why many firewalls have source routing disabled by default. This setting should be verified as disabled.
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	If remote access processes are not fully documented, access may be inadvertently granted to users or systems that should not have such access. Policies and operational procedures should be kept up to date so personnel understand the proper processes and to prevent unauthorized access to the network.
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.	Remote-access technologies are frequently used as "back doors" to critical resources. By limiting remote-access connections to only pre-determined and authorized locations, unnecessary access is minimized.

Requirements	Testing Procedures	Guidance
	TSP 2.5.2.b Examine remote access system configuration and access logs to verify access is accepted only from authorized locations and systems.	Defining authorized systems reduces the risk of an unknown or untrusted system gaining access to the network.
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.	Because personally owned devices can introduce risk to corporate systems, additional controls are necessary to ensure the remote device does not introduce a security vulnerability to a TDE system or put sensitive data at risk. An example of this may be where the VPN establishes a virtual desktop within the hardware (e.g., a virtual environment within the employee-owned device), and the TSP can prove that the security of that virtual environment is not impacted by anything on the employee-owned device.
	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.	
TSP 2.5.4 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.	**TSP 2.5.4** 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.	Access that originates from outside the TSP's network presents a higher risk, as the level of security implemented in those networks is unknown.
TSP 2.5.5 Remote changes must comply with PCI DSS change-management requirements.	**TSP 2.5.5** 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.	If change control procedures aren't followed for all changes, security features could be bypassed or omitted, unauthorized changes could occur, and the change could inadvertently introduce a security vulnerability to the environment.
TSP 2.5.6 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.	**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.	Periodic reviews of remote access privileges gives the organization an opportunity to identify and remove unneeded or incorrect access, and to ensure that only individuals with a current business need are granted remote access.

Requirements	Testing Procedures	Guidance
	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.	
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.	Multi-factor authentication is a practical and effective method to strengthen authentication to ensure only the authorized user is using the non-console or remote account.
	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.	
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.	If non-console (including remote) access does not use secure authentication and encrypted communications, sensitive administrative or operational level information can be revealed to an eavesdropper. A properly implemented VPN protects against malicious individuals utilizing unprotected connections to access critical systems and data.
	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.	

Requirements	Testing Procedures	Guidance
TSP 2.6 Access to HSMs		
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. **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 not otherwise subject to any commercial, financial, or other commitment that might influence their evaluation of the vendor's product.*	Because HSMs have high security needs, additional controls are necessary to restrict and protect logical access to these systems. If non-console access to HSMs is used, the security of the HSM non-console access solution is critical to the overall security of the HSM itself. An HSM non-console access solution is typically comprised of both hardware components (for example, network appliances, smart cards) and software components (for example, client-side applications) that define and manage how non-console access is handled.
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.	To ensure that non-console access to HSMs originates from a secure location, such access may only be provided to systems located within that TDE or another CDE/TDE under the control of the TSP.
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.*		

Requirements	Testing Procedures	Guidance
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.	Because these devices have network connectivity to an HSM, it's imperative that devices are being used as intended. If devices are left in unsecured locations they could be modified or tampered with in order to gain unauthorized access to the HSM.
	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.	
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 2.6.3.2.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.	Devices dedicated to performing HSM maintenance or administration functions do not need to be online when not in use. Securing these devices when they are not in use prevents malicious individuals from using the device to connect to the HSM.
	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.	
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.	Controlling physical access to devices prevents unauthorized personnel from getting close enough to modify or add anything onto the physical device.
	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.	
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.	If user authentication mechanisms are not properly secured, an attacker could gain authentication information or use the mechanisms to impersonate the authorized user.

Requirements	Testing Procedures	Guidance
	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.	
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.	Operation of non-console access devices must be strictly controlled to ensure they are used only for intended and approved purposes.
	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.	
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 defined and documented for devices with non-console access to HSMs.	Ensuring that only the necessary services and protocols are installed helps to prevent unnecessary software on the device from introducing vulnerabilities into the HSM environment.
	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.	
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.	The required security configurations for each device will depend on the particular device technology and function. For example, if a device does not have the applicable security patches installed before they are granted access to the TDE, vulnerabilities or exploits present on the device could be introduced into the environment.

Requirements	Testing Procedures	Guidance
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.	If the device's active network connections are not properly controlled, the device could provide a bridge between the HSM and another network, allowing a malicious individual to "piggy-back" on the authorized connection. To protect against "piggy-backing", devices should not be connected to any network other than the one being used to access the HSM. For example, connectivity on multi-homed devices should be disabled for all but the interface accessing the HSM, and any VPN/SSH tunnels to other networks should be closed before opening a tunnel to the HSM.
	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.	
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.	Methods to verify that only authorized devices are permitted to connect to the HSM can include digital signatures and other cryptographic techniques.
	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.	
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.	Controls to prevent man-in-the-middle attacks, such as binding of the device certificate upon the initial communication, protect the non-console connection against hijacking.
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.	Controls to prevent reply attacks, such as the use of random nonces, prevent attackers from being able to reuse data from the connection to initiate their own, unauthorized connection at a later time.
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.	Non-console access to HSMs should only be used for the purpose of HSM maintenance/administration. Because the loading and export of clear-text keys, key components and/or key shares requires a higher assurance of physical security, all such activities are required to be performed at the HSM.
	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.	

Requirements	Testing Procedures	Guidance
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.	If an administrator is not physically at the HSM console, additional controls may be necessary to ensure that all dual control and split knowledge responsibilities are adhered to.
	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.	
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.	A properly implemented VPN protects non-console connections to HSMs, preventing malicious individuals from gaining access to cryptographic keys and key-management data.
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 2.7.1** Examine system configuration settings to verify that strong cryptography is used for authentication and transmission.	Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.). Strong cryptography (as defined in the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms*) is based on an industry-tested and accepted algorithm (not a proprietary or "home-grown" algorithm) with strong cryptographic keys.
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.	If mechanisms are not implemented to detect unauthorized changes to communication controls, a malicious individual could add, remove, or alter configuration settings without detection. This could potentially render security controls ineffective and allow an attacker to gain access to tokenization services without impact to regular processing.
	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.	
	TSP 2.7.2.c Examine audit logs and alerts, and interview responsible personnel to verify that alerts are investigated.	

Requirements	Testing Procedures	Guidance
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.	Multi-factor authentication requires at least two different forms of authentication for higher-risk access. Requiring a second authentication factor helps to reduce the risk of a compromised credential being used to gain unauthorized access to networks and systems. Once the multi-factor authentication process is complete and access granted, additional multi-factor authentication is not required for access to individual systems or applications in the TDE.
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.	Without account-lockout mechanisms in place, an attacker can continually attempt to guess a password through manual or automated tools (for example, password cracking), until they achieve success and gain access via a legitimate user's account.
	TSP 2.7.4.b Review audit logs to verify that access is declined after not more than three consecutive unsuccessful access attempts.	
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.	If a user account is locked out due to multiple failed access attempts, controls to delay reactivation of the locked account stops a malicious individual from continuing to guess the credentials. Additionally, requiring independent validation from an authorized individual provides assurance that it is the actual account owner requesting reactivation of their account.
	TSP 2.7.5.b Review user IDs authorized with reset privileges and interview personnel to verify that authority for resets is appropriately assigned.	
	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.	
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.	Audit logs provide the ability to detect suspicious activity. Thus, it is imperative that remote access solutions be configured to generate audit logs and that these logs be regularly reviewed to identify potentially suspicious access activity.
	TSP 2.7.6.b Review documented procedures and interview personnel to verify access logs are reviewed at least weekly to identify suspicious activity	

Requirements	Testing Procedures	Guidance
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 2.7.7** 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.	When properly configured, IPSec VPNs can provide strong security for communications by protecting against eavesdropping, replay attacks, man-in-the-middle attacks, and denial of service attacks. However, if not appropriately configured, the security capabilities provided by an IPsec VPN could be impaired, resulting in a potentially vulnerable implementation. A trusted CA is typically a third party that utilizes a chain of trust model to provide assurance for a particular certificate. If an internal CA is used (where the TSP is using self-signed certificates) the internal CA also needs to be verified as meeting industry requirements, such as TS101456.

Requirements	Testing Procedures	Guidance
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.	Exploitation of wireless technology is a common path for malicious users to gain access to the network and sensitive data. Attackers often target wireless devices or networks via rogue applications, endpoint attacks, and phishing attacks in order to gain access to the wireless device or network. If connections between the TDE and wireless networks are not prohibited, malicious individuals that gain access to the wireless network can use this to connect to the TDE and compromise tokenization services. Because wireless-enabled systems could be used as a bridge to the TDE, wireless capability needs to be disabled on systems that are used to access the TDE, prior to and at all times during the access period. Systems with wireless capability that are used to access the TDE must disable the wireless capability prior to and at all times when connected to the TDE.
	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.	
	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.	
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.	Unauthorized wireless devices may be hidden within or attached to a computer or other system component, or be attached directly to a network port or network device, such as a switch or router. Any such unauthorized device could result in an unauthorized access point into the environment. Scanning should identify any wireless transmissions originating from within the TDE to prevent unauthorized data leakage or access.
	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.	

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.

Requirements	Testing Procedures	Guidance
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.	Cryptographic keys must be stored and functions handled securely to prevent unauthorized or unnecessary access that could result in the exposure of keys and compromise cardholder data. Key-management activities typically include all token encryption/decryption operations, such as encryption/decryption of mapping references, as well as key lifecycle functions such as key generation and storage.
	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: • 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."	
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.	The manner in which cryptographic keys are managed is a critical part of the continued security of the encryption.

Requirements	Testing Procedures	Guidance
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 3.1.3** 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	Cryptographic keys exists in clear-text within these devices and so they have to be stored securely and be used only when there is a valid business need. When not in use, powering the device down and not connecting it to the network will help prevent unauthorized access.
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.*	Annex A includes the Minimum Key Sizes and Equivalent Key Strengths for Approved Algorithms. Use of strong cryptographic keys significantly increases the security of encrypted Payment Tokens and cardholder data.
	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.*	
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	Encryption is only as strong as the weakest key used in the cryptographic operation, If the KEK is weak, then the encryption key can be compromised and hence the token and card data will be left unprotected.
	TSP 3.1.5.b Observe key-management operations and devices 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	
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.	If cryptographic keys are embedded into software, a malicious user could gain access to the code and retrieve the keys. Once compromised, the key could be used to decrypt all Payment Token and cardholder data that it was protecting.
	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.	

Requirements	Testing Procedures	Guidance
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.	**TSP3.1.7.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.	Ensuring that critical functions are conducted by personnel who are accountable to the organization provides the necessary oversight of responsibility assignments for the security of the data.
	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.	
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.	Personnel who perform the various key-management activities need to understand what steps to take and why. If not, they can inadvertently leak critical data or cause operational impact. The training should cover various key-management activities as applicable to the role performed.
	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.	
	TSP 3.1.8.c Interview responsible personnel to ensure they have undergone relevant training for the key-management functions they perform.	
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.	The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Recording the function or key-management activity being performed (for example, key loading), and the purpose of the affected key (for example, PAN encryption) provides the TSP with a complete and concise record of key-management activities. Identifying whether the activity resulted in success or failure confirms the status upon conclusion of the activity. By recording these details for the auditable events a potential compromise can be quickly identified, with sufficient detail to know who, what, where, when, and how.
	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 performed • Purpose • Success or Failure of activity	

Requirements	Testing Procedures	Guidance
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.	Cryptographic keys must be strongly protected to prevent unauthorized or unnecessary access that could result in the exposure of encrypted data.
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. ii. 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: 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.	The principles of split knowledge and dual control must be included in all key life cycle activities involving key components to ensure protection of keys. Effective implementation of these principles does not rely on users following procedures; additional controls such as automated processes, physical barriers, and hardware controls that physically separate access to key components are required to prevent any one individual from being able to recreate an actual key. The only exceptions to these principles are where keys are managed as cryptograms or stored within an SCD.
	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.	

Requirements	Testing Procedures	Guidance
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 • With an associated MAC (message authentication code) created using the algorithm defined in ISO 16609.	Public keys are used to encrypt data that only the TSP with the corresponding private key can decrypt. If the public key is not secured, it can be spoofed to send unauthorized messages to the TSP. A trusted CA is typically a third party that utilizes a chain of trust model to provide assurance for a particular certificate. If an internal CA is used, the internal CA also needs to be verified as meeting industry requirements, such as TS101456.
	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.	
TSP 3.3 Key-Management Security Administration ***Note:*** *These requirements relate to the procedures and activities for managing keys and key sets*		
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**.**	When the key-management responsibilities are transferred, it is critical that the newly responsible individual is aware of the applicable procedures and controls. The secure administration of all key-management activity plays an important role in terms of logical security.
	TSP 3.3.1.b Interview responsible personnel in applicable key-management roles to verify they are aware of and following the documented procedures.	

Requirements	Testing Procedures	Guidance
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.	Examples of devices often used to control access to HSMs and other equipment include physical keys, authentication codes, smart cards, and other device enablers. Dual control can be applied at the equipment level or the device enabler level. For example: • Two keys or smart cards are required to access or initiate the equipment. Each key/card is assigned to a separate individual, and no one individual has access to both keys/cards. • Only one key or smart card is required to access or initiate the equipment. Access to and use of this key or card requires at least two individuals. Physical keys, authorization codes, passwords, and other enablers must be managed so that no one person can use both the enabler(s) and the equipment for which it is intended, as this would result in a single individual being able to perform key-management functions.
	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.	

Requirements	Testing Procedures	Guidance
TSP 3.3.3 Key Managers must be designated and managed as follows.		
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.	The Key Manager plays a critical function to safeguard Payment Token and cardholder data and it is essential that they are nominated by the highest ranking authority for security, It is critical that there are well defined processes and a plan in place for contingency in case the primary is unable to perform their job
	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.	
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.	It is critical that the Key Manager is notified immediately of any breach impacting the keys. If the Key Manager is not available, then their back-up should be notified. Documented procedures should explain how this issue would be escalated for further investigation and resolution, including initiation of the organization's incident response procedures (per PCI DSS Requirement 12.10) in the event of a compromise.

Requirements	Testing Procedures	Guidance
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.	Being accountable for key custodian training and acknowledgement provides the Key Manager with assurance that the custodians can fulfill their role effectively and securely. The organizational hierarchy also plays a role in ensuring that no single Key Manager controls, either directly or via their key custodians, sufficient key components to form a threshold to create a key. Key custodians are responsible for the day-to-day functions involving the keys. It is critical that they are aware of their responsibilities and obligations and is able to fulfill it based on documented processes. The custodians should be appropriately trained for their job and the organization hierarchy should not encourage collusion.
	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.	
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 3.3.3.4** 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.	The Key Manager function should be distinct from the key custodian's function. The Key Manager should not have the access to carry out key-management functions as another key custodian, thereby circumventing the dual control rule.

Requirements	Testing Procedures	Guidance
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.	An individual must not be assigned as a back-up custodian for more than one primary key custodian, as this would circumvent key threshold and dual control principles.
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.	Clearly documenting the steps performed by key custodians for various key-management functions provides primary and back-up custodians the information they need to correctly carry out the procedures.
	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.	
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.	Similar to access controls, the suitability of key custodians and their back-ups must be reviewed annually. As organizational and role changes can impact the reporting structures, care must be taken to ensure that principles outlined in TSP 3.3.3.3 and TSP 3.3.4.1 are met at all times.
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.	As key custodians perform critical and time sensitive functions, it is necessary for them and their back-ups to be available at all times and adhere to a higher code of conduct.

Requirements	Testing Procedures	Guidance
	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.	
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 responsibilities for safeguarding key components, shares, or other keying materials entrusted to them.	As the key custodians perform critical and sensitive functions, they need to adhere to a higher code of conduct. A formal acknowledgment helps ensure key custodians have read and understood their responsibilities, and have made a commitment to protect the sensitive data.
	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.	
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.	Access to the key-management devices is further restricted by use of a PIN or a passphrase. If this value were not strong, or not stored securely, a fraudster would be able to guess this and use it to get cryptographic materials.
	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.	
	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.	
TSP 3.4 Key Generation		

Requirements	Testing Procedures	Guidance
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.	Use of a random or pseudo-random process is intended to ensure keys are generated so that it is not feasible to determine that certain keys are more probable than other keys from the set of all possible keys. This can be met by using an approved key-generation function of a PCI–approved HSM, or an approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM. Satisfying the NIST statistical tests, or equivalent industry tests, ensures adequate randomness of the keys and key components during their generation.
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 or higher certification for physical security	A hardware security module (HSM) that has been approved to rigorous industry standards is acceptable to use for key generation.
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.	*Annex A* includes the Minimum Key Sizes and Equivalent Key Strengths for Approved Algorithms. Use of strong cryptographic algorithms and keys significantly increases the security of encrypted Payment Tokens and cardholder data.
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 3.4.4** 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.	Cables that have been tampered with may expose clear-text keys or key components/shares to disclosure via wiretapping.

Requirements	Testing Procedures	Guidance
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.	Separating individual key components/shares to specific individuals ensures that no one individual can create an entire key.
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.	Key components that are generated on paper must be only known to the authorized key custodian to ensure confidentiality.
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.	Residue from a paper generated key component can potentially allow for re-creation of that key component.
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.	Any generated key must not be accessible in clear-text to any individual to ensure that no one individual can have access to that key.
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.	The use of pre-serialized, tamper-evident envelopes to hold the key components/shares protects from any physical tampering of the key components/shares inside.
	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.	

Requirements	Testing Procedures	Guidance
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 3.4.10** 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.	Minimum requirements for generated asymmetric keys ensure they meet the definition of strong cryptography.
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.	Keys not in their allowable forms are at risk of exposure or may already have been tampered with.
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.	If intercepted during electronic transmission, clear-text keys and key components/shares lose their confidentiality.
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.	**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.	When transmitting paper-based key components/shares, additional steps must be taken to ensure their confidentiality.

Requirements	Testing Procedures	Guidance
iv. Key components or shares must be placed in pre-serialized, tamper-evident envelopes for shipment.	**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.	
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.	Performing a physical inspection of the key components/shares received by the authorized key custodian ensures they haven't been tampered with during shipping.
	TSP 3.5.4.b Observe the authorized custodian perform the items in 3.5.4.a above to verify all steps are followed.	
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.	Knowing who sent the certificate and its status prior to accepting it ensures its validity in preparation for key loading.
	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**.**	

Requirements	Testing Procedures	Guidance
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.	Having a controlled environment with dual control of the key loading function ensures only the appropriate keys are the ones used in the key loading process.
	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.	
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.	If the target cryptographic devices, cabling and paper components have been tampered with, the keys or its components/shares can be exposed in the loading process.
	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.	
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 3.6.3** 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.	If the key/key component/key share-holding mechanism falls in possession of someone other than the designated custodian or his/her back-up, those key components/shares are considered compromised.

Requirements	Testing Procedures	Guidance
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.	Using a device that is not a secure cryptographic device to perform the key transfer from one device to another weakens the integrity of that key transfer.
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.	The Key Manager is the one ultimately responsible for the key loading process; therefore all such activities must be under his/her control. Key custodians performing key-loading tasks must be authorized by the Key Manager.
	TSP 3.6.5.b Observe key loading activities to verify that all such activities are under control of the Key Manager.	
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.	Dual control for the loading of key components/shares contained in a holding device is imperative so that no one individual can perform key loading.
	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.	
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.	When performing key loading, any disclosure of one individual's key component/share to another party (particularly the individual sharing dual control) can potentially lead to another individual to have a complete set of key components/shares to perform key loading.

Requirements	Testing Procedures	Guidance
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.	To ensure key components/shares are accessible in human-readable form for the minimum possible time, they should be returned to a non-human-readable state immediately upon completion of loading.
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.	Without validating the authenticity of the keys or key components/shares, it is difficult to ascertain if the keys or key components/shares have been manipulated in some way prior to key loading.
	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.	

Requirements	Testing Procedures	Guidance
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.	Key components/shares that have been loaded and confirmed to be operational are no longer needed in the key-loading device. If the key and/or key components/shares will not be used for future key loading, they should be securely destroyed.
	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.	
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: • 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.	Storing the key components/shares in secure locations such as safes, with any removal being identified, protects against unauthorized removal of the components/shares.
	TSP 3.7.1.b Observe the envelopes used to verify that they are pre-serialized and tamper-evident.	
	TSP 3.7.1.c Observe storage locations to verify the envelopes are stored in separate, secure locations and cannot be removed without detection.	

Requirements	Testing Procedures	Guidance
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.	Maintaining and auditing the inventory listing of the key components/shares contained in the safes ensures proper accounting of their location.
	TSP 3.7.2.b Examine inventory and audit documentation to verify inventory is complete and audits are performed at least quarterly.	
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.	Limiting possession of both the storage media and its access code solely to the designated key custodian (or his/her back-up) ensures no other party can have access to the secret or private key component/share on that media.
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.	The contents of the logs for access to the key components/shares must be able to document the details of any such access for investigative purposes in the event that any key component/share is compromised.
	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)	
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.	If the master key protecting keys is compromised, then those keys are subject to the same compromise.

Requirements	Testing Procedures	Guidance
TSP 3.8 Key Usage		
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	The more a key is used, the greater the opportunity for its compromise or abuse. Using separate key pairs for signing and encryption operations reduces the risk and potential impact if a key pair is compromised. For example, if a private encryption key is recovered it could be used to decrypt information encrypted with the public encryption key, but it cannot be used to sign information. Symmetric keys form a hierarchy that is linked to the value of the information enciphered by the key and the controls in place to change the key. Key encrypting keys are used to encipher working keys whereas working keys typically encipher data. The data enciphered by a key-encryption key has potentially more value than the data enciphered by a working key. In addition, working keys are typically enciphering greater volumes of data than key-encryption keys. This potentially makes them more vulnerable to brute force attacks. Thus they tend to have a shorter crypto period. Using a key-encrypting key in this way exposes it to the same vulnerability and if a key-encrypting key is compromised the collateral damage is potentially greater because many working keys will be exposed together with the data they protect.
	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.	

Requirements	Testing Procedures	Guidance
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.	**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	The more frequently a key is used, the greater the opportunity for its compromise or abuse. If the same key is used over a number of different key zones this means that, for example: • All parties sharing the key can decipher content including content that may be confidential to a specific zone. • Insecure key-management practices by one entity results in the exposure of content over all entities. • A malicious entity with the shared key can inject a message into another zone and there will be no cryptographic mechanism to prove the zone origin of the message.
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.	If the HSM does not enforce key separation it may be possible for a malicious user with access to the HSM API to use a key that has been established for one purpose and abuse it in another; for example, to decipher a token or a key used to generate a token.
	TSP 3.8.3b Observe HSM settings and configurations to verify they enforce a separation of keys.	
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.	Where an issuer provides keys to the TSP with a defined expiry date, the issuer has determined the length of time for which that key can be used. Ensuring that the defined usage period is adhered to supports the cryptographic needs of both the TSP and the issuer. If an issuer provides a key without a defined expiry date for that key, the TSP should consider the key to be valid until the issuer withdraws the key or advises of its expiry.
	TSP 3.8.4b Observe issuer keys currently in use to verify they are within the issuer-specified expiry date.	

Requirements	Testing Procedures	Guidance
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.	The cryptoperiod defines the duration of time that the key may be used. For keys used to encrypt/decrypt account data, this is typically defined as either a maximum threshold of transactions, or hours, or both—for example, 1024 transactions or 24 hours, whichever is reached first. Upon reaching the defined usage threshold, the key is retired and no longer used. Considerations for defining the cryptoperiod include, but are not limited to, the strength of the underlying algorithm, size or length of the key, risk of key compromise, and the sensitivity of the data being encrypted. There are a number of industry standards that provide references for key usage timeframes, including the following (not all-inclusive): • European Payments Council EPC342-08 Guidelines on Algorithms Usage and Key Management • ISO 11568, Banking - Key management (retail), Parts 1, 2 and 4 • ISO 13491-1, "Banking - Secure cryptographic devices (retail), Parts 1 and 2 • NIST SP 800-57 Recommendation for Key Management, Part 1
	TSP 3.8.5.b Observe keys currently in use to verify they have not exceeded their defined cryptoperiod.	

Requirements	Testing Procedures	Guidance
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.	Non-production keys are typically not subject to the same level of key-management controls as production keys—for example, they are often not generated using a suitable random generation process. Also, it is potentially easier for unauthorized individuals to access these keys; they are sometimes even published.
	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.	
	TSP 3.8.6.c Observe processes for generating and loading keys into test systems to verify they have no association with production keys.	
	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.	
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 3.8.7.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.	If the key is left indefinitely then eventually sufficient time will elapse for an exhaustive key search to be performed successfully.
	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.	
	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.	

Requirements	Testing Procedures	Guidance
	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.	
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.	The more a key is used, the greater the opportunity for its compromise or abuse. This includes the number of locations where that key is stored as each is a potential target for a breach.
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.	Some HSMs do not encipher keys under a master file key but use a key variant. A key variant is created by combining (typically using XOR) a key with a known control vector to obtain another key. The security of this process relies on the generation of the key variant remaining within the physical protection of the HSM.
	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.	
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.	It is an essential part of key management to keep account of the whereabouts and status of all keys in use or ever used by the system. A lost key will mean that all information protected by that key is potentially compromised.
	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	
	TSP 3.8.10.c Interview personnel to verify that key-inventory procedures are known and followed.	

Requirements	Testing Procedures	Guidance
TSP 3.8.11 All derivation keys must be unique per issuer.	**TSP 3.8.11** Examine key-management documentation and interview personnel to verify that all derivation keys are unique per issuer.	Ensuring that derivation keys are unique for each issuer limits the usage of that key to the necessary functions for that entity. This also avoids the potential for a key intended to protect one entity's data being used by another entity to capture that data.
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.	Integrated Chip (IC) keys must be unique for the particular chip it is intended for in order to prevent that key being used to capture data from multiple cards.
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.	Key back-up and recovery are important procedures that should be documented as part of any disaster recovery plan. If not implemented there will be impact on business recovery until new keys can be established.
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.	Dual control requires two or more people to perform a function where no single person can access or use the authentication credentials of another person. Key recovery is a sensitive procedure as it can be used to recover a production key. Dual controls mitigate risk of this abuse by eliminating the possibility of one person being able to perform this operation. Dual controls are applicable for manual key-management operations, or where key management is not implemented by the encryption product.
	TSP 3.9.2.b Interview appropriate personnel.	

Requirements	Testing Procedures	Guidance
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	It should be just as difficult for fraudsters to compromise production keys as back-up keys.
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.	A device with an undiagnosed failure should be regarded as being in an insecure state by default. For example, it may have failed as part of a deliberate act to compromise the keys.
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.	The Information Security Policy should be consistently applied to ensure that it is equally difficult to compromise the processes associated with back-up keys as production keys.
TSP 3.9.6 All access to back-up storage locations must be witnessed and logged under dual control.	**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.	Access to back-up storage is a sensitive procedure as it can be used to recover a production key. Dual controls mitigate risk of this abuse by eliminating the possibility of one person being able to access these back-up locations.

Requirements	Testing Procedures	Guidance
TSP 3.10 Key Destruction ***Note:*** *These requirements relate to the destruction of keys, components, and shares.*		
TSP 33.10.1 Immediately destroy key components/shares that are no longer required after successful loading and validation as operational.	**TSP 3.10.1.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.	Once a key has been loaded onto its intended device, destroying copies of the key and its components/shares from all previous storage locations and loading devices avoids having unnecessary data in the environment that could be used to recreate the key outside of its intended device.
	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.	
	TSP 3.10.1.c Review storage locations for key components/shares that have been loaded to verify they are no longer present.	
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 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.	If steps are not taken to destroy information contained within a cryptographic device prior to disposal, malicious individuals may be able to retrieve information from the disposed media, leading to a data compromise at a later stage. Such devices may be sold on after decommissioning, after which time it becomes very difficult to keep track of their whereabouts and whether or not their keys have been recovered by fraudsters.
	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.	
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.	Securely destroying all copies of keys as soon as they are no longer needed ensures that only necessary keys are retained, and provides assurance that malicious individuals cannot retrieve old keying information and potentially gain information about current key sets.
	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.	
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.	Retaining logs of key destruction activities provides a trusted record of which keys were destroyed, and when.

Requirements	Testing Procedures	Guidance
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.	If steps are not taken to destroy information contained on hard disks, portable drives, CD/DVDs, or paper prior to disposal, malicious individuals may be able to retrieve information from the disposed media, leading to a data compromise. For example, malicious individuals may use a technique known as "dumpster diving," where they search through trashcans and recycle bins looking for information they can use to launch an attack.
	TSP 3.10.5.b Observe key-destruction processes to verify that no part of the key or component can be recovered.	
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.	To ensure that malicious individuals cannot retrieve keying information from a disposed device, the device itself may need to be physically destroyed in a manner that prevents any data from being recovered.
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.	Techniques such as crosscut shredding, incineration, and pulping are needed to provide reasonable assurance that data from hard-copy materials cannot be reconstructed.
	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.	
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.	Anything less robust than these procedures may enable an attacker to recover the data from the discarded electronic media.

Requirements	Testing Procedures	Guidance
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.	Dual control requires two or more people to perform a function where no single person can access or use the authentication credentials of another person. Key destruction is a sensitive procedure. If not performed and recorded with some level of assurance a production key may persist indefinitely without detection. Dual control is used to eliminate the possibility of one person managing this sensitive process.
	TSP 3.10.9.b Interview personnel and observe demonstration of processes for removing keys from service to verify that dual control is implemented.	
	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.	
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.	Using an individual who is not a key custodian mitigates any potential abuse of the process through internal reporting hierarchies. Having a written sworn statement, such as an affidavit, provides a legally-binding attestation that the expected process was witnessed to have been completed.
	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.	
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)	Sufficient information should be required to ensure all details of the event are recorded to support investigation or to allow the event to be recreated.
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 must be retained for the life span of the key(s) to which they relate.	Retaining logs for the life span of the applicable key(s) allows investigators sufficient log history to better determine the potential impact of a lost or compromised key.

Requirements	Testing Procedures	Guidance
	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.	
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.	Adequate protection of the audit logs includes strong access controls that limit access to only authorized individuals, such as the Key Manager and any other personnel with a justifiable business need.
	TSP 3.11.3.b Verify through observation that access to key-management logs is only permitted to authorized individuals.	
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.	Resetting the sequence number generator or other mechanisms, such as the time and date stamps in the HSM, is a technique used by attackers to hide gaps in audit logs.
	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.	
TSP 3.11.5 The CISO (or equivalent) or an authorized individual must investigate all audit log validation failures.	**TSP 3.11.5** Review documented procedures and interview personnel to verify the CISO (or equivalent) investigates all audit log validation failures.	If the audit/logging system generates a validation failure, a senior individual can provide an objective analysis of what caused the failure.
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.	Protecting audit logs from accidental or deliberate deletion is critical to ensure logs are available when needed, to confirm actions performed and support investigation procedures. Audit logs should only be deleted when their retention is no longer required—for example; key-management logs must not be deleted prior to the related key's end-of-life. Deletion of logs should be performed by an authorized individual and process.
	TSP 3.11.6.b Examine system configurations to verify controls are implemented to prevent unauthorized deletion of audit trails.	

Requirements	Testing Procedures	Guidance
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: i. 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. ii. 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. iii. An investigation into the cause of the compromise, including a documented analysis of how and why the event occurred and the damages suffered. iv. The removal from operational use of all compromised keys within a predefined time frame and a means of migrating to new key(s). v. Where keys are issuer-owned, the issuer must be notified immediately for further instruction.	**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.	Implementing defined procedures to be followed in the event of a known or suspected key compromise enables the entity to identify, contain, and recover from the compromise as quickly and efficiently as possible. Such procedures are focused on minimizing the impact of fraudulent activities and the potential impact to the business. Timely and appropriate communications to affected parties minimizes the potential for negative impact beyond the entity's own usage of the compromised key.
	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.	
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.	To ensure the impact of a compromised key is limited to its usage at the time of the compromise, the replacement key must be a new key that is generated independently of the compromised key.

Requirements	Testing Procedures	Guidance
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.	A quick response that includes initiation of key-replacement procedures minimizes the potential impact if a key has been compromised.
	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.	
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.	Potentially compromised keys cannot be relied upon or used until it is verified, one way or the other, if the key is actually compromised. If compromise is confirmed, immediate replacement of the key is necessary to prevent further loss of data.
	TSP 3.12.4.b Verify through interviews that procedures are understood and communicated to affected personnel.	
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.	Keys that are protected by a potentially compromised KEK are also potentially compromised.
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.	Compromise of a key-encrypting key results in the compromise of all keys being protected by that key, rendering all such keys unusable.
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 all keys derived from that MDK are replaced.	The compromise of a MDK renders all keys derived from that MDK as compromised.
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.	The impact of a potential key compromise to the organization is significant and requires escalation to the senior security role as soon as possible.
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 that has been revoked are withdrawn as soon as possible and replaced.	Data that is protected by a compromised key is no longer secure. Timely replacement using the new key helps minimize the window within which the data could be compromised.

Requirements	Testing Procedures	Guidance
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).	Physical keys or other mechanisms that are used to enable otherwise restricted commands on the HSM should only be present under the control of authorized operators when performing such restricted commands.
	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).	
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.	The integrity of HSM is paramount to the security of the entire key hierarchy. If an unauthorized person gained access to the HSM prior to it being brought into service, they could modify its hardware and software, and tamper with the built-in protection measures.
	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.	

Requirements	Testing Procedures	Guidance
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.	Installation logs are a critical component of HSM lifecycle records. Retaining records for at least six months after all applicable keys are retired ensures that records are available for a reasonable time if needed for an investigation.
	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	
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.	Whatever methods are used, they must prevent the possibility of disclosure of any secret data or keys during HSM repair.
	TSP 3.13.4.b Observe demonstration of processes for removing HSMs from service to verify all operational keys are deleted from the device.	
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.	Removal logs are a critical component of HSM lifecycle records. Retaining records for at least six months after all applicable keys are retired ensures that records are available for a reasonable time if needed for an investigation.

Requirements	Testing Procedures	Guidance
	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 the HSM and any keys generated or protected by the HSM.	
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.	Whenever a HSM is in use or being accessed by a human operator, dual control is required to ensure that no one individual can perform key-management functions.

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

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

Requirements	Testing Procedures	Guidance
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.	The more people who have access to cardholder data, Payment Tokens, and Payment Token Data in the TDE, the more risk this data could be used maliciously. Limiting access to those with a legitimate business reason for the access helps an organization prevent mishandling of the data through inexperience or malice.
	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.	
	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.	
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.	Access requirements evolve over time as individuals change roles or leave the company, and as job functions change. Management needs to regularly review, revalidate, and update user access, as necessary, to reflect changes in personnel, including third parties, and users' job functions.

TSP 5. Identify and authenticate all access to TDE systems

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

Requirements	Testing Procedures	Guidance
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. **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.	Administrative access, also known as privileged access or "superuser" access has the ability to perform all functions on a system and very often can control or override existing security controls. Therefore it is important that the credentials associated with these accounts to gain access to high value token data environments are protected and used only by the authorized user. Multi-factor authentication is a practical and effective method to strengthen authentication to ensure only the authorized user is logging on to the administrative account.
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.	First use passwords should be changed promptly with the new user choosing their own strong, confidential password as soon as possible. If a temporary first use password is left active, it could be used by a malicious user to gain access under the guise of the new user.
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 – Special characters	Strong passwords/phrases are the first line of defense into a network since a malicious individual will often first try to find accounts with weak or non-existent passwords. If passwords are short or simple to guess, it is relatively easy for a malicious individual to find these weak accounts and compromise a network under the guise of a valid user ID. For passwords that are used to access particularly sensitive functions or data, a greater level of strength and complexity than this requirement may be appropriate.

Requirements	Testing Procedures	Guidance
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.	If the opportunity presents itself, a malicious individual will often first try to observe a password or passphrase being entered.
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.	Passwords/phrases that are valid for a long time without a change provide malicious individuals with more time to work on breaking the password/phrase. Defining a minimum active period for a new password prevents users from "cycling" through their allowance of previously used passwords in an attempt to keep their password unchanged.
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 5.3.1.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.	Without account-lockout mechanisms in place, an attacker can continually attempt to guess a password through manual or automated tools (for example, password cracking), until they achieve success and gain access to a user's account. Validating the identity of users requesting password resets ensures that a reset password, and the account access it provides, is not given to an unauthorized individual.
	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.	
	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.	

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.

Requirements	Testing Procedures	Guidance
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.	A clear line of sight allows for an unobstructed view of the perimeter and adjacent terrain to ensure that all persons approaching facility entrances are observed. This is achieved by implementing a “clear zone” between perimeter barriers and exterior structures, parking areas, natural features, etc. For example, parking immediately adjacent to a facility should be restricted, and shrubbery kept to a minimum near doors, windows, fence lines, gates, and access roads to reduce risk of obscuring surveillance. In addition to CCTV surveillance, security staff that routinely patrol perimeter barriers may provide greater assurance.
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.	Solid construction is critical to protect against physical breaches. A malicious user could take advantage of structural weaknesses in order to bypass the controlled entrances and gain unauthorized entry.
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 6.1.3.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.	Perimeter door security requirements may be implemented at different levels depending on building structure and occupancy. For example, at a dedicated, standalone facility the controls are implemented at the exterior of the building, whereas in a multi-tenant building (where the tenant cannot control exterior doors or building-level controls), controls are implemented at the perimeter of TSP’s space within the building.
	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.	

Requirements	Testing Procedures	Guidance
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.	Multi-tenant buildings introduce additional risk due to shared walls, floors and ceilings, thus controls need to be established to prevent access through common or shared constructs. Floor-to-ceiling, wall-to-wall construction (sometimes referred to as slab-to-slab construction) prevents attackers using false ceilings and/or raised floors to gain covert physical access to the TDE.
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.	Emergency exit doors are an absolute necessity for any building structure to protect human life in the event of an emergency. If not properly managed, these exit points could be leveraged by an attacker to gain unauthorized entry into a secure area.
	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.	
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 personnel permitted to access the TDE are approved by Security Manager.	As the individual responsible for the overall security of the TDE, the Security Manager should be aware of and approve all access requests to the TDE, including personnel, third parties and visitors.

Requirements	Testing Procedures	Guidance
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	A positively controlled mantrap is typically a small room with an entry door on one wall and an exit door on the opposite wall. One door of a mantrap cannot be unlocked and opened until the opposite door has been closed and locked. Access controls can be a combination of automated (for example, electronic access cards and physical barriers) and manual (for example, a human security guard performing visual verification and confirmation of identity). These controls ensure that the second door is not opened until authentication is complete, and that only one individual is provided access per authentication.
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.	Identifying individuals physically entering and exiting the sensitive area provides valuable information in the event of an investigation.
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.	Electronic access control systems, such as a keypad with individually assigned PIN codes, or individually assigned access cards, provide assurance that the individual gaining access is who they claim to be.
	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.	
TSP 6.2.5 Multi-factor authentication is required for entry to the TDE and telecommunications rooms.	**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	Examples of multi-factor authentication include use of an access card with PIN/passcode, and use of an access card with a biometric reader. Visual verification of government-issued photo ID by an authorized guard at the entry point is also acceptable as one of the two factors.

Requirements	Testing Procedures	Guidance
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.	**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	These controls provide assurance that the identity of every individual in the TDE is known at any given time.
TSP 6.2.7 A physical intrusion-detection system that is connected to the alarm system must be in place for the TDE.	**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.	To be effective, an intrusion-detection system should be activated whenever the TDE is intended to be unoccupied. The intrusion-detection system may be activated automatically (for example, motion detectors are automatically activated when all authorized personnel have exited the TDE), or via manual process.
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.	Physical access to HSMs requires passing an additional physical control—e.g., via locked cabinets or cages, or a separate secure room. HSMs could be in multiple racks within the same dedicated physical space, or in one or more dedicated rooms, and so on. Whether one or many, each dedicated HSM space must be physically separate from non-TDE systems.
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.	Securing networking and communications hardware prevents malicious users from intercepting network traffic or physically connecting their own devices to wired network resources.

Requirements	Testing Procedures	Guidance
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.	If not sized appropriately or fitted with controls to prevent covert access, conduit openings can be used by attackers to bypass the approved access mechanisms and gain access to the TDE.
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.	Low light level CCTV cameras and/or artificial lighting may be required to ensure recognizable images are captured at all times of day. Periodic testing of camera functionality verifies that the "live" feed being captured is actually a live and accurate image of the environment, and that correct time-stamps are being assigned to the images. Testing activities may utilize both automated and manual methods—for example, system checks to confirm camera zoom/pan functions are working together combined with human verification that the picture images are sufficiently clear to allow identification of individuals.
	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.	

Requirements	Testing Procedures	Guidance
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.	Adequate lighting at all times is necessary to ensure effectiveness of CCTV monitoring.
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.	Cameras within the TDE can be set to record continually, or be activated via motion sensors or upon use of an access point to ensure they are monitoring the TDE at any time someone is present. The combined camera views must include all activities necessary to provide complete coverage of the TDE physical area. Blind spots are areas outside of the CCTV cameras' combined viewing area or that are obstructed from the cameras' view. Blind spots could result in unauthorized access to the TDE, as the access would not be monitored by the CCTV cameras. Cameras should be positioned to prevent the monitoring of computer screen displays, keyboards, PIN pads, or other systems which may expose sensitive data
	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.	

Requirements	Testing Procedures	Guidance
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.	Having a dedicated control room allows an entity to monitor and control physical access to and within the facility from a central location. The control room may be a security office, security operations center, or other room that is dedicated to this purpose.
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.	Whatever the time of day, the recording equipment needs to produce clear images that are not out-of-focus, blurred, washed out, or excessively darkened. If recording is activated via motion detection, the active recording time must be sufficient to ensure that all activity is captured—for example, to capture motion occurring at least 10 seconds before and 10 seconds after the motion that triggered the recording.
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.	When clocks are not properly synchronized, the captured images cannot be correlated to create an accurate record of the sequence of events. Synchronization may use automated or manual mechanisms.
	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.	
	TSP 6.3.6.c Examine system configurations for CCTV cameras, access control and intrusion-detection systems to verify that clocks are synchronized.	
	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.	

Requirements	Testing Procedures	Guidance
	TSP 6.3.6.e Examine documented procedures and interview personnel to verify that CCTV clocks are checked weekly to verify synchronization.	
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.	If entry to the TDE also provides access to CCTV footage, a malicious individual could erase the footage in order to remove any record of unauthorized activities on TDE systems.
	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.	
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.	Where digital-recording mechanisms are used, storage capacity and redundancy controls are critical to prevent the loss of any information captured over the most recent 90-day period. Where analogue recording is used, appropriate media rotation schedules are needed to prevent media being re-used within 90 days of its most recent recording.
	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.	
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.	If any access points are uncontrolled, unauthorized individuals could gain access that is not monitored or logged.
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.	Some personnel may require access only during business hours; others may require access outside of business hours—e.g., onsite operational or technical support personnel.

Requirements	Testing Procedures	Guidance
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.	**TSP 6.4.3.a** 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.	If entry to the TDE also provides access to the access-control systems, an individual could accidentally or maliciously tamper with or disable the system. An additional power supply ensures physical security controls are maintained during power outages, until the power can be restored or alternative processes implemented.
	TSP 6.4.3.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.	
	TSP 6.4.3.c 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.	
TSP 6.4.4 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	**TSP 6.4.4.a** Examine access control system configuration to verify that audit trails are enabled and configured to log all access attempts to the TDE.	Maintaining audit logs of physical access enables an organization to identify and trace potentially suspicious activities.
	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	
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.	Regular reviews of access logs by the Security Manager allows for identification and timely response to any unnecessary or suspicious access events.
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.	In order to provide a complete record of events or to assist with an investigation, all logs need to be retained for a consistent period of time.

Requirements	Testing Procedures	Guidance
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	Without regular testing, inefficiencies or failures in the access control system could remain unaddressed, resulting in increased exposure to physical breach.
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.	An audible alarm immediately alerts personnel to potential security issues so that response can be initiated as quickly as possible. Doors being held or propped open may result in unintended or unauthorized access.
	TSP 6.5.1.b Examine audit logs from the access control system to verify the door conditions are recorded.	
	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	
	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.	
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.	Even if an attacker is able to disable localized alarms, the central monitoring location will still be notified. A central monitoring location also allows for a coordinated response to be launched.

Requirements	Testing Procedures	Guidance
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.	Timely response to alarm events by appropriate security personnel minimizes the potential impact of a security breach and allows for timely recovery.
	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. • The physical inspection was performed by authorized personnel—i.e., a security officer, local law enforcement personnel or designated TSP personnel.	
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.	A record of alarm events can identify trends or patterns in behavior that occurred over a period of time that are material to an investigation.
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.	Photo identification provides a rapid identification mechanism for all parties, and allows authorized personnel to easily notice if such identification is not clearly visible. ID badges are sometimes combined with an access-control badge, although this is not required.
	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.	

Requirements	Testing Procedures	Guidance
	TSP 6.6.1.c Observe individuals entering and within the TDE to verify that badges are worn and visible at all times.	
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.	Removing access location information from ID badges prevents a lost or stolen badge from providing enough information for an attacker to know which building or facility the badge provides access to.
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.	Due to the high level of trust associated with granting personnel access to the TDE, a background check is required for all such personnel.
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.	Because the TDE is a secure area, only trusted individuals are to be provided access. Considerations for whether a short-term visitor or other guest is escorted or undergoes a background check include the duration, frequency and purpose of the visits.
	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.	

Requirements	Testing Procedures	Guidance
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.	Personnel need to be aware of and following access policies and procedures to ensure that ID badges and access mechanisms are only used by the personnel to which they are assigned, and that only intended users are provided access.
	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.	
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 6.7.1** 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.	A Master Key System is a key arraignment having two or more levels of keying. The "master" key is the higher level of key that can lock/unlock all of the doors associated with subordinate keys.
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.	Because facility master keys can override other physical controls, only the Security Manager, who has emergency access responsibility, or their designee, should have access to such keys.
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.	Determining the minimum number of keys necessary for business needs includes consideration for the number of individuals with specific responsibilities requiring access to or custodianship of such keys. The total number of keys in existence should allow for efficient, authorized access and usage when required,
	TSP 6.7.3.b Examine physical key storage locations to verify that unissued keys are stored in locked security containers at all times.	

Requirements	Testing Procedures	Guidance
	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.	without introducing a need to monitor and secure keys that are not needed.
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.	Removing access location information from keys prevents a lost or stolen key from providing enough information for an attacker to know the building or facility the key provides access to.
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	**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	A key-issuance log documenting which keys are assigned to whom, and when, provides the ability to locate any key at any time. Additionally, the log provides an auditable record of key custodianship if the need to investigate key usage arises.
	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.	
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.	This process will help ensure individuals that act as physical key custodians are aware of and commit to their responsibilities for protecting the keys from unauthorized access and use.
	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.	

Requirements	Testing Procedures	Guidance
	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.	
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.	If keys are loaned or transferred between personnel, it will not be possible to gain an accurate record of who used the key and when. Key custodians are accountable for ensuring their assigned keys are only used by the personnel to whom they are assigned.
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	Ensuring that alarm conditions are validated by an individual other than the person using the key prevents the unauthorized use of physical keys to bypass the electronic access-controlled system.
	TSP 6.7.8.b Examine policies and procedures to verify that such alarm conditions are validated by another individual.	
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 either stored within the TDE or in the custody of an authorized individual.	If not properly secured, removable media could fall into the wrong hands and be used to introduce vulnerabilities to the TDE (e.g., through installation of malicious code), or result in the loss of sensitive data.

Requirements	Testing Procedures	Guidance
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.	Keeping an accurate log of media movements and transfer of custodianship provides assurance that all media is accounted for at all times.
	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	
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.	Examples of methods for securely destroying electronic media include secure wiping, degaussing, or physical destruction (such as grinding or shredding hard disks). There are a number of industry and regional standards covering media destruction practices. Guidance on procedures for different types of media may also be found in ISO 9564-1: Personal Identification Number Management and Security.
	TSP 6.8.3.b Examine media destruction records to verify that a log is maintained and signed to confirm the destruction process.	

TSP 7. Monitor all access to TDE

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

Requirements	Testing Procedures	Guidance
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	The ability to identify attack patterns and undesirable behavior across systems is critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something goes wrong. Determining the cause of a compromise is very difficult, if not impossible, without a process to corroborate information from critical system components, and systems that perform security functions—such as firewalls, IDS/IPS, and file-integrity monitoring (FIM) systems. Thus, logs for all critical systems components and systems that perform security functions should be collected, correlated, and maintained. This could include the use of software products and service methodologies to provide real-time analysis, alerting, and reporting—such as security information and event management (SIEM), file-integrity monitoring (FIM), or change detection.
	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.	

TSP 8. Maintain an Information Security Policy

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

Requirements	Testing Procedures	Guidance
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.	Though roles are not required to have the specific job title of CISO or Security Manager, it's important that these responsibilities are assigned to an appropriate individual, or individuals. The role of CISO is typically a senior manager with adequate security knowledge to be responsible for the TSP's Information Security Management. The role of Security Manager is assigned to the individual ultimately responsible for physical security.
	TSP 8.1.1.b Interview personnel and review biographical information to verify identified individual has IT security knowledge.	
	TSP 8.1.1.c Interview personnel and examine documentation to identify manager with overall security responsibilities of the facility and for the TDE.	
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.	Executive management assignment of PCI DSS compliance responsibilities ensures executive-level visibility into the PCI DSS compliance program and allows for the opportunity to ask appropriate questions to determine the effectiveness of the program and influence strategic priorities. Overall responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization.
	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.	
	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.	

Requirements	Testing Procedures	Guidance
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	A formal compliance program allows an organization to monitor the health of its security controls, be proactive in the event that a control fails, and effectively communicate activities and compliance status throughout the organization. The PCI DSS compliance program can be a dedicated program or part of an over-arching compliance and/or governance program, and should include a well-defined methodology that demonstrates consistent and effective evaluation. Example methodologies include: Deming Circle of Plan-Do-Check-Act (PDCA), ISO 27001, COBIT, DMAIC, and Six Sigma.
	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	
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	The formal definition of specific PCI DSS compliance roles and responsibilities helps to ensure accountability and monitoring of ongoing PCI DSS compliance efforts. These roles may be assigned to a single owner or multiple owners for different aspects. Ownership should be assigned to individuals with the authority to make risk-based decisions and upon whom accountability rests for the specific function. Duties should be formally defined and owners should be able to demonstrate an understanding of their responsibilities and accountability.
	TSP 8.2.3.b Interview responsible personnel and verify they are familiar with and performing their designated PCI DSS compliance responsibilities.	

Requirements	Testing Procedures	Guidance
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 8.2.4.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.	Personnel responsible for PCI DSS compliance have specific training needs exceeding that which is typically provided by general security awareness training. Individuals with PCI DSS compliance responsibilities should receive specialized training that, in addition to general awareness of information security, focuses on specific security topics, skills, processes, or methodologies that must be followed for those individuals to perform their compliance responsibilities effectively. Training may be offered by third parties—for example, SANS or PCI SSC (PCI Awareness, PCIP, and ISA), payment brands, and acquirers—or training may be internal. Training content should be applicable for the particular job function and be current to include the latest security threats and/or version of PCI DSS. For additional guidance on developing appropriate security training content for specialized roles, refer to the PCI SSC's information supplement on *Best Practices for Implementing a Security Awareness Program.*
	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.	

Requirements	Testing Procedures	Guidance
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.	Without formal processes for the prompt (as soon as possible) detection and alerting of critical security control failures, failures may go undetected for extended periods and provide attackers ample time to compromise systems and steal sensitive data from the cardholder data environment.
	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.	
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 - 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	Documented evidence (e.g., records within a problem management system) should support that processes and procedures are in place to respond to security failures. In addition, personnel should be aware of their responsibilities in the event of a failure. Actions and responses to the failure should be captured in the documented evidence.

Requirements	Testing Procedures	Guidance
	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	
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.	Hardware and software technologies are constantly evolving, and organizations need to be aware of changes to the technologies they use, as well as the evolving threats to those technologies. Organizations also need to be aware of changes made by technology vendors to their products or support processes, to understand how such changes may impact the organization's use of the technology. Regular reviews of technologies that impact or influence PCI DSS controls can assist with purchasing, usage, and deployment strategies, and ensures controls that rely on those technologies remain effective.
	TSP 8.3.2.b Review the results of the recent reviews to verify reviews are performed at least annually.	
	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.	

Requirements	Testing Procedures	Guidance
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	Implementing PCI DSS controls into business-as-usual activities is an effective method to ensure security is included as part of normal business operations on an ongoing basis. Therefore, it is important that independent checks are performed to ensure BAU controls are active and working as intended. The intent of these independent checks is to review the evidence that confirms business-as-usual activities are being performed. These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, firewall reviews, etc.—to assist the entity's preparation for its next PCI DSS assessment.
	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	

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.