Payment Card Industry (PCI)

Card Production and Provisioning Logical Security

Requirements and Test Procedures

Version 3.0.1

June 2022

Document Changes

Date	Version	Description
December 2012	1.x	RFC version
May 2013	1.0	Initial Release
March 2015	1.1	Enhancements for clarification
July 2016	2.x	RFC Version
January 2017	2.0	Addition of Mobile Provisioning and other changes. See Summary of Changes from v1.1 to v2.
January 2022	3.0	See Summary of Changes from v2.0 to v3.0.
June 2022	3.0.1	Errata

Contents

Scope

All systems and business processes associated with the logical security activities associated with card production and provisioning such as data preparation, pre-personalization, card personalization, PIN generation, PIN mailers, and card carriers and distribution must comply with the requirements in this document. Dependent on the services provided by the entity, some sections of this document may not be applicable.

This document describes the logical security requirements required of entities that:

- Perform cloud-based or secure element (SE) provisioning services;
- Manage over-the-air (OTA) personalization, lifecycle management, and preparation of personalization data; or
- Manage associated cryptographic keys.

It does not apply to providers who are only performing the distribution of secure elements.

Wherever the requirements specify personalization, the requirements also apply to cloud-based provisioning networks—e.g., those for host card emulation. Cloud-based systems differ from those based on requiring the use of a secure element on a mobile device.

Within these requirements, all cited documentation must be validated at least every twelve months.

Appendix A: Applicability of Requirements makes further refinement at the requirement level for physical cards and mobile provisioning.

Although this document frequently states “vendor,” the specific applicability of these requirements is up to the individual Participating Payment Brands; and the payment brand(s) of interest should be contacted for the applicability of these requirements to any card production or provisioning activity.

Entities may adopt additional security controls as they deem appropriate, provided they are in addition to and enhance the procedures set forth in this manual.

Purpose

For the purposes of this document, personalization is defined as the preparation and writing of issuer or cardholder-specific data to the magnetic stripe or integrated circuit on the card. Subsequent use of the term “card personalization” includes data preparation, magnetic-stripe encoding, chip encoding, and mobile provisioning. Physical security requirements must also be satisfied. These requirements are intended to establish minimum security levels with which vendors must comply for magnetic-stripe encoding and chip personalization. However, physical requirements and procedures are beyond the scope of this document but can be found separately, in the *Payment Card Industry (PCI) Card Production and Provisioning Physical Security Requirements.*

Focus

The development, manufacture, transport, and personalization of payment cards and their components have a strong impact on the security structures of the payment systems, issuers, and vendors involved in their issuance. Data security is the primary focus of this document. Therefore, requirements for accessing, transporting, and storing data utilized during card production and provisioning are defined later in this document.

Laws and Regulations

In addition to the logical security requirements contained in this document, there will almost certainly be relevant regional and national laws and regulations, including consumer protection acts, labor agreements, health and safety regulations, etc. It is the responsibility of each individual organization independently to ensure that it obeys all local laws and regulations. Adherence to the requirements in this document does not imply compliance with local laws and regulations.

If any of the requirements contained in this manual conflict with country, state, or local laws, the country, state, or local law will apply.

Loss Prevention

Compliance with the requirements specified in this manual will not warrant or imply the prevention of any or all unexplained product losses. Approved vendors are responsible for preventing any such losses. Vendors are liable for any unexplained loss, theft, deterioration, or destruction of card products or components that may occur while such products are in the vendor's facility. Vendors are required to carry liability insurance covering all the risks stated above, taking into consideration the plant location, physical conditions and security of the plant, the number and duties of the employees, and the nature and volume of the contracted work.

Limitations

Transaction authorization and settlement activities are performed on networks and systems that are separate from the card production and provisioning environment and are out of scope for this document.

The individual Participating Payment Brands are responsible for defining and managing compliance programs associated with these requirements. Contact the Participating Payment Brand(s) of interest for any additional criteria.

Section 1: Roles and Responsibilities

1.1 Information Security Personnel

Requirement	Test Procedure
a) The vendor must designate, in writing, a senior manager with adequate security knowledge to be responsible for the vendor's Information Security Management and security of the cloud-based provisioning platform. These requirements refer to this person as the "Chief Information Security Officer" ("CISO").	Examine applicable policies and procedures to verify that a senior manager has been designated as CISO and has IT security knowledge and responsibility of IT security management and cloud-based provisioning platform. Interview the CISO to determine their understanding of their roles and responsibilities.
b) The CISO must be an employee of the vendor.	Examine employment documentation to verify employment and position.
c) The CISO must, on a monthly basis, report to executive management the current status of security compliance and issues that pose potentials risks to the organization.	Examine documented processes and verify reports or meeting minutes to ensure that monthly security compliance status or issues that pose potential risks are being reported by CISO to executive management.

1.2 Assignment of Security Duties

Requirement	Test Procedure
a) The CISO must:	
i. Be responsible for compliance to these requirements.	Interview the CISO and examine documentation to determine scope of responsibility.
ii. Have sufficient authority to enforce the requirements of this document.	Examine applicable policies and procedures to verify that a senior manager has been designated as CISO and has IT security knowledge and responsibility of IT security management and cloud-based provisioning platform.
iii. Not perform activities that he or she has the responsibility for approving.	Examine logs or similar documentation to confirm the CISO does not perform activities related to the approval process for the vendor's Information Security Management and security of the cloud-based provisioning platform for which they have responsibility for approving.
iv. Designate a backup person who is empowered to act upon critical security events in the event the CISO is not available.	Examine documentation that identifies the designated backup person who is empowered to act upon critical security events in the absence of the CISO. Interview the backup person to determine his or her understanding of his or her roles and responsibilities.

1.2 Assignment of Security Duties

Requirement	Test Procedure
v. Identify an IT Security Manager (if not themselves) responsible for overseeing the vendor's security environment.	Interview the CISO and examine documentation to conclude the individual or an appropriate designee has responsibility the vendor security environment.
vi. The back-up CISO and the IT Security Manager must be employees of the vendor.	Interview the back-up CISO to verify role. Examine employment documentation to verify employment and position.
b) When the CISO backup is functioning on behalf of the CISO, the backup must not perform activities for which they have approval responsibility and must not approve activities that they previously performed.	Examine logs or similar documentation to confirm the backup CISO does not perform activities related to the approval process for the vendor's Information Security Management and security of the cloud-based provisioning platform for which they have approval responsibility.
c) Where managers have security compliance responsibilities, the activities for which the manager has responsibility must be clearly defined.	Examine documentation to authenticate the manager's security roles and responsibilities are clearly defined.
d) Staff responsible for day-to-day production activities must not be assigned security compliance assessment responsibility for the production activities that they perform.	Interview security personnel or examine documentation—e.g., reviewing accounts on personalization machines and in the production workflow—to determine independence exists between day-to-day production operations and personnel performing security compliance assessments for those same production activities.

Section 2: Security Policy and Procedures

2.1 Information Security Policy

Requirement	Test Procedure
a) The vendor must define and document an information security policy (ISP) for the facility and disseminate to all relevant personnel (including vendors, sub-contractors, and business partners).	Examine the information security policy and verify that the policy is published. Interview a sample of relevant personnel to verify they are aware of the policy and that they have access to it.
b) Senior management must review and endorse the validity of the ISP at least once each year.	Examine evidence—e.g., formal sign-off—that the information security policy has been reviewed and endorsed by senior management within the most recent 12-month period.
c) The ISP must include a named individual assigned as the "policy owner" and be responsible for management and enforcement of that policy.	Examine the ISP to verify that: • The information security policy designates a specific policy owner by name. • The policy owner is responsible for management and enforcement of that policy. Interview the policy owner to verify that the policy owner: • Has acknowledged his or her responsibility. • Ensures that the policy is updated and changes communicated as needed.
d) The vendor must maintain audit trails to demonstrate that the ISP and all updates are communicated and received by relevant staff. Evidence of staff review and acceptance of ISP must be maintained.	Examine audit trails to verify they exist and: • ISP updates are communicated to relevant staff. • Evidence of staff reviews and acceptance is maintained—e.g., automated systems for policy disbursement. Interview a sample of staff to ensure that they are aware of the current ISP.

2.2 Security Procedures

Requirement	Test Procedure
a) The vendor must maintain procedures for each function associated with the ISP to support compliance with these requirements.	Examine procedural documents to ensure procedures have been defined for each function described in the ISP—e.g., password policy, remote access policy.
b) Procedures must be documented and followed to support compliance with these Security Requirements. The security procedures must be reviewed, validated, and where necessary updated annually.	Interview a sample of staff to determine that procedures are followed to support compliance with these Security Requirements. Examine evidence that the procedures are reviewed, validated, and where necessary, updated annually.
c) Security procedures must describe the groups, roles, and responsibilities for all activities that protect cardholder data.	Examine policies to verify that they clearly define information security responsibilities for all personnel. Interview a sample of responsible personnel to verify they understand the security policies.

2.3 Incident Response Plans and Forensics

Requirement	Test Procedure
The vendor must:	
a) Have a documented incident response plan (IRP) for known or suspected compromise of any classified data. The IRP must be communicated to relevant parties.	Examine the incident response plan and related procedures to verify the entity has a documented IRP addressing known or suspected compromise of any classified data. Interview personnel to determine that the IRP is communicated to relevant parties.
b) Ensure staff report any unexpected or unusual activity relating to production equipment and operations.	Interview staff to determine that they report any unexpected or unusual activity relating to production equipment and operations. Examine evidence of existence of reported incidents.

2.3 Incident Response Plans and Forensics

Requirement	Test Procedure
c) Within 24 hours, report in writing any known or suspected compromise of confidential or secret data to the Vendor Program Administrator (VPA) and the impacted issuers. Confirmed incidences must be reported to appropriate law enforcement agencies upon confirmation. The written communication must contain information regarding the loss or theft including but not limited to the following information: • Name of issuer • Type of data • Name and address of the vendor • Identification of the source of the data • Description of the incident including: – Date and time of incident – Details of companies and persons involved – Details of the investigation – Name, e-mail, and telephone number of the person reporting the loss or theft – Name, e-mail, and telephone number of the person to contact for additional information (if different from the person reporting the incident)	Examine ISP documentation to verify notification procedures for suspected compromise of confidential or secret data to the VPA and impacted issuers are in place and requires reporting within 24 hours. Examine reported incidences to verify that law enforcement agencies were included in the written notification. Each notification must include at minimum the information outlined in Requirement 3.3c.
d) Investigate the incident and provide at least weekly updates about investigation progress.	Examine written notifications to determine weekly updates were issued during the investigation process.
e) Supply a final incident report providing the investigation results and any remediation.	Examine reports to determine a final report was provided and that the report contains results and any remediation.
f) Identify and preserve specific logs, documents, equipment, and other relevant items that provide evidence for forensic analysis.	Examine incident response procedures to identify what logs, documents, equipment, or other relevant information is being preserved. Validate identified information is being preserved.

Section 3: Data Security

The data security requirements in this and embedded sections apply to confidential and secret data. The vendor must maintain detailed procedures relating to each activity in this section.

3.1 Classifications

Requirement	Test Procedure

Definitions

Secret Data

Information assets classified as secret require additional measures to guard against unauthorized use or disclosure that would result in significant business harm or legal exposure. This classification is typically used for highly sensitive business or technical information. Secret data is data that, if known to any individual, would result in risks of widespread compromise of financial assets.

All symmetric (e.g., Triple DES, AES) and private asymmetric keys (e.g., RSA)—except keys used only for encryption of cardholder data—are secret data and must be managed in accordance with Section 7 of this document, "Key Management: Secret Data."

Examples:

- *Chip personalization keys*
- *PIN keys and keys used to generate CVVs, CVCs, CAVs, or CSCs*
- *PINs*

Confidential Data

Confidential data is considered any information that might provide the vendor with a competitive advantage or could cause business harm or legal exposure if the information is used or disclosed without restriction. Confidential data is data restricted to authorized individuals. This includes cardholder data and the keys used to encrypt cardholder data.

Examples:

- *PAN, expiry, service code, cardholder name, Track 2 or Track 2 equivalent*
- *TLS keys*
- *Vendor evidence preserving data*
- *Authentication credentials for requesting tokens*
- *Mobile Station International Subscriber Directory Number (number used to identify a mobile phone number)*

Unrestricted/Public Data

Unrestricted/public data includes any data not defined in the above terms—i.e., information that is developed and ready for public dissemination, including any information that has been explicitly approved by management for release to the public. Controls are out of scope of these requirements and may be defined by the vendor.

3.1 Classifications

Requirement	Test Procedure
3.1.1 Protection Controls	
a) Documented security requirements must exist that define the protection controls commensurate to the classification scheme.	Examine documentation to verify that data-protection controls are documented, and that the data-classification scheme differentiates between secret, confidential, and public data.
b) All payment data must have an identifiable owner who is responsible for classification for ensuring protection controls are implemented and working.	Examine documentation to verify that data ownership identification is included in the data-protection controls. Examine a sample of stored data to verify that the data owner and security classification are identifiable.

3.2 Encryption

Requirement	Test Procedure
All secret and confidential data must be:	
a) Encrypted using algorithms and key sizes as stated in Normative Annex A.	Examine key-management policies and procedures to verify that cryptographic keys used for secret and confidential data use algorithms and keys sizes that are in accordance with Annex A. Examine evidence for a sample of keys to verify that the key algorithms (select at least one asymmetric and one symmetric) and sizes used for secret and confidential data conform to the values defined in Annex A.
b) Encrypted at all times during transmission and storage.	Interview personnel to identify controls in place for the transmission and storage of secret and confidential data. Examine transmission channels and data storage areas to verify that encryption is enabled and operating effectively for secret and confidential data.
c) Decrypted for the minimum time required for data preparation and personalization.	Examine data flow and storage documentation and other supporting evidence to verify secret and confidential data is encrypted during storage and only decrypted for the minimum time needed to prepare data for personalization and perform personalization.

3.2 Encryption

Requirement	Test Procedure
d) The vendor must only decrypt or translate cardholder data on the data-preparation or personalization or cloud-based provisioning network and not while it is on an Internet- or public facing network.	Examine documentation that describes the data flow to verify secret and confidential cardholder data: • Is decrypted only on the data-preparation, personalization, or cloud-based provisioning systems. • Is never decrypted while the data is on an Internet- or public-facing network. • Remains encrypted in the DMZ. Additional validation and assurance can be provided through checking the DMZ network for decryption/encryption software.

3.3 Access to Cardholder Data

Requirement	Test Procedure
The vendor must:	
a) Document and follow procedures describing the vendor's data access requirements.	Examine documentation to verify that the cardholder data access policy and procedure are documented. Observe a demonstration showing authorized access to cardholder data and that access attempted by an unauthorized user is declined.
b) Prevent direct access to cardholder data from outside the cloud-based provisioning network or the personalization network.	Examine access-control settings to verify cardholder data cannot be accessed from outside the cloud-based provisioning and personalization networks and systems.
c) Prevent logical access from outside the high security area (HSA) to the data-preparation or personalization networks.	Examine access-control settings to verify logical access to the data preparation and personalization networks is prevented from outside the high security area (HSA).
d) Ensure that access is on a need-to-know basis and that an individual is granted no more than sufficient access to perform his or her job.	Examine a sample of access-control settings to verify that: • The access rights for the individual are known. • The reason for the access permission is available and access is justified. • The individual does not have access permissions beyond those sufficient to perform his or her job.
e) Establish proper user authentication prior to access.	Examine documentation to determine whether user authentication procedures are defined. Observe a demonstration of the user authentication process to verify it conforms to procedures and provides confidence that the user was authenticated.

3.3 Access to Cardholder Data

Requirement	Test Procedure
f) Make certain that access audit trails are produced that provide sufficient details to identify the cardholder data accessed and the individual user accessing the data.	Examine a sample of audit trails to verify they exist for individual access to cardholder data and provide sufficient detail to identify the individual user.
g) Ensure that PANs are masked when displayed or printed unless there is a written issuer authorization. When PANs are masked, only a maximum of the first six and last four digits of the PAN can be visible. Business requirements must be documented and approved by the issuer.	Examine evidence that PANS are masked such that only the first six and last four digits are visible when displayed or printed. Examine evidence to verify that when a PAN is not masked the issuer has authorized the visible PAN and that the business justification is documented.
h) Apply appropriate measures to ensure that any third-party access meets the following requirements: • Third-party access to cardholder or cloud-based provisioning data must be based on a formal contract referencing applicable security policies and standards. • Access to cardholder or cloud-based provisioning data and the processing facilities must not be provided until the appropriate access controls have been implemented and a contract defining terms for access has been signed.	For all third-party service providers that have access to cardholder or provisioning data: • Examine evidence that a formal contract with the service provider exists and that it includes identification of and compliance with the applicable security policies and standards. • Examine evidence to verify that access to cardholder and cloud-based provisioning data is not provided until a formal contract defining access terms is signed.
i) Ensure that only authorized database administrators have the ability to directly access cardholder or cloud-based provisioning databases. Other user access and user queries must be through programmatic methods.	Examine database-access policies and procedures to verify that only authorized database administrators are granted direct access to cardholder or cloud-based provisioning databases while all other access is controlled through programmatic processes. Examine a sample of access-control settings to verify that only authorized database administrators are granted direct access to cardholder or cloud-based provisioning databases while all other access is controlled through programmatic processes.
j) Ensure that direct access to databases is restricted to authorized database administrators. Systems logs for database administrator access must exist and be reviewed weekly.	Examine evidence that data access activity logs exist and that the logs are reviewed at least weekly. Observe a demonstration that direct access to data contained in databases is limited to authorized database administrators.
k) Ensure that application (program) IDs used for cloud-based processes are used only for their intended purposes and not for individual user access.	Examine evidence to verify that application IDs for cloud-based processes cannot be used for individual user access and the IDs can only be used for their intended purpose. Observe a demonstration to verify that application IDs used for cloud-based processes cannot be used for individual user access.

3.4 Transmission of Cardholder Data

Requirement	Test Procedure
The requirements in this section apply to data transmitted to or from the issuer or authorized processor.	
a) Cardholder data transmission procedures must incorporate the maintenance of a transmission audit log that includes, at a minimum: • Date and time of transmission • Identification of the data source	Examine a sample of cardholder data transmission logs to verify they exist and at a minimum contain the date/time of transmission and identification of the data source.
b) Cardholder data transmitted to or received from an external source or transferred on the cloud-based provisioning network must be encrypted and decrypted per the encryption requirements of this document.	Interview DBAs to identify where cardholder data is encrypted and decrypted when transmitted to or received from an external source or transferred on the cloud-based provisioning network. Examine network and/or data-flow diagrams or other evidentiary documentation to verify that provisioning cardholder data transmitted to / received from an external source is only encrypted/decrypted as per the encryption requirements in this document—e.g., encryption strengths, algorithms, locations, durations, etc.
c) The vendor must establish mechanisms that ensure the authenticity and validate the integrity of cardholder data transmitted and received.	Examine policies and procedures to verify that cardholder data transmitted and received is authenticated and validated. Interview personnel to verify that upon transmission or receipt the cardholder data authentication and validation process complies with the defined procedure.
d) The vendor must protect the integrity of cardholder data against modification and deletion at all times.	Examine procedures and the production data flow to verify that cardholder data integrity is protected against modification and deletion.
e) The vendor must accept cardholder data only from pre-authorized sources that are defined and documented.	Examine documentation to verify that authorized cardholder data sources are defined. Examine data transmission logs to verify that cardholder data is received from and sent only to pre-authorized locations.
f) The vendor must log and inform the card brands of all issuers sending the vendor cardholder data in clear text.	Examine policy and procedure documentation to verify a process is in place to identify clear-text cardholder data sent by an issuer and report it to the VPA. Examine evidence to verify that any identified clear-text cardholder sent by an issuer was reported to the VPA.
g) If the file is not successfully transmitted, or only part of the cardholder data is received, the recipient must contact the sender to resolve. The vendor must inform the issuer or authorized processor upon discovery that the file was not successfully received. Any incomplete cardholder data transmission received must be deleted under dual control and logged accordingly.	Examine documentation to verify the vendor has procedures to: • Resolve cardholder data transmission errors. • Notify the issuer or authorized processor upon discovery that the file was not successfully received. • Delete under dual control and log any incomplete cardholder data transmissions.

3.5 Retention and Deletion of Cardholder Data

Requirement	Test Procedure
The vendor must:	
a) Ensure that procedures that define the vendor's data-retention policy are documented and followed.	Examine policies and procedures to verify that a data-retention policy exists. Examine evidence that the retention policy is followed.
b) Delete cardholder data within 30 days of the date the card file is personalized unless the issuer has authorized longer retention in writing. • Ensure that the authorized retention period does not exceed six months from the date the card is personalized. • Ensure each issuer authorization to retain cardholder data is valid for no longer than two years.	Examine a sample of retained cardholder data to verify that it is not retained longer than 30 days after personalization unless the issuer has authorized longer retention in writing. Verification of data deletion must include any data backups and return files in the DMZ that contain cardholder data. Examine evidence of issuer authorization for personalization data retained longer than 30 days after personalization. Examine issuer authorization that allows for cardholder data retention longer than 30 days to verify that the authorization is less than two years old. Examine a sample of cardholder data authorized for retention longer than 30 days and verify that: • Cardholder data is deleted in compliance with the authorized retention period. • Cardholder data is not retained longer than the six-month maximum.
c) Delete data on the personalization machine as soon as the job is completed.	Examine a sample of completed batches to verify that cardholder data is deleted from the personalized machine once the job is completed.
d) Confirm the deletion of manually deleted cardholder data including sign-off by a second authorized person.	Examine evidence for a sample to verify that any cardholder data manually deleted was deleted with sign-off by an authorized secondary party.
e) Conduct quarterly audits to ensure that all cardholder data beyond the data retention period has been deleted.	Examine evidence for a sample to verify that quarterly audits were conducted to ensure all cardholder data was deleted if it was retained beyond its authorized retention period.
f) Ensure that all cardholder data has been irrecoverably removed before the media is used for any other purpose.	Examine evidence for a sample to verify that all cardholder data was irrecoverably removed before the media was used for another purpose.
g) Ensure media destruction is performed under CCTV surveillance according to industry standards (see *ISO 9564-1: Personal Identification Number Management and Security*) under dual control, and that a log is maintained and signed confirming the destruction process.	Observe CCTV recordings for an example to verify that: • Media is destroyed in accordance with industry standards and under dual control; and a • log is maintained and signed confirming the destruction process.

3.5 Retention and Deletion of Cardholder Data

Requirement	Test Procedure
h) Ensure cardholder data is always stored within the high security area (HSA).	Examine the data storage policy and procedures to verify cardholder data is being stored within the designated high security area. Observe the cardholder data storage location to verify it is a high security area.
i) Ensure that cardholder data retained for longer than 30 days after personalization complies with the following additional requirements. This data must: i. Be removed from the active production environment. ii. Be stored on a separate server or media iii. Be accessible only under dual control.	Observe the cardholder data storage area utilized for data retained longer than 30 days after personalization to verify that the data: • Is removed from the active production environment. • Is stored on a separate server or media. • Can only be accessed under dual control.

3.6 Media Handling

Requirement	Test Procedure
a) The vendor must have a documented removable-media policy that includes laptops, mobile devices, and removable storage devices—e.g., USB devices, tapes, and disks.	Examine the vendor's policies and procedures for removable media documentation to verify it exists and includes devices such as laptops, mobile devices, USB devices, tapes, and disks.
b) All removable media—e.g., USB devices, tapes, disks—within the HSA must be clearly labeled with a unique identifier and the data classification.	Observe a sample of removable media within the HSA to verify it is clearly labeled with a unique identifier and data classification.
c) All removable media must be securely stored, controlled, and tracked.	Observe the removable media storage location to verify the area is secure. Examine the removable media check-in/out process to verify an audit trail is maintained and that it provides an accurate record of media possession.
d) All removable media within the HSA or the cloud-based provisioning environment must be in the custody of an authorized individual, and that individual must not have the ability to decrypt any sensitive or confidential data contained on that media.	Examine a sample of checked-out, removable media within the HSA or the cloud-based provisioning environment to verify: • The media is in the custody of the person to whom the media was issued. • The individual is authorized to possess the media. • That individual does not have the ability to decrypt any sensitive or confidential data contained on that media other than in compliance with procedures for handling sensitive or confidential data. • The media does not contain clear-text confidential data.

3.6 Media Handling

Requirement	Test Procedure
e) 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 identifier • Date and time • Name and signature of current custodian • Name and signature of custodian recipient • Reason for transfer	Examine the media audit trail documentation to verify that it contains at least the following data points: • Unique media identifier • Date and time logged out and returned • Name and signature of the current custodian • Name and signature of custodian recipient • Reason for transfer
f) Transfers of custody between two individuals must be authorized and logged.	Examine evidence that any transfer of checked out media is authorized and logged.
g) Transfer of removable media to and from the HSA must be authorized and logged.	Examine a sample of media that was removed from the HSA to verify that the removal was authorized and logged.
h) Physically destroy any media holding secret or confidential data when it is not possible to delete the data so that it is no longer recoverable.	Examine evidence that media containing secret or confidential media is destroyed in a manner that makes it impossible to recover the data.

3.7 Contactless Personalization

Requirement	Test Procedure
The security requirements for dual-interface cards that are personalized using the contact interface are the same as for any other chip card. The requirements in this section apply to personalization of chip cards via the contactless NFC interface.	
The vendor must:	
a) Ensure personalization signals cannot be detected beyond the HSA.	Examine evidence to verify testing was performed showing that contactless personalization signals cannot be detected external to the HSA.

3.7 Contactless Personalization

Requirement	Test Procedure
b) Conduct a scan of area surrounding the HSA whenever the personalization environment is changed to confirm personalization data sent by wireless communication does not reach beyond the HSA.	Examine evidence to verify that testing for personalization signals outside the HSA was performed after the last significant change to the personalization environment. Significant changes include but are not limited to: • The introduction of new personalization equipment • Modification of personalization equipment shielding • Structural changes to the HSA perimeter
c) Ensure that when personalization signals are encrypted, they comply with the encryption standards defined in Normative Annex A. If the signals are encrypted, 4.7 a, b, and d herein do not apply.	Examine evidence that encrypted personalization signals comply with the encryption requirements defined in Normative Annex A.
d) Perform a manual or automated inspection of the secure personalization area at least twice each month in order to detect any rogue radio-frequency (RF) devices.	Examine evidence that manual or automated scans for rogue RF devices are performed at least twice per month.
e) Ensure that personalized cards (including rejects) are stored and handled as batches of two or more cards or enclosed within protective packaging that restricts reading card emissions until the cards are packaged for final distribution or destruction.	Examine evidence to verify personalized contactless cards are stored and handled: • As batches of two or more cards, or • Enclosed within protective packaging that restricts reading card emissions

3.8 Data Used for Testing

Requirement	Test Procedure
a) Test (non-production) keys and test (non-production) data cannot be used with production equipment.	Examine documented policies and procedures to verity test keys and test data are restricted from use in production. Observe the location of the test environment to verify that it is separate from production. Interview personnel to verify testing is performed using test keys, data, equipment, and environment.
b) Cards used for final system validation or user acceptance that use production keys and/or data must be produced using production equipment.	Examine evidence to verify cards using production keys were produced for final system validation and user-acceptance testing in the production environment using production equipment.

3.9 Mobile Provisioning Activity Logs

Requirement	Test Procedure
a) The vendor must maintain an electronic log for both when cards are successfully and unsuccessfully provisioned. The log must be maintained for a minimum of 45 days.	Examine a sample of electronic logs to verify that successful and unsuccessful provisioning activity is logged. Examine evidence that provisioning activity logs are retained for at least 45 days.

3.10 Decommissioning Plan

Requirement	Test Procedure
a) The vendor must document its policies and procedures by which assets associated with card production and provisioning activities are secured in the event production activities are terminated.	Examine policies and procedures to verify that there is a decommissioning plan by which assets associated with card production and provisioning activities are secured in the event production activities are discontinued.
b) The procedures must identify all data storage, card design materials, cards, card components, physical keys, cryptographic keys, and hardware utilized for production activities that must be secured.	Examine the decommissioning plan to verify it includes the process by which the following items, at a minimum, are secured: • Cardholder data • Card design materials • Cryptographic keys • Production hardware • Physical keys
c) The disposition expectations for each identified item must be defined. For example, items may be returned to the owner, transported to an authorized user, or destroyed.	Examine the decommissioning plan to verify that the disposition expectation is defined for each item covered in the plan.

Section 4: Network Security

4.1 Typical Vendor Network

Requirement	Test Procedure
The requirements in this section do not apply to vendors that only perform key management or pre-personalization activities on a stand-alone wired system (not connected to any network) and do not perform data preparation or personalization within their facilities. *See Appendix B, "Topology Examples," for network examples.*	
Definitions ***Issuer/Data Source*** *This is the issuer that owns the cardholder data or that sends it to the vendor on behalf of the issuer.* ***Private Network (Leased lines), Internet, POTS*** *Cardholder data is typically sent over these three main types of network to the personalization vendor.* ***Data Preparation Network*** *This is the network that contains the server(s) where the cardholder data is stored pending personalization. This is also the network where the data is prepared and sent to the production floor.* ***Personalization Network*** *This is the network that contains the card personalization machines.*	
4.1.1 Card Production and Provisioning DMZ	
a) The DMZ must be dedicated to card production/provisioning activities.	Examine network diagrams and system configurations to verify that a DMZ dedicated to card production/provisioning activities is established.
b) The card production and provisioning network must be segregated from other parts of an organization's network.	Examine network diagrams and system configurations to verify that card production and provisioning network(s) are segregated from other parts of an organization's network.
c) All connections to and from the personalization network must be through a system in the DMZ.	Examine network diagram to verify all communication to and from the personalization network is exchanged via a system in the DMZ.
d) The DMZ must be located in the server room of the HSA.	Observe the system components comprising the DMZ to verify it is located in the server room within the HSA.

4.1 Typical Vendor Network

Requirement	Test Procedure
e) DMZ infrastructure equipment located within the HSA server room must be in a dedicated rack with access restricted to the minimum number of authorized individuals.	Observe the DMZ system components to verify they are located in dedicated rack(s) capable of restricting individual access. Examine policies and procedures regarding access to the dedicated rack(s) and verify the list of individuals with access is restricted to the minimum number of individuals required for effective operations.
f) All switches and cabling associated with the DMZ equipment must be stored within the same rack with only the minimum required number of cable connections entering/exiting the rack in order to provide connectivity to firewalls.	Observe DMZ switches and cabling to verify they are all stored within the same rack. Observe the DMZ cable connections to verify that only the minimum number of cable connections required to provide connectivity to firewalls are entering/exiting the rack.
4.1.2 Mobile Provisioning Networks	
a) HCE provisioning must be on its own network, but SE based provisioning is not required to be separated from other personalization networks.	Examine network diagrams to verify that the HCE provisioning system is separated from other personalization network systems. Examine logical configuration settings—e.g., firewall rules—to verify segmentation.

4.2 General Requirements

Requirement	Test Procedure
The vendor must:	
a) Maintain a current network topology diagram that includes all system components on the network. The diagram must clearly define the boundaries of all networks.	Examine network topology diagram to verify it exists, clearly defines the boundaries for all networks, and includes all system components that reside in the HSA.
b) Ensure the network topology diagram is reviewed, updated as appropriate, and verified at least once each year and whenever the network configuration is changed.	Interview network administration personnel to verify the policy and procedures require topology review and update upon making changes to the network and at least annually. Examine evidence that the network topology diagram was reviewed and updated when the network configuration was changed and at least within the last 12 months if there were no changes.
c) Ensure that the CISO accepts, by formal signature, the security implications of the current network topology.	Examine evidence that the CISO has accepted the security implications of the current network topology and that the document includes his or her formal signature.

4.2 General Requirements

Requirement	Test Procedure
d) Document the flow of cardholder and cloud-based provisioning data within the environment from its receipt/generation to end of its lifecycle. The diagram(s) are kept current and updated as needed upon changes to the environment and must undergo an overall review for accuracy at least every 12 months.	Examine the cardholder and cloud-based provisioning data-flow diagram to verify that cardholder data flows across systems and networks from its receipt/generation to end of its lifecycle. Interview the IT Manager to verify the diagram(s) are kept current and updated as needed and that it undergoes an overall review for accuracy at least every 12 months. .
e) Ensure that the personalization and data-preparation systems are on dedicated network(s) independent of the back office—e.g., accounting, human resources, etc.—and Internet-connected networks. A virtual LAN (VLAN) is not considered a separate network.	Examine network configurations to verify personalization and data-preparation systems are on dedicated network(s) independent of the back office—e.g., through the use of a firewall(s) and not a VLAN between the personalization/data-preparation systems and the back office and Internet-connected networks.
f) Physically and logically segment systems and applications that make up the cloud-based provisioning network from other vendor networks and Internet-connected networks. For example, in a traditional card vendor environment this could be a separate rack in a server room, or in a provisioning-only entity, housed in a separate room or cage in a data center. It cannot be in the same rack as other servers used for different purposes.	Examine network diagrams and other relevant materials to verify that any cloud-based provisioning network is physically and logically segmented from the broader environment. Observe where the cloud-based provisioning network components are housed to verify they are separate from other vendor networks and Internet-connected networks. For example, they cannot be in the same rack as other servers used for different purposes.
g) Put controls in place to restrict, prevent, and detect unauthorized access to the cloud-based and personalization networks. Access from within the high security area to anything other than the personalization or cloud-based networks must be “read-only”.	Examine policies and procedures to verify that: • Access to the cloud-based and personalization networks is restricted, and unauthorized access is prevented and detected. • Access from within the high security area to anything other than the personalization or cloud-based networks is “read-only.” Examine a sample of access rules to verify that access from within the high security area to anything other than the personalization or cloud-based networks is “read-only.”
h) Be able to immediately assess the impact if any of its critical connecting points ~~a~~re compromised.	Examine documented incident response procedures to verify processes are in place that allow for immediate assessment of the impact of any compromise of critical connecting points~~.~~
i) Have controls in place to restrict “write” permission to any system external to the personalization network to only pre-approved functions that have been authorized by the VPA, except for systems in the dedicated DMZ. These write functions must not transmit cardholder data if this involves direct write from the system containing the information.	Examine system configurations to verify that: • “Write” permissions to any system external to the personalization network and not in the dedicated DMZ are restricted to only pre-approved functions that have been authorized by the VPA; and • “Write” functions do not allow the transmission of cardholder data involving direct writes from the system(s) containing the information.

4.2 General Requirements

Requirement	Test Procedure
j) Control at all times the physical connection points leading into the personalization network and cloud-based provisioning network.	Observe physical connection points leading into the personalization network and cloud-based provisioning network to verify they are controlled at all times.
k) Prevent data from being tampered with or monitored by protecting the network cabling associated with personalization-data movement.	Observe a sample of personalization network cabling to verify that access is restricted, the cabling is protected, and safeguards are in place to avoid tampering.
l) Transfer required issuer data and keys into the personalization network or the cloud-based provisioning network via a defined and documented process.	Examine procedures to verify they define the process by which issuer data and keys are transferred to the personalization and cloud-based provisioning networks. Interview personnel to verify that the data transfer process conforms to documented procedures.
m) Ensure a process is in place for updates and patches and identification of their criticality, as detailed in Section 5.3, "Configuration and Patch Management."	Examine documented procedures to verify they include a process for updates and patches that includes identification of their criticality as delineated in the Section 5.3, "Configuration and Patch Management."
n) Have the capability to detect, isolate, and correct abnormal operations on cloud-based provisioning network systems and on cloud-based provisioning network endpoints on a real-time basis, 24/7.	Interview personnel to verify that system-monitoring assets are functional and utilized. Examine evidence to verify that abnormal operations on cloud-based provisioning network systems and on cloud-based provisioning network endpoints can be: • Detected, • Isolated, and • Corrected on a real-time and 24/7 basis.

4.3 Network Devices

Requirement	Test Procedure
The requirements in this section apply to all hardware—e.g., routers, controllers, firewalls, storage devices—that comprises the data-preparation and personalization networks.	
The vendor must:	
a) Document the process to authorize all changes to network devices and protocols.	Examine documented procedures to verify a process is in place to authorize all changes to network devices and protocols prior to implementation. Examine a sample of change-management logs for network devices and protocols to verify the changes are authorized.

4.3 Network Devices

Requirement	Test Procedure
b) Document the current network device configuration settings, rulesets, and justification for each device.	Examine a sample of network device documentation to verify configuration settings, rulesets, and their justifications are documented. Interview personnel to verify they are familiar with the documentation and process by which the documentation is updated.
c) Ensure all available services are approved by an authorized security manager.	Interview personnel to identify available services. Examine evidence that available services were approved by an authorized security manager.
d) Implement logical and physical security controls that protect the integrity of network devices used.	Examine documentation of logical and physical security controls that protect the integrity of network devices used to verify existence. Observe a sample of the controls to verify effective implementation.
e) Implement mechanisms to effectively monitor the activity on network devices.	Interview personnel to verify mechanisms are defined and implemented to effectively monitor the activity on network devices. Examine policies and procedures to verify mechanisms are defined to effectively monitor the activity on network devices.
f) Implement patches in compliance with Section 5.3, “Configuration and Patch Management.”	Examine a sample of device configurations and verify that patches have been implemented in compliance with Section 5.3.
g) Maintain an audit trail of all changes and the associated approval.	Examine a sample of change-control logs to verify that an audit trail of changes and associated approvals is maintained.
h) Implement unique IDs for each administrator.	Examine a sample of administrator IDs and verify that unique IDs are used.
i) Implement network device backups—e.g., system software, configuration data, and database files—prior to any change, and securely store and manage all media.	Examine change-control documentation to verify there is a process for backing up network devices prior to any changes to those devices. Examine procedures for backups and managing backup media to verify media are securely stored and managed. Observe the media storage location to verify it provides a secure storage environment.
j) Implement a mechanism to ensure that only authorized changes are made to network devices.	Examine network device change logs to verify that changes to network devices were authorized before implementation.

4.4 Firewalls

Requirement	Test Procedure
The requirements in this section apply to firewalls protecting the data-preparation and personalization networks.	
4.4.1 General	
The vendor must:	
a) Ensure all documents relating to firewall configurations are stored securely.	Observe the firewall configuration documentation storage area to verify: • Hard copy and non-digital documentation are stored in locked/secured areas accessible only to authorized personnel. • Digital records are stored in a secure directory with access limited to authorized personnel.
b) Deploy an external firewall outside the HSA to protect the HSA's DMZ.	Examine network diagrams and other relevant materials to verify that an external firewall outside the HSA is implemented to protect the HSA's DMZ in accordance with acceptable configurations. Examine firewall rules to verify that an external firewall is in place outside the HSA to protect the HSA's DMZ.
c) Install a firewall between the data-preparation network and the personalization network unless both are located within the same high security area or network.	Examine firewall rules to verify the separation via a firewall between the data-preparation network and the personalization network unless both are located within the same high security area or network.
d) Deploy physically separate firewalls between the external network and the DMZ and between the DMZ and the cloud-based provisioning network.	Examine network diagrams and firewall rules to verify that firewalls are installed between the external network and the DMZ and between the DMZ and the cloud-based provisioning network.
e) Have the capability to detect, isolate, and correct abnormal operations on network systems on a real-time basis, 24/7, on the external (DMZ) facing firewall.	Examine documentation to verify that abnormal operations on network systems can be: • Detected, • Isolated, and • Corrected on a real-time, 24/7, basis. Examine a sample of logs to verify that abnormal operations on network systems are: • Detected, • Isolated, and • Corrected on a real-time, 24/7, basis.

4.4 Firewalls

Requirement	Test Procedure
f) Implement appropriate operating-system controls on firewalls.	Examine configurations to verify that appropriate operating-system controls are implemented on firewalls.
g) Review firewall rule sets and validate supporting business justification either: • Monthly, or • Quarterly with review after every firewall configuration change.	Examine evidence that firewall rule sets have been validated either: • Monthly, or • After every firewall configuration change and every 3 months. Examine a sample of firewall rule sets to verify that their business justification is documented.
h) Restrict physical and logical access to firewalls to only those designated personnel who are authorized to perform firewall or router administration activities.	Observe the firewall/router environment to verify that that physical access to firewalls is limited to only those designated personnel who are authorized to perform administration activities. Examine a sample of access rules to verify logical access is restricted to only those designated personnel who are authorized to perform firewall or router administration activities.
i) Ensure the firewall rule set is such that any server only requiring inbound connections (for example, web servers) is prohibited from making outbound connections, and vice versa.	Examine firewall rules to verify that firewall and router configurations prohibit making outbound connection when only inbound traffic is expected. Examine firewall rules to verify that firewall and router configurations prohibit incoming connections when only outbound traffic is expected.
j) Ensure that only authorized individuals can perform firewall administration.	Examine policies and procedures to verify that only authorized individuals can perform firewall administration. Interview personnel to verify firewall administration is restricted to authorized individuals. Examine a sample of access rules to verify that only authorized individuals can perform firewall administration.
k) Run firewalls and routers on dedicated hardware. All non-firewall-related software such as compilers, editors, and communication software must be deleted or disabled.	Examine documentation to verify that non-firewall related software is deleted or disabled from firewalls and routers. Examine a sample of firewalls and routers to verify they are dedicated hardware from which all non-firewall related software has been deleted or disabled.
l) Implement daily, automated analysis reports to monitor firewall activity.	Examine evidence that automated tools exist to monitor and analyze firewall activity. Observe a sample of firewall analysis reports to verify that automated analysis is in place and that daily reports are produced.
m) Use unique administrator passwords for firewalls used by the personalization system as well as those passwords used for other network devices in the facility.	Examine authentication policies and procedures to verify passwords for firewall administration are different than passwords used for other network devices. Interview personnel to verify that unique passwords are established for firewall administration.

4.4 Firewalls

Requirement	Test Procedure
n) Implement both mechanisms to protect firewall and router system logs from tampering, and procedures to check the integrity of the logs monthly.	Examine evidence that firewall and router system logs are protected from modification and a mechanism is in place to check their integrity monthly.
o) Explicitly permit inbound and outbound traffic to the cloud-based provisioning and personalization networks. A rule must be in place to deny all other traffic.	Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cloud-based provisioning and personalization network. Examine a sample of firewall and router configurations to verify that: • Approved inbound and outbound traffic for cloud-based provisioning and personalization networks is explicitly permitted; and • All other inbound and outbound traffic is specifically denied—for example by using an explicit "deny all" or an implicit "deny after allow" statement.
4.4.2 Configuration	
The firewalls must:	
a) Be configured to permit network access to required services only.	Examine policies and procedures for permitting network access to only required services. Examine a sample of system configuration settings to verify that the configurations permit network access to only required services.
b) Be hardened in accordance with industry best practices, if the firewall is implemented on a commercial off-the-shelf (COTS) operating system.	Examine policies and procedures for hardening firewalls in accordance with industry best practices. Examine a sample of firewall configuration files to verify the configurations are consistent with industry-accepted hardening standards.
c) Prohibit direct public access between any external networks and any system component that stores cardholder data.	Examine policies and procedures for prohibiting direct public access between any external networks and any system component that stores cardholder data to verify existence. Examine a sample of firewall and router configurations to verify there is no direct access between the Internet and system components that store cardholder data.
d) Prevent the disclosure of private IP addresses and routing information from internal networks to the Internet by implementing IP masquerading or Network Address Translation (NAT) on the firewall between the DMZ and personalization and the cloud-based provisioning networks.	Examine policies and procedures for implementing IP masquerading or Network Address Translation (NAT) on the firewall between the DMZ and personalization and the cloud-based provisioning networks to verify existence. Examine a sample of firewall and router configurations to verify that methods are in place on the firewall between the DMZ and personalization and the cloud-based provisioning networks to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.

4.4 Firewalls

Requirement	Test Procedure
e) If managed remotely, be managed according to Section 4.6, "Remote Access."	If firewalls are managed remotely, examine policy and procedures documentation to verify management activities are managed according to Section 4.6.
f) Be configured to deny all services not expressly permitted.	Observe a sample of configuration settings to verify that all services not expressly permitted default to "deny."
g) Disable all unnecessary services, protocols, and ports. Authorized services must be documented with a business justification and be approved by the IT Security Manager.	Interview personnel to identify necessary services, protocols, and ports. Examine a sample of systems/networks to verify that unnecessary services are disabled. Examine a sample of services, protocols, and ports to verify that their business justification is documented, and that they were approved by the IT Security Manager.
h) Disable source routing on the firewall.	Examine a sample of firewall configurations to verify that source routing is disabled.
i) Notify the administrator in real time of any items requiring immediate attention.	Examine policy and procedures to verify that administrator(s) are to be notified in real time of any items requiring immediate attention. Interview administrators to verify that administrator(s) are notified in real time and that immediate attention is given when required.
j) Maintain documented baseline security configuration standards for system components based on industry-accepted system hardening standards, which include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST) At a minimum, baseline configuration must address: • User and group access security • File and directory security • Restricted services • System update and installation standards • Installed security software	Examine policies and procedures to verify that a baseline configuration has been established for the organization's system components and addresses at a minimum, but not limited to: • User and group access security • File and directory security • Restricted services • System update and installation standards • Installed security software Interview personnel to verify the baseline configuration standard is based on an industry standard.

4.4 Firewalls

Requirement	Test Procedure
k) The vendor must perform baseline security configurations checks in the cloud- based provisioning environment either: • Monthly, or • Quarterly with review after each configuration change.	Examine evidence to verify that the baseline security configuration was validated either: • Monthly, or • Quarterly with review after each configuration change. Examine a sample of baseline configuration checks to verify that they occurred either: • Monthly, or • Quarterly with review after each configuration change.

4.5 Anti-virus Software or Programs

Requirement	Test Procedure
The vendor must:	
a) Define, document, and follow procedures to demonstrate: • Identification of security alerts—e.g., subscribing to security alerts such as Microsoft and the Computer Emergency Response Team (CERT) • Identification of system component updates that affect the supportability and stability of operating systems, software drivers, and firmware components • Inventory of current systems in the environment including information about installed software components and about running services	Examine policies and procedures documentation to verify coverage of: • Identification of security alerts—e.g., subscribing to security alerts such as Microsoft and the Computer Emergency Response Team (CERT) • Identification of system component updates that affect the supportability and stability of operating systems, software drivers, and firmware components • Inventory of current systems in the environment including information about installed software components and about running services Interview personnel to ensure procedures are known and followed.
b) Deploy anti-virus software on all systems potentially affected by malicious software—e.g., personal computers and servers.	Examine a sample of system components potentially affected by malicious software to verify that anti-virus software is deployed.
c) Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	Examine a sample of system components to verify that: • Anti-virus software is present and running. • Activity logs are generated.

4.5 Anti-virus Software or Programs

Requirement	Test Procedure
d) Check for anti-virus updates at least daily and install updates in a manner consistent with Patch Management. Documentation must exist for why any updates were not installed.	Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date. Examine a sample of systems to verify that either updates (based upon alerts collected as part of 4.5.a) were applied or documentation exists for why they were not.

4.6 Remote Access

Requirement	Test Procedure
For purposes of this section, this applies to remote administration by the vendor, and not issuer connections.	
4.6.1 Connection Conditions	
a) Remote access is permitted only for the administration of the network or system components.	Examine policies and procedures to verify that remote access is permitted only for the administration of the network or system components. Examine a sample of users with remote access to verify such access is permitted only for the administration of the network or system components.
b) Access from outside the facility to the physical access-control system is not permitted except as used in conjunction with an approved SOC.	Examine a sample of system configurations to verify that remote access is not permitted from outside the facility to the physical access-control system except as used in connection an approved SOC.
c) Remote access—i.e., from outside the HSA—for administrative activities is permitted only from pre-determined and authorized locations using vendor-approved systems.	Examine a sample of remote access system configurations and access logs to verify access is accepted only from pre-determined and authorized locations using vendor-approved systems.
d) Access using personally owned hardware is prohibited.	Examine policies and procedures to verify that remote access using a personally owned device is prohibited. Examine a sample of remote access system configurations and access logs to verify that remote access from personally owned devices is not permitted.
e) Remote access is not permitted where qualified personnel are temporarily off-site and remote access is a convenience.	Examine policies and procedures to verify that remote access is not permitted when qualified personnel are temporarily off-site.

4.6 Remote Access

Requirement	Test Procedure
f) The remote access process must be fully documented and include at least the following components:	Examine policies and procedures to verify the remote access process is fully documented and includes the following components but is not limited to:
i. System components for which remote access is permitted	• System components for which remote access is permitted
ii. The location from which remote access is permitted	• The location from which remote access is permitted
iii. The conditions under which remote access is acceptable	• The conditions under which remote access is acceptable
iv. Users with remote access permission	• Users with remote access permission
v. The access privileges applicable to each authorized user	• The access privileges applicable to each authorized user
g) All access privileges must be validated on a quarterly basis by an authorized individual.	Examine documentation from a sample of reviews to verify that remote access privileges are reviewed at least quarterly by an authorized individual.
h) Remote access is prohibited to any system where clear-text cardholder data is being processed.	Examine a sample of system configurations to verify that remote access is not permitted to any system where clear-text cardholder data is being processed.
i) Remote access is prohibited to clear-text cardholder data, clear-text cryptographic keys, or clear-text key components/shares.	Examine remote access policies and procedures to verify that remote access is not permitted to clear-text cardholder data, clear-text cryptographic keys, or clear-text key components/shares.
j) The vendor must:	Examine policies and procedures to verify the following, at a minimum:
i. Ensure that systems allowing remote connections accept connections only from preauthorized source systems.	• Systems allowing remote connections accept connections only from preauthorized source systems.
ii. Ensure remote administration is predefined and preauthorized by the vendor.	• Remote administration is predefined and preauthorized by the vendor.
iii. Ensure remote changes comply with change-management requirements as outlined in Section 5.2, “Change Management.”	• Remote changes comply with change-management requirements as outlined in Section 5.2, “Change Management.”
iv. Ensure that all remote access locations are included in the facility’s compliance assessment and meet these requirements.	• All remote access locations are included in the facility’s compliance assessment and meet these requirements.
v. Be able to provide evidence of compliance validation for any remote access location.	• The vendor is able to provide evidence of compliance validation for any remote access location.

4.6 Remote Access

Requirement	Test Procedure
k) Ensure that non-vendor staff performing remote administration maintain liability insurance to cover potential losses. All personnel performing remote administration must meet the same pre-screening qualification requirements as card production staff working in high security areas.	Interview a sample of non-vendor staff performing remote administration and verify that they maintain liability insurance to cover potential losses. Examine policies and procedures to verify that personnel performing remote administration must meet the same pre-screening qualification requirements as employees working in high security areas.
l) All remote access must use a VPN that meets the requirements in the following section.	Examine a sample of remote access to verify that remote access occurs using a VPN that meets the requirements of Section 4.6.2, "Virtual Private Network (VPN)."
4.6.2 Virtual Private Network (VPN)	
a) For remote access, VPNs must start from the originating device—e.g., PC or off-the-shelf device specifically designed for secure remote access—and terminate at either the target device or the personalization firewall. If the termination point is the firewall, it must use IPSec or at least a TLS connection in accordance with PCI Data Security Requirement 4.1 to the target device.	Examine VPN system documentation and a sample of configuration settings to verify that: • For remote access, VPNs must start from the originating device and terminate at either the target device or the personalization firewall. • When terminating at the personalization firewall, an IPSec or TLS connection to the target device is used in accordance with PCI Data Security Requirement 4.1.
b) For remote access to DMZ components, the VPN must terminate at the target device.	Examine policy and procedure documentation to verify that it defines that VPN tunnels for remote access to DMZ components must terminate at the target device.
c) SSL and TLS 1.0/1.1 are expressly prohibited in connection with the aforementioned.	Examine a sample of system configurations to verify that for remote access to DMZ components, SSL and TLS 1.0 are disabled.
d) Traffic on the VPN must be encrypted using Triple DES with at least double-length keys or Advanced Encryption Standard (AES).	Examine a sample of system configurations to verify that only the listed algorithms are permitted.
e) Modifications to the VPN must be in compliance with the change-management requirements as outlined in Section 5.2, "Change Management."	Examine a sample of modifications made to VPN configurations and verify that changes are in compliance with the change-management requirements as outlined in Section 5.2, "Change Management."
f) Mechanisms—e.g., digital signatures, checksums—must exist to detect unauthorized changes to VPN configuration and change-control settings.	Examine a sample of VPN configuration files and change-control settings to verify they are protected from unauthorized modifications using mechanisms such as digital signatures and checksums.
g) Multi-factor authentication must be used for all VPN connections.	Examine a sample of VPN system documentation and configuration settings to verify multi-factor authentication is used for VPN connections. Observe a sample of VPN access processes to verify multi-factor authentication is used.

4.6 Remote Access

Requirement	Test Procedure
h) Access must be declined after three consecutive unsuccessful access attempts.	Examine a sample of system component configuration setting to verify that authentication parameters are set to require that user accounts be locked out after not more than three consecutive invalid logon attempts.
i) Access counters must only be reset by an authorized individual after user validation by another authorized individual.	Examine documentation for access counter resets to verify that it is only reset by an authorized individual after user validation by another authorized individual.
j) The connection must time out within five minutes if the session is inactive.	Examine a sample of system component configuration settings to verify that system/session idle time-out features have been set to five minutes or less.
k) Remote access must be logged, and the log must be reviewed weekly for suspicious activity. Evidence of log review must be maintained.	Examine documented procedures to verify remote access logs are reviewed at least weekly to identify suspicious activity and that evidence of log review is retained. Examine a sample of system configurations and audit logs to verify that remote access is logged and logs are reviewed.
l) VPN traffic using Internet Protocol Security (IPsec) must meet the following additional requirements:	Examine a sample of VPN configuration files to verify that the following requirements, at a minimum, are met:
i. Tunnel mode must be used except where communication is host-to-host.	• Tunnel mode is used except where communication is host-to-host.
ii. Aggressive mode must not be used for tunnel establishment.	• Aggressive mode is not to be used for tunnel establishment.
iii. The device authentication method must use certificates obtained from a trusted Certificate Authority.	• The device authentication method uses certificates obtained from a trusted Certificate Authority.
iv. Encapsulating Security Payload (ESP) must be used to provide data confidentiality and authentication.	• Encapsulating Security Payload (ESP) is 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.	• The Perfect Forward Secrecy (PFS) option of Internet Key Exchange (IKE) is used to protect against session key compromise.

4.7 Wireless Networks

Requirement	Test Procedure
4.7.1 General	
The vendor must:	
a) Implement a documented policy regarding wireless communications and clearly communicate this policy to all card production staff.	Examine usage policies to verify that they address wireless communications. Interview a sample of personnel and validate that the policy is clearly communicated to all card production staff.
b) Not use wireless communications for the transfer of any personalization data and/or cloud-based provisioning data.	Examine wireless communications policies to verify that wireless communications are prohibited for the transfer of any personalization data and/or cloud-based provisioning data.
c) Identify, analyze, and document all connections. Analysis must include purpose, risk assessment, and action to be taken.	Examine a sample of connections to verify that connections are identified, analyzed, and documented including purpose, risk assessment, and action to be taken.
d) Use a wireless intrusion-detection system (WIDS) capable of detecting hidden and spoofed.	Examine output from recent wireless scans to verify that, at a minimum: • The scan is performed for all wireless networks. • Hidden and spoofed networks can be detected.
e) When using a wireless network, use the WIDS to conduct random scans within the HSA at least monthly to detect rogue and hidden wireless networks.	Examine output from recent wireless scans to verify that the WIDS is used to conduct random scans within the HSA at least monthly to detect rogue and hidden wireless networks.
f) Document, investigate, and take action to resolve any issues identified when unauthorized connections or possible intrusions are detected. The investigation must occur immediately. Resolution must occur in a timely manner.	Examine policies and procedures for resolving any issues identified when unauthorized connections or possible intrusions are detected to verify existence, including that investigations must occur immediately and that resolutions occur in a timely manner. Examine output from recent scan reports and verify that all unauthorized connections or possible intrusions are detected, investigated immediately, and resolved in a timely manner.
g) Use a scanning device that is capable of detecting rogue and hidden wireless networks, regardless of whether or not the vendor uses a wireless network. Random scans of the HSA must be conducted at least monthly.	Examine policies and procedures to verify that a scanning device is used for rogue and hidden wireless networks—regardless of whether or not the vendor uses a wireless network—and that random scans of the HSA occur at least monthly. Examine a sample of output from recent scans to verify that the scanning device is used to conduct random scans of the HSA at least monthly.

4.7 Wireless Networks

Requirement	Test Procedure
4.7.2 Management *If wireless communication channels are used to transport any non-personalization data within or near the personalization environment, the following requirements apply:*	
a) All wireless connections must be authorized by management, with their purpose, content, and authorized users defined and periodically validated.	Examine policies and procedures to verify that wireless connections are authorized by management, with their purpose, content, and authorized users defined and periodically validated. Examine a sample of documentation for wireless connections to verify the connections are authorized by management and periodically validated.
b) Wireless networks must only be used for the transmission of non-cardholder data—e.g., production control, inventory tracking—and be properly secured. *The vendor must have controls in place to ensure that wireless networks cannot be used to access cardholder data.*	Examine policies and procedures to verify wireless networks are used for the transmission of non-cardholder data—e.g., production control, inventory tracking—and are properly secured.
c) The vendor must deploy a firewall to segregate the wireless network and the wired network.	Examine a network schematic to verify that a firewall is deployed to segregate the wireless network and the wired network. Examine firewall settings and router configurations to verify that a firewall is installed between all wireless networks and the wired network.
d) All wireless gateways must be protected with firewalls.	Examine a sample of firewall settings and router configurations to verify that wireless gateways are protected with firewalls.
e) All wireless access points must be configured to prevent remote administration over the wireless network.	Examine documentation to verify wireless access points are configured to prevent remote administration over the wireless network. Examine a sample of system configurations to verify they prevent remote administration over the wireless network.
f) All wireless traffic must be encrypted with Triple DES or AES and an encryption key of at least 128 bits, using WPA, WPA2, or 802.11x (or an equivalent protocol). WEP encryption must be disabled.	Examine vendor documentation and wireless configuration settings to verify the use of Triple DES or AES and an encryption key of at least 128 bits, using WPA, WPA2, or 802.11x (or an equivalent protocol), and the disablement of WEP encryption.

4.7 Wireless Networks

Requirement	Test Procedure
g) The service set identifier (SSID) must not be broadcast.	Examine system configuration settings to verify that the service set identifier (SSID) is not broadcast. Observe via a network-detecting device to determine whether SSIDs are being broadcast for any wireless communication channels used to transport any non-personalization data within or near the personalization environment—if yes, then a finding.
h) The vendor must change all default security settings for wireless connections, including passwords, SSID, admin passwords, and Simple Network Management Protocol (SNMP) community strings.	Examine policies and procedures to verify they require that all default security settings for wireless connections are changed upon installation including passwords, SSID, admin passwords, and Simple Network Management Protocol (SNMP) community strings. Examine a sample of system configuration settings to verify that default security settings are not used for wireless connections.
i) The vendor must validate any wireless access points that contain flash memory at least once each month to ensure that the firmware contains the authorized software version and appropriate updates.	Examine supporting documentation to verify that the vendor validates any wireless access points that contain flash memory at least once each month to ensure that the firmware contains the authorized software version and appropriate updates. Examine a sample of evidentiary matter to verify that validation of wireless access points that contain flash memory occurs at least once each month to ensure that the firmware contains the authorized software version and appropriate updates.
j) The vendor must disable the SNMP at all wireless access points.	Examine vendor documentation to verify that SNMP is disabled at all wireless access points. Observe a sample via using the system administrator's help to verify the vendor has disabled SNMP at wireless access points.
k) Static passwords used to join wireless networks must be compliant with the requirements in Section 6.2, "Password Control," but may be shared with other individuals in the organization on a need-to-know basis.	Examine documented standards and verify that static passwords used to join wireless networks are compliant with the requirements in Section 6.2 and are only shared with other individuals in the organization on a need-to-know basis.
4.7.3 Additional Requirements for Wi-Fi Standard *If the wireless network uses Wi-Fi based on IEEE 802.11, the vendor must ensure that the following requirements are met.*	
a) Default SSIDs must be changed upon installation and new passwords must be at least 8 characters.	Examine vendor documentation to verify that default SSIDs are not used and new passwords are at least 8 characters. Observe a sample via using the system administrator's help to verify that default SSIDs have been changed and the new passwords are at least 8 characters.

4.7 Wireless Networks

Requirement	Test Procedure
b) A log of media access-control addresses and associated devices (including but not limited to make, model, owner, and reason for access) must be maintained, and a check of authorized media access-control addresses on the access point (AP) must be conducted at least quarterly.	Examine a sample of logs of media access-control addresses and associated devices to verify they include at least the make, model, owner, and reason for access. Interview personnel to verify that a check of authorized media access-control addresses on the access point (AP) is conducted at least quarterly. Examine a sample of scan reports and verify that checks of authorized media access-control addresses on the access point (AP) occur at least quarterly.
c) A media access control address-based access-control list (ACL) must be used for access control of clients.	Interview responsible personnel to verify the use of ACLs for access control of clients. Examine supporting documentation to verify a media access control address-based access-control list (ACL) is used for access control of clients.
d) Wi-Fi Protected Access (WPA) must be enabled if the wireless system is WPA-capable.	Examine a sample of configurations and scan reports to verify that, where capable, Wi-Fi Protected Access (WPA) is enabled.
e) Default passwords on the AP must be changed.	Examine supporting documentation to verify that default passwords on the AP are required to be changed upon installation. Observe a sample via the system administrator's help to verify that default passwords on the AP are changed.
f) The management feature for the AP must be disabled on the wireless interface and must only be managed via the trusted, wired interface.	Examine configurations and verify that the management feature for the access point is disabled on the wireless interface and can only be managed via the trusted, wired interface.
g) The AP must be assigned unique Internet protocol (IP) addresses instead of relying on Dynamic Host.	Examine configurations and verify that an access point is assigned unique Internet protocol (IP) addresses instead of relying on Dynamic Host.

4.8 Security Testing and Monitoring

Requirement	Test Procedure
4.8.1 Vulnerability	
The vendor must:	
a) Perform quarterly external network vulnerability scans using an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC).	Examine policies and procedures to verify that quarterly external network vulnerability scans using an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC) are required. Examine a sample of external vulnerability scans and verify that quarterly external vulnerability scans occurred in the most recent 12-month period and were completed by a PCI SSC Approved Scanning Vendor (ASV).
b) Perform internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system-component installations, changes in network topology, firewall-rule modifications, product upgrades). Scans after changes may be performed by internal staff.	Examine policies and procedures to verify that internal and external network vulnerability scans are required at least quarterly and after any significant change in the network. Examine a sample (including the most recent significant change in the network) of internal and external network vulnerability scans to verify scans occur at least quarterly and after any significant change in the network.
c) Ensure all findings from network vulnerability scans are prioritized and tracked. Corrective action for high-priority vulnerabilities must be started within two working days.	Interview responsible personnel to verify that all findings from network vulnerability scans are prioritized and tracked, and that corrective action for high-priority vulnerabilities is started within two working days. Examine a sample of documentation to verify that findings from network vulnerability scans are prioritized and tracked, and that corrective action for high-priority vulnerabilities is started within two working days.
d) Retain evidence of successful remediation and make this evidence available during site compliance evaluations upon request.	Interview responsible personnel to verify evidence of successful remediation is retained and available upon request.
4.8.2 Penetration	
The vendor must:	
a) Perform internal and external penetration tests at least once a year and after any significant infrastructure changes.	Examine policies and procedures to verify that internal and external penetration tests are performed at least once a year and after any significant infrastructure changes. Examine the most recent internal and external penetration tests to verify that the following requirements, at a minimum, were met:
i. The internal penetration test must not be performed remotely.	• The internal penetration test was not performed remotely.

4.8 Security Testing and Monitoring

Requirement	Test Procedure
ii. Penetration tests must be performed on the network layer and include all personalization network components as well as operating systems.	• Penetration tests were performed on the network layer and included all personalization network components as well as operating systems.
iii. Penetration tests must be performed on the application layer and must include at least the following: – Injection flaws—e.g., SQL injection. Also consider OS Command Injection, LDAP, and XPath injection flaws as well as other injection flaws. – Buffer overflow – Insecure cryptographic storage – Improper error handling – Insecure communications – All other discovered "high-risk" network vulnerabilities with criteria for ranking vulnerabilities, including: • Consideration of the Common Vulnerability Scoring System (CVSS) base score, and/or • The classification by the vendor, and/or • Type of systems affected.	• Penetration tests were performed on the application layer and included at least the following: – Injection flaws—e.g., SQL injection – Buffer overflow – Insecure cryptographic storage – Improper error handling – Insecure communications – All other discovered high-risk network vulnerabilities
b) Ensure all findings from penetration tests are prioritized and tracked. Corrective action for high-priority vulnerabilities must be started within two working days.	Interview responsible personnel to verify that all findings from penetration tests are prioritized and tracked, and that corrective action for high-priority vulnerabilities is started within two working days. Examine a sample of documentation to verify that findings from penetration tests are prioritized and tracked, and that corrective action for high-priority vulnerabilities is started within two working days.
c) Retain evidence of successful remediation and make this evidence available during site compliance evaluations upon request.	Interview responsible personnel to verify evidence of successful remediation is retained and available upon request.

4.8 Security Testing and Monitoring

Requirement	Test Procedure
4.8.3 Intrusion Detection Systems	
The vendor must:	
a) Use intrusion-detection systems (IDS) for network traffic analysis. IDS may be implemented as part of an intrusion-prevention system (IPS) if an IPS is used. These must be deployed, managed, and maintained across the vendor's networks not only for intrusion detection and prevention but also to monitor all data-preparation and personalization network traffic and cloud-based provisioning networks. This includes all traffic generated by machines within the personalization network, including IDS data from within the DMZ. For networks where clear-text PINs traverse, the systems must not be configured to allow capture of clear PIN values.	Examine policies and procedures to verify that intrusion-detection systems are in place to monitor all traffic across the vendor networks, generated by machines within the perimeter, all data-preparation and personalization network traffic, and cloud-based provisioning networks. Examine a sample of system configurations and network diagrams to verify that intrusion-detection systems are in place to monitor all traffic across the vendor networks, generated by machines within the perimeter, all data-preparation and personalization network traffic, and cloud-based provisioning networks. Examine a sample of system configurations to verify that the systems are not configured to allow capture of clear PIN values in networks where clear-text PINs traverse.
b) Ensure the IDS alerts personnel to suspicious activity in real time.	Interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises in real time. Examine a sample of records to verify the IDS alerts personnel to suspicious activity in real time.
c) Ensure the IDS monitors all traffic at the personalization network perimeter as well as at critical points inside the personalization network, such as but not limited to firewalls and public-facing interfaces or servers where cardholder data is decrypted.	Examine system configurations and network diagrams to verify that intrusion-detection systems are in place to monitor all traffic: • At the perimeter of the personalization network • At critical points inside the personalization network

Section 5: System Security

5.1 General Requirements

Requirement	Test Procedure
The vendor must:	
a) Document security controls that protect cardholder data and the cloud-based provisioning network.	Examine documentation to identify security controls that protect CHD and the cloud-based provisioning network. Interview personnel to determine that the procedures are known and followed.
b) Ensure that any system used in the personalization process or in the cloud-based provisioning process is only used to perform its intended function—i.e., control personalization or cloud-based provisioning process activities.	Examine documentation to: • Identify systems and their functions that are used in the personalization process or in the cloud-based provisioning process. • Verify that systems and functions are only used to perform their intended function—i.e., control personalization or cloud-based provisioning process activities.
c) Change supplier-provided default parameters prior to or during installation in the production environment.	Examine configuration settings to verify they are different than what has been published as defaults coming with the product.
d) Encrypt non-console administrative access when it takes place from within the personalization network.	Examine services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access. Interview personnel and review documentation to identify non-console administrative access in the personalization network and verify that non-console administrative access is encrypted.
e) Synchronize clocks on all systems associated with personalization or cloud-based provisioning networks with an external time source based on International Atomic Time or Universal Time Coordinated (UTC).	Examine configuration standards and processes—e.g., external time synchronization sources—to verify that time-synchronization technology is implemented and kept current.
f) Restrict and secure access to system files at all times.	Examine access controls to system files to determine that access is restricted. Observe access attempts for both authorized and unauthorized individuals to verify that access is restricted as documented.
g) Ensure that virtual systems do not span different network domains.	Examine system-architecture documentation and configuration settings to verify that virtual systems do not span different network domains.

5.1 General Requirements

Requirement	Test Procedure
h) Ensure that all components of the personalization network physically reside within the HSA.	Examine system documentation and architecture diagrams to: • Identify components that make up the personalization network and HSA. • Verify that system components are resident within the HSA. Observe the physical network infrastructure to verify it conforms to the documented network diagram.
i) Ensure that PIN printing takes place on a dedicated network that is either separated from other networks by its own firewall or standalone—i.e., the printer and HSM are integrated—or that the PIN printer is directly attached to the HSM, which decrypts the PINs so that it cannot be intercepted.	Examine system documentation, including firewall rules and architecture diagrams to verify the PIN printer is: • Separated from other networks by its own firewall; or • Standalone—i.e., the printer and HSM are integrate—; or • Directly attached to the HSM.
j) Ensure that the access-control system complies with the system security requirements in this document.	Examine documentation and interview personnel to: • Identify controls associated with the access-control system. • Verify controls for the access-control system comply with system security requirements defined in this document.
k) Ensure that the access-control system is compliant to Section 6 of this document, “User Management and System Access Control.”	Examine access-control systems documentation to verify that controls are implemented in accordance with Section 6 of this document, “User Management and System Access Control.”

5.2 Change Management

Requirement	Test Procedure
The vendor must:	
a) Ensure that change-control procedures address, at a minimum: • Ensuring that requests for changes are submitted by authorized users • Identification of components that will be changed • Documentation of impact and back-out procedures • Attestation of successful testing, when required • Maintenance of an audit trail of all change requests • Record of whether or not the change was successful	Examine change-control policies and procedures to verify the following are defined: • Ensuring that requests for changes are submitted by authorized users • Identification of components that will be changed • Documentation of impact and back-out procedures • Attestation of successful testing, when required • Maintenance of an audit trail of all change requests • Record of whether or not the change was successful
b) Ensure that network and system changes follow a documented change-management process, and that the process is validated at least every 12 months.	Examine a sample of changes to network and system components to verify changes follow the documented change-management process. Examine documentation and supporting evidence to verify that the change-management process is validated at least every 12 months.
c) Ensure all changes are approved by the CISO or authorized individual prior to deployment.	Examine a sample of changes to network and system components to verify changes were approved by the CISO or authorized individual before deployment.
d) Ensure that the change-management process includes procedures for emergency changes.	Interview personnel and review documentation to verify that the change-management process includes procedures for emergency changes. Examine a sample (if applicable) of emergency changes to verify they followed procedures.
e) Implement version identification and control for all software and documentation.	Examine documentation to verify the organization's change-management policies and procedures include requirements for version control and identification.
f) Ensure that the version identification is updated when a change is released or published.	Examine documentation to verify that version identification is updated when a change is released or published.
g) Implement a controlled process for the transfer of a system from test mode to live mode, and from live mode to test mode.	Examine documentation to verify the existence of a controlled process for the transfer of a system from test mode to live mode, and from live mode to test mode.
h) Ensure that both development and production staff must sign off on the transfer of a system from test to live, and from live to test. This sign-off must be witnessed under dual control.	Examine a sample of change-management documentation for system transfers from test to live and from live to test to verify that: • Both development and production staff sign off on the transfer of a system from test to live, and from live to test; and • This sign-off must be witnessed under dual control.

5.3 Configuration and Patch Management

Requirement	Test Procedure
The vendor must:	
a) Implement a documented procedure to determine whether applicable patches and updates have become available.	Examine documented procedures to verify that they include determination of whether applicable patches and updates have become available.
b) Make certain a process is implemented to identify and evaluate newly discovered security vulnerabilities and security patches from software vendors.	Examine documentation to verify that processes are defined to identify new security vulnerabilities and obtain security patches from appropriate software vendors.
c) Ensure that secure configuration standards are established for all system components.	Examine documentation to verify that secure configuration standards are established for all system components.
d) Ensure that the configuration standards include system hardening by removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Examine configuration standards and verify there are requirements to remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
e) Ensure that the configuration of all system components associated with data transmission, storage, and personalization are validated against the authorized configuration monthly.	Examine documentation to verify all system components associated with data transmission, storage, and personalization are validated against the authorized configuration monthly.
f) Ensure all systems used in support of both personalization and cloud-based provisioning networks are actively supported in the form of regular updates.	Examine documentation to verify that all systems used in support of both personalization and cloud-based provisioning networks are actively supported in the form of regular updates.
g) Evaluate and install the latest security-relevant patches for all system components within 30 days of their release (if they pass validation tests).	Examine a sample of system components and related software to: • Compare the list of security patches installed on each system component to the most recent vendor security-patch list; and • Verify the applicable vendor-supplied security patches are installed within 30 days of their release.
h) Verify the integrity and quality of the patches before application, including source authenticity.	Examine procedures to verify that a process is defined, the source of the patches is authenticated, and that the quality of the patch is validated before installation. Interview personnel to verify that patch installation process conforms to written procedures.

5.3 Configuration and Patch Management

Requirement	Test Procedure
i) Make a backup of the system being changed before applying any patches. The backup must be securely stored.	Examine a sample of system components and related software and compare the list of security patches installed against backup file entries to verify backups are performed. Observe security control mechanisms for backups and verify they are in place and active. Interview personnel and review patch update procedures to verify backups are required before applying patches. Identify controls for secure storage.
j) Implement critical patches to all Internet-facing system components within 7 business days of release. When this is not possible, the CISO, IT Security Manager, and IT director must clearly record that they understand that a critical patch is required and authorize its implementation within a maximum of 30 business days.	Examine policies and procedures related to security-patch installation to verify processes are defined for installation of critical patches to Internet-facing system components within 7 business days of release. Examine a sample of Internet-facing system components and compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify that: • Applicable, critical vendor-supplied security patches are installed within 7 days of release. OR • Supporting documentation is in place recording that the CISO, IT Security Manager, and IT director understand and accept the risk and ensure implementation occurs within 30 business days.
k) Ensure that emergency hardware and software implementations comply with the procedures and validation requirements established for emergency implementations.	Examine the documented procedures for emergency hardware and software implementation. Examine a sample of emergency and hardware and software changes to verify they follow documented procedures.
l) Ensure that emergency hardware and software implementations follow the configuration and patch management requirements in this section.	Examine a sample of emergency hardware and software implementations to verify that all configuration and patch management procedures are followed. Interview personnel and review documentation to verify that emergency changes followed stated configuration and patch management requirements.

5.4 Audit Logs

Requirement	Test Procedure
The vendor must:	
a) Ensure that audit logs exist for all networks and network devices in the vendor environment and for systems and applications connected to the cloud-based provisioning network. This includes operating system logs, security software logs, product logs, and application logs containing security events.	Examine all networks and network devices in the vendor environment—including systems and applications connected to the cloud-based provision network—to ensure that audit logs are enabled and function correctly. Interview personnel to ensure that audit trails are enabled and active for identified items, including operating system logs, security software logs, product logs, and application logs containing security events.
b) Ensure that audit logs include at least the following components: • User identification • Type of event • Valid date and time stamp • Success or failure indication • Origination of the event • Identity or name of the affected data, system component, or resources • Access to audit logs • Changes in access privileges	Examine the audit logs to ensure they contain the required components.
c) Ensure that procedures are documented and followed for audit log review and reporting of unusual activity. Log reviews may be automated or manual and must include authentication, authorization, and directory servers. At a minimum, log review frequency must adhere to the following: • Immediate (real time) response to threats designated as alerts for high risk associated events • Daily review of IDS and IPS systems • Weekly review for wireless access points and authentication servers • Monthly review for routers • Monthly review of user account audit logs for databases, applications, and operating systems	Examine policies and procedures to verify that procedures are defined for reviewing and reporting of unusual activity and include requirements for log frequency as stated in the requirement. Examine a sample of each type of log and frequency and obtain evidence that log review was performed. Unless specified by the procedures, the order of assessment is at the discretion of the auditor. Interview personnel to verify the stated policies and procedures are known and followed.

5.4 Audit Logs

Requirement	Test Procedure
d) Verify at least once a month that all systems are meeting log requirements.	Examine evidence that demonstrates monthly verification that systems are meeting the logging requirements. Interview personnel to ensure they verify at least monthly that systems are meeting the logging requirements.
e) Ensure that logs for all critical and cloud-based provisioning systems are backed up daily, secured, and retained for at least one year. Logs must be accessible for at least three months online and one year offline.	Examine logs for critical and cloud-based provisioning systems to: • Verify that logs are securely backed up daily. • Verify that logs are accessible online for at least three months. • Verify that logs are retained offline for one year. For both online and backed-up audit logs, review relevant security controls to ensure access is appropriate.
f) Protect and maintain the integrity of the audit logs from any form of modification.	Examine relevant security controls for both online and backed-up audit logs to ensure the ability to modify or delete audit logs is prohibited.
g) Implement a security-incident and event-logging framework for its organization.	Examine documentation to ensure existence of an incident-response process. Interview personnel to verify they are aware of their security-incident and event-logging framework. Examine log entries to verify framework is active and in use.

5.5 Backup and Recovery for Mobile Provisioning Networks

Requirement	Test Procedure
a) The backup and recovery procedures for mobile provisioning must be documented.	Examine documentation to verify existence of procedures supporting the backup and recovery of the mobile provisioning network.
b) The procedures must include the backup and recovery of hardware and software that support the provisioning activity.	Examine documented procedures to verify they include requirements for the backup and recovery of hardware and software that support the provisioning activity.
c) The procedures must differentiate between and address short-term and long-term service outages.	Examine documented procedures to verify they include requirements for both short-term and long-term service outages.
d) The vendor must protect backup copies from intentional or unintentional modifications or destruction.	Examine applicable access-control lists to ensure the ability to modify or delete audit backups is prohibited.

5.5 Backup and Recovery for Mobile Provisioning Networks

Requirement	Test Procedure
e) Backups, whether stored within or outside of the HSA, must be encrypted and protected equivalent to the primary data as delineated in Section 3.1, "Classifications."	Interview personnel and review documentation to identify backups and their data classification. Examine documentation about the system used to protect backups to ensure that it is protected equivalent to the primary data—e.g., including the vendor, type of system/process, and the encryption algorithms used to encrypt backups. Examine a sample of backups and verify strong cryptography, with associated key-management processes and procedures where used.
f) Controls must be established to prohibit creating unauthorized backups.	Examine existing security controls to verify they prohibit the creation of unauthorized backups.
g) If the recovery procedures include an alternate processing site, the alternate site must be approved for provisioning before the provisioning service may begin at the alternate site.	Interview personnel and review documentation to identify alternate processing sites. Examine documentation to verify that the alternate site has been approved to perform provisioning services before the provisioning occurs.

5.6 Software Design and Development

Requirement	Test Procedure
5.6.1 General	
The vendor must:	
a) Document the design, development, and maintenance processes.	Examine documentation of design, development, and maintenance processes to verify existence.
b) Ensure these activities are based on industry standards and security is an integral part of the software life cycle process. Web applications must be developed based on secure coding guidelines such as: the OWASP Guide, SANS CWE Top 25, and CERT Secure Coding.	Examine policies and procedures to verify that: • The software life cycle process aligns with industry standards; and • Web application development is based on recognized secure coding guidelines.
c) Document all software components for each system and describe the functionality provided.	Examine documentation to verify it covers software components for each system and describes how they function.
d) Protect any software backup copies from accidental destruction.	Examine a sample of backups to verify they are adequately protected from accidental destruction.

5.6 Software Design and Development

Requirement	Test Procedure
5.6.2 Design	
a) The vendor must document the flow of personalization data within the environment from the receipt/generation to end of lifecycle.	Examine data-flow diagrams for personalization data within the environment from the receipt/generation to end of lifecycle. Interview personnel to verify documentation includes information to support the receipt/generation of data to the end of the lifecycle.
5.6.3 Development	
The vendor must:	
a) Ensure access to source code for applications used on the personalization network is restricted to authorized personnel only.	Interview personnel to identify locations of application source code. Examine system configuration and access control lists to identify users and processes that have access to source code components. Examine approval records to ensure access to source code was authorized.
b) Ensure that in-house developed personalization software logs any restart (and details associated with that restart event).	Interview personnel to identify in-house developed personalization logs. Examine log configuration settings to verify restart actions are included. Examine a sample of personalization logs to verify restart actions (and details associated with that restart event) are captured.
c) Ensure that in-house developed personalization software enforces authorization at restart.	Examine restart procedures to ensure in-house developed personalization software enforces authorization at restart.
d) Ensure separation of duties exists between the staff assigned to the development environment and those assigned to the production environment.	Examine policies and procedures to verify a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. Examine access-control settings to verify that access controls are in place to enforce separation personnel assigned to the development/test environments and the production environment(s).
e) Ensure that software source code is restricted to only authorized staff. Staff access of source code must follow a documented process. The authorizations and approvals must be documented.	Examine system configuration and access-control lists to identify users and processes that have access to source code components. Examine documented policies and procedures for granting access to source code and verify authorizations and approvals are required. Examine a sample of access request records to verify the access followed the documented process and was authorized.

5.7 Use of Web Services for Issuer Interfaces

Requirement	Test Procedure
The vendor must ensure that:	
a) Mutual authentication is required. It must be implemented using either client and server X.509 certificates issued and signed by a trusted Certificate Authority (CA) or a VPN constructed in accordance with Section 4.6.2, "Virtual Private Network."	Examine documentation for web services for issuer interfaces to identify mutual authentication is used. Examine system configurations and settings to ensure X.509 certificates, signed by a trusted Certificate Authority (CA) or VPN, are used. If VPN is used, examine the VPN configuration and settings to ensure they adhere to requirements in Section 4.6.2.
b) The most current approved version of TLS is used to secure the connection and requires the following minimum cryptography standards. Refer to the Normative Annex A section of this document for acceptable algorithms and key strengths. • The strongest encryption reasonable must be implemented for the application if both client and server support higher than these minimum standards. • Implementations must disallow cipher renegotiation within an established TLS session. • Integrity protection must be provided through the use of the SHA-2 or higher algorithm.	Examine system configuration settings to verify: • Strong cryptography is used for the application. • Implementations disallow cipher renegotiation within an established TLS session. • Integrity protection is provided through the use of the SHA-2 or higher algorithm.
c) All web services client and servers that are exposed to untrusted networks are protected by a suitably configured application firewall supporting message validation.	Examine network diagrams and settings to identify interfaces where web services are exposed to untrusted networks—e.g., Internet. Examine network system configurations and review applicable firewall rule sets to verify traffic is restricted and message validation is required.
d) Implement controls to ensure message integrity.	Examine network documentation to identify controls to support message integrity. Examine network system configurations and review applicable firewall rule sets to verify message integrity is ensured.

5.8 Software Implementation

Requirement	Test Procedure
The vendor must:	
a) Establish and maintain a documented software release process. Quality assurance must include testing of the code for security issues prior to any software releases.	Interview personnel to verify a software release process exists and is in use. Examine documentation to verify a quality assurance process is required as part of the software release process and testing of code is performed before software is released. Examine a sample of recent software updates and identify evidence to verify testing of the code was performed.
b) For internally developed software, ensure that security testing includes verification that temporary code, hard-coded keys, and suspicious code are removed.	Examine policies/procedures to identify testing processes for internally developed software. Examine documentation to verify it addresses removing temporary code, hard-coded keys, and suspicious code. Examine a sample of recent internally developed software updates and verify steps to remove temporary code, hard-coded keys, and suspicious code were performed.
c) Ensure all software implementation complies with Section 5.2, "Change Management."	Examine a sample of recent software updates to verify they comply with Section 5.2, "Change Management."
d) Test software prior to implementation to ensure correct operation.	Examine a sample of recent software updates and verify evidence exists that testing software prior to implementation was performed.
e) Prevent debugging within production environment.	Interview personnel to identify the controls in place to prevent debugging in the production environment. Examine policies/procedures to verify they address prevention of debugging within production environment.
f) Have a predefined PC device configuration for PC devices used within the HSA.	Examine configuration standards for PC devices used within the HSA. Examine a sample of PC devices used in the HSA and obtain evidence that the devices have been configured according to specified configuration standards.
g) Implement an approval process for all software beyond the standard PC device configuration for PC devices used within the HSA.	Examine polices/procedures to identify the approval process for software used within the HSA. Examine a sample of recent software updates and verify approvals were required.
h) Ensure no unauthorized software can be installed.	Interview personnel to identify controls established to prevent unauthorized software from being installed. Examine the implementation of applicable controls to verify they are in place and in use.

5.8 Software Implementation

Requirement	Test Procedure
i) Ensure all software is transferred from development to production in accordance with the change-control process.	Examine policies/procedures to identify change-control processes for software, including the methods used to transfer software from development to production. Examine a sample of recent software updates and verify steps to transfer software from development to production were performed.

Section 6: User Management and System Access Control

6.1 User Management

Requirement	Test Procedure
The vendor must:	
a) Ensure that procedures are documented and followed by security personnel responsible for granting access to vendor's networks, applications, and information.	Interview personnel to identify both those authorized to perform, and the processes followed for granting access to vendor's network, applications, and information. Examine documented procedures to ensure they address granting access to vendor's networks, applications, and information. Examine a sample of recent access requests to verify they were processed by authorized personnel and in accordance with documented procedures.
b) Restrict approval and level of access to staff with a documented business need before access is granted.	Examine policies/procedures to ensure they address that: • Approval and level of access must be restricted to those with a documented business need before access is granted; and • Documented approvals of access in place must be retained while the account is active.
c) Retain documented approvals while the account is active, at a minimum.	Examine a sample of access requests to verify: • Users obtained associated approvals, and • Approval documentation has been retained for all active accounts.
d) Restrict systems access by unique user ID to only those individuals who have a business need.	Examine a sample of user accounts to verify each individual associated with a unique user ID has a documented, valid business need for the system access.
e) Incorporate multi-factor authentication for all non-console access into HSA systems for personnel with administrative access.	Interview personnel to verify that multi-factor authentication is used for all non-console access into HSA systems for personnel with administrative access.
f) Incorporate multi-factor authentication for all remote network access (both user and administrator and including third-party access for support or maintenance) originating from outside the entity's network.	Examine a sample of remote network access system documentation and configuration settings to verify multi-factor authentication is used for remote network access connections. Observe a sample of remote network access processes to verify multi-factor authentication is used.

6.1 User Management

Requirement	Test Procedure
g) Only grant individuals the minimum level of access sufficient to perform their duties.	Interview security administration personnel to verify access is granted based on least-privilege principles sufficient to perform their duties. Examine policies/procedures to verify they require that access be granted based on least-privilege principles sufficient to perform their duties. Examine a sample of recent access requests to verify user access is limited to least privilege and based on documented business need.
h) Make certain that systems authentication requires at least the use of a unique ID and password.	Examine policies/procedures for system access to verify they require at least the use of a unique ID and password. Examine system authentication settings and verify that user IDs in the system are unique and in order to gain access, a password is required.
i) Restrict administrative access to the minimum number of individuals required for management of the system.	Interview management to understand the minimum number of administrative user resources required to support the personalization environment. Examine user ID lists and security privileges to identify users with administrative access and verify the number of users with administrative aligns with management's expectations.
j) Ensure that group, shared, and generic accounts and passwords are disabled wherever the system supports unique values.	Examine polices/procedures to verify they require that group, shared, and generic accounts and passwords are disabled wherever the system supports unique values. Examine a sample of system components and user ID lists to verify group, shared, and generic accounts and passwords are disabled.
k) Ensure that where generic administrative accounts cannot be disabled, these accounts are used only when unique administrator sign-on credentials are not possible and only in an emergency.	Interview system administration personnel to identify existence of generic accounts and how their usage is controlled. Examine policies/procedures for the management of generic administrative accounts that cannot be disabled. Verify these accounts are used only when unique administrator sign-on credentials are not possible and only in an emergency. Examine system security event log to identify when applicable generic administrative accounts were used and verify there is supporting documentation that authorizes their use in an emergency.
l) Ensure that when generic administrative accounts are used, the password is managed under dual control where no individual has access to the full password. Each component of the password must comply with the password control requirements in Section 6.2 below except for password length when an exception condition exists.	Interview system administration personnel to verify password-management practices require that generic administrative passwords are managed under dual control and in accordance with Section 6.2 Examine policies/procedures for the management of generic administrative account passwords and verify procedures require that such passwords be managed under dual control and in accordance with Section 6.2.

6.1 User Management

Requirement	Test Procedure
m) Validate all system access at least quarterly.	Interview personnel to verify system access is re-validated at least quarterly. Examine validation evidence to verify the activity is performed.
n) Revalidate card production staff access to any systems upon a change of duties.	Interview personnel to verify card production staff access is revalidated when the employee has a change in duties. Examine a sample of HR transfer records and verify that revalidation was performed.
o) Ensure that access controls enforce segregation of duties.	Interview personnel to identify that policies/procedures support segregation of duties. See glossary definition, “Segregation of Duties,” in the Security Requirements.
p) For cloud-based provisioning, restrict issuer access and privileges to only the issuer’s own cardholder data.	Interview personnel and identify controls that restrict issuer access and privileges to only the issuer’s own cardholder data. Examine access-control settings to ensure access conforms to stated policies.
q) Strictly limit privileged or administrative access and ensure such access is approved by both the user’s manager and the IT Security Manager.	Interview personnel to identify controls that limit privileged or administrative access. Examine access-control settings to ensure access confirms to stated policies. Examine a sample of administrative-access requests and verify access was approved by the user’s manager and IT Security Manager.
r) Establish management oversight of privileged access to ensure compliance with segregation of duties.	Interview personnel to identify controls that provide oversight of privileged access and compliance with segregation of duties policies. Examine policies/procedures to verify they require oversight of privileged access that ensures compliance with segregation of duties. Examine evidence—e.g., audit logs—to verify management oversight is performed.
s) Ensure that all privileged administrative access is logged and reviewed weekly.	Examine policies/procedures to verify that they require weekly review of privileged administrative access. Examine evidence—e.g., access logs—to verify reviews are performed according to policies and procedures.

6.2 Password Control

Requirement	Test Procedure
6.2.1 General	
The vendor must:	
a) Implement a policy and detailed procedures relating to the generation, use, renewal, and distribution of passwords.	Examine policy and detailed procedures to identify processes for generation, use, renewal, and distribution of passwords.
b) Implement procedures for handling lost, forgotten, and compromised passwords.	Examine policy and detailed procedures to identify processes for handling lost, forgotten, and compromised passwords. Interview system administrators to validate adherence to procedures.
c) Distribute password procedures and policies to all users who have access to cardholder data, or any system used as part of the personalization process.	Examine procedures for disseminating password procedures and policies to users with access to cardholder data or any system used as part of the personalization process. Interview a sample of user population to verify password procedures and policies were distributed.
d) Ensure that only users with administrative privileges can administer other users' passwords.	Examine procedures for managing user IDs and verify that only users with administrative privileges can administer user passwords. Observe a sample of user password resets and verify only users with administrative privileges can perform a reset.
e) Not store passwords in clear text.	Examine system documentation and configuration settings to verify that passwords are not stored in clear text. Examine a sample of system components and their password files to verify that passwords are unreadable during storage.
f) Change all default passwords.	Examine a sample of system components and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords. Verify that ALL default passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)
6.2.2 Characteristics and Usage	
The vendor must ensure that:	
a) Systems are configured so that newly issued and reset passwords are set to a unique value for each user.	Interview personnel to verify newly issued and reset passwords are set to a unique value for each user. Examine a sample of system configuration settings to verify newly issued and reset passwords are set to a unique value for each user.

6.2 Password Control

Requirement	Test Procedure
b) Newly issued passwords are changed on first use.	Examine system configuration settings to verify newly issued passwords are changed on first use.
c) "First use" passwords expire if not used within 24 hours of distribution.	Examine system configuration settings to verify that first-time passwords are set to expire if not used within 24 hours.
d) Systems enforce password lengths of at least 12 characters, with an exception for operating systems that do not support 12 characters. Passwords can never be less than a minimum length of 8 characters or an equivalent strength.	Examine the system configuration settings for a sample of system components to verify that password parameters are set to require a minimum length of at least 12 characters or meet the exception condition.
e) Passwords consist of using a combination of at least three of the following categories: • Upper-case letters • Lower-case letters • Numbers • Special characters	Examine the system configuration settings for a sample of system components to verify that user passwords are set to require at least three of the following categories: • Upper-case letters • Lower-case letters • Numbers • Special characters
f) Passwords are not the same as the user ID.	Examine the system configuration settings for a sample of system components to verify passwords cannot be the same as the user ID.
g) Passwords are not displayed during entry.	Observe authentication procedures for entering a password and verify the password is not displayed as it is entered.
h) Passwords are encrypted during transmission and rendered unreadable when stored.	Examine password configurations to verify passwords are encrypted during transmission and rendered unreadable when stored. Examine a sample of passwords in transit and in storage to verify password values are not in clear text.
i) Passwords have a maximum life not to exceed 90 days and a minimum life of at least one day.	Examine the system configuration settings for a sample of system components 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.
j) When updating passwords, the system prevents users from using a password that is the same as one of their previous four passwords.	Examine the system configuration settings for a sample of system components to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.

6.2 Password Control

Requirement	Test Procedure
k) The user's identity is verified prior to resetting a user password.	Interview system administration personnel to verify the user's identity is verified prior to resetting a user password. Examine password reset procedures to verify the user's identify is verified prior to resetting a user password. Observe a password reset request to verify user identify is verified.
l) Authentication credentials to the tokenization process are secured to prevent unauthorized disclosure and use.	Interview personnel and review policies/procedures to identify controls that protect authentication credential to the tokenization process.

6.3 Session Locking

Requirement	Test Procedure
The vendor must:	
a) Enforce the locking of an inactive session within a maximum of 15 minutes. If the system does not permit session locking, the user must be logged off after the period of inactivity.	Examine the system configuration settings for a sample of system components to verify that system/session inactivity time out has been set to 15 minutes or less. Observe a user session to verify the user is logged out after 15 minutes if the system does not permit session locking.
b) Enforce a manual log-out process where manufacture and personalization equipment does not have the ability to automatically log off a user.	Interview personnel to verify a manual log-out process is defined and in use when mechanisms do not exist to automatically log off a user.

6.4 Account Locking

Requirement	Test Procedure
a) Accounts that have been inactive for a specified period (with a maximum of 90 days) must be removed from the system.	Examine user accounts to verify that any inactive accounts over 90 days old are either removed or disabled.

6.4 Account Locking

Requirement	Test Procedure
b) Systems must enforce the locking of a user account after a maximum of six unsuccessful authentication attempts.	Examine the system configuration settings for a sample of system components to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts.
c) Locked accounts must only be unlocked by the security administrator. Alternatively, user accounts may be unlocked via automated password reset mechanisms. Challenge questions with answers that only the individual user would know must be used. 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.	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. Interview administrators to verify that an account is unlocked only after the identity of the user is verified. Examine polices/procedures for automated password reset mechanisms to verify they require conformance to the stipulated criteria. Observe the mechanism including the challenge/response criteria, for accounts that can be unlocked via an automated reset mechanism, to verify the questions are designed as stipulated in the requirement.
d) A user's account must be locked immediately upon that user leaving the vendor's employment until it is removed.	Examine policies/procedures to verify that user access is locked when the user leaves the vendor's employment. Examine a record sample of users leaving vendor employment to verify that their account(s) were locked immediately.
e) A user's account must be locked immediately if that user's password is known or suspected of being compromised.	Examine policies/procedures to verify that any user account is immediately locked if the password is known or suspected of being compromised.
f) The user account logs including but not limited to the following must be reviewed at least twice each month for suspect lock-out activity: • Remote access • Database • Application • OS	Examine the system configuration settings and audit logs for a sample of system components to verify that lock-out activity is logged. Examine documented procedures to verify access logs are reviewed at least weekly to identify suspicious activity.

Section 7: Key Management: Secret Data

7.1 General Principles

Requirement	Test Procedure
a) A written description of the vendor's cryptographic architecture must exist. In particular, it must detail all the keys used by each HSM. The key description must describe the key usage.	Examine the written description of the vendor's cryptographic architecture to verify that it includes details of all keys used by each HSM and a description of usage for each key.
b) 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. The only exceptions to these principles involve those keys that are managed as cryptograms or stored within an SCD.	Examine polices/procedures for key management to verify that they require the implementation of dual control and split knowledge for cryptographic key management.
c) Effective implementation of these principles must enforce the existence of barriers beyond procedural controls to prevent any one individual from gaining access to key components or shares sufficient to form the actual key.	Interview personnel to identify that controls exist beyond procedural controls to prevent any one individual from gaining access to key components or shares sufficient to form the actual key. Examine a sample of evidence to verify controls are in place and functioning to prevent any one individual from gaining access to key components or shares sufficient to form the actual key.
d) Where clear 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. These computers must be dedicated and be hardened and managed under dual control at all times.	Examine documented procedures for all key-handling methods to verify that where clear key components or shares pass through a PC or other equipment, the equipment is: • Powered off when not in use; • Not connected to any network; • Dedicated and hardened; and • Managed under dual control at all times.
e) Keys used for protection of keying material or other sensitive data must meet the minimums delineated in Annex A.	Examine documentation—e.g., cryptography architecture—to identify keys used for the protection of keying material and other sensitive data and to verify the keys adhere to the minimums delineated in Annex A.
f) All key-encrypting keys used to transmit or convey other cryptographic keys must be at least as strong as the key being transmitted or conveyed.	Interview personnel to identify key-encrypting keys used to transmit or convey other cryptographic keys. Examine documentation to verify identified keys are at least as strong as the keys being transmitted or conveyed.

7.1 General Principles

Requirement	Test Procedure
g) Cryptographic keys must not be hard-coded into software.	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. Examine the software configuration—for example, shell scripts, command files, communication scripts, software code etc.—for a sample of system components to verify that cryptographic keys are not embedded.
h) Audit trails must be maintained for all key-management activities.	Examine policies and procedures to verify that all key-management activities and all activities involving clear-text key components must be logged. Examine a sample of key-management audit trails to verify existence.
i) Key-management activities must be performed by vendor or issuer staff.	Examine documented key-management policies and procedures verify that all functions are performed by vendor or issuer staff. Interview responsible personnel to verify that all functions are performed by vendor or issuer staff.
j) Key-management activities must only be performed by fully trained and authorized personnel.	Examine documented procedures and processes to verify that only authorized personnel have the ability to perform key-management activities. Interview responsible personnel to ensure they have undergone relevant training for the key-management functions they perform.
k) Digital certificates used in conjunction with cloud-based provisioning products or services must be issued either from a trusted Certificate Authority (CA) or directly under an issuer or application provider PKI.	Examine documentation to identify digital certificates used in conjunction with cloud-based provisioning products or services. Interview personnel to verify the certificates have been issued either from a trusted Certificate Authority (CA) or directly under an issuer or application provider PKI.

7.1 General Principles

Requirement	Test Procedure
l) All key-management activities must be documented, and all activities involving clear key components must be logged. The log must include: • Unique identification of the individual that performed each function • Date and time • Function • Purpose	Interview personnel to verify that key-management activities are documented and 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 Examine a sample of audit logs and other documentation to verify that key-management activities are documented and activities involving clear-text key components are logged, and that the logs include: • Unique identification of the individual that performed each function • Date and time • Function performed • Purpose

7.2 Symmetric Keys

Requirement	Test Procedure
Ensure that:	
a) Symmetric keys only exist in the following forms: • As plaintext inside the protected memory of a secure cryptographic device • As a cryptogram • 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.	Examine documented procedures and system configurations to verify symmetric keys exist only in the following forms: • As plaintext inside the protected memory of a secure cryptographic device • As a cryptogram • 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.
b) Key components for each specific custodian must be stored in a separate, secure container that is accessible only by the custodian and/or designated backup(s).	Examine a sample of key components and verify for each specific custodian that the keys are stored in a separate, secure container that is only accessible by the custodian and/or designated backup(s). This should include verification of access to physical keys, override keys, and/or PIN codes to access the containers.

7.2 Symmetric Keys

Requirement	Test Procedure
c) No single person shall be able to access or use all components or a quorum of shares of a single secret cryptographic key.	Examine a sample of key components and verify no single person has access to or can use all components or have access to a quorum of shares of a single secret cryptographic key.

7.3 Asymmetric Keys

Requirement	Test Procedure
Ensure that:	
a) Private keys exist only in the following forms: • As plaintext inside the protected memory of a secure cryptographic device • As a cryptogram • As two or more components or as part of an "m of n" sharing scheme where the value of "m" is at least 2; managed using the principles of dual control and split knowledge	Examine documented procedures to verify private keys exist only in the following forms: • As plaintext inside the protected memory of a secure cryptographic device • As a cryptogram • As part of an "m of n" sharing scheme where the value of "m" is at least 2
b) Key components for each specific custodian must be stored in a separate, secure container that is accessible only by the custodian and/or designated backup(s).	Examine a sample of key components and verify for each specific custodian that key components are stored in a separate, secure container that is accessible only by the custodian and/or designated backup(s).
c) No single person shall be able to access or use all components or a quorum of shares of a single private cryptographic key.	Examine documented procedures to verify that a single person cannot access or use all components or a quorum of shares of a single private cryptographic key. Interview responsible personnel to verify that the implemented method(s) ensure that no single person can access or use all components or a quorum of shares of a single private cryptographic key.

7.3 Asymmetric Keys

Requirement	Test Procedure
d) Public keys must have their authenticity and integrity ensured. In order to ensure authenticity and integrity, a public key must be encrypted, or if in plaintext form, must exist only in one of the following forms: • Within a certificate, • Within a PKCS#10, • Within a SCD, or • With a MAC (message authentication code) created using the algorithm defined in ISO 16609.	Examine documented procedures for public keys to verify that public keys must exist only in one of the following forms: • Within a certificate, • Within a PKCS#10, • Within an SCD, or • With an associated MAC (message authentication code) created using the algorithm defined in ISO 16609. Interview responsible personnel to verify that the implemented method(s) ensure the authenticity and integrity of public keys.
e) Asymmetric keys also adhere to: • The payment system requirements for obtaining the issuer certificate • The payment system specification for asymmetric keys	Examine documentation to identify requirements for obtaining an issuer certificate and the associated payment system(s) specifications. Examine for a sample of asymmetric keys evidence to verify requirements were met.

7.4 Key-Management Security Administration

Requirement	Test Procedure
The secure administration of all key-management activity plays an important role in terms of logical security. The following requirements relate to the procedures and activities for managing keys and key sets.	
7.4.1 General Requirements	
a) The vendor must define procedures for the transfer of key-management roles between individuals.	Examine documented procedures to verify that procedures for transferring key-management roles between individuals are defined**.** Interview responsible personnel in applicable key-management roles to verify they are aware of and are following the documented procedures.

7.4 Key-Management Security Administration

Requirement	Test Procedure
b) All physical equipment associated with key-management activity, such as physical keys, authentication codes, smart cards, and other device enablers—as well as equipment such as personal computers—must be managed following the principle of dual control.	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. Observe the process of accessing physical equipment to verify that dual control is required to access or perform key-management functions.
7.4.2 Key Manager	
a) There must be a nominated Key Manager with overall responsibility for all activities relating to key management.	Examine documentation to verify the Key Manager has overall responsibility for all activities relating to key management.
b) CISO must approve the Key Manager for the position within the vendor.	Examine approval authorization documentation to verify CISO (or delegate) approved the Key Manager.
c) The Key Manager must:	
i. Have a nominated deputy.	Interview the Key Manager to verify that the Key Manager has a nominated deputy. Examine documentation to identify the nominated deputy for the Key Manager.
ii. Own and be responsible for ensuring that all key-management activity is fully documented.	Interview the Key Manager to verify that key-management activity is fully documented. Examine documented policies and procedures for appropriateness.
iii. Be responsible for ensuring that all key-management activity is carried out in accordance with the documented procedures.	Interview the Key Manager to verify that all key-management activity is carried out in accordance with documented procedures.
iv. In collaboration with the personnel department, vet all key custodians to ensure their suitability for the role.	Examine policies/procedures to identify vetting process for key custodians to ensure they are suitable for their role. Examine documented evidence for a sample of key custodians that supports the vetting process.
v. Be an employee of the vendor. This also applies to the deputy key manager.	Examine employee rosters for the organization and verify that key custodians and the deputy key manager are employees of the vendor.
d) The Key Manager must be informed immediately of any security breach or loss of integrity relating to key activities.	Examine policies/procedures to identify process for reporting security breaches or other incidents associated with key activities to ensure the Key Manager is included in the process.
e) The Key Manager must be responsible for ensuring that:	

7.4 Key-Management Security Administration

Requirement	Test Procedure
i. All key custodians have been trained with regard to their responsibilities, including incremental changes, and this forms part of their annual security training.	Examine policies/ procedures to verify the requirement for annual security training for key custodians and that it includes key-custodian responsibilities. Examine evidence for a sample of key custodians that verifies annual training is performed.
ii. Each custodian signs a statement, or is legally bonded, acknowledging that they understand their responsibilities.	Examine a sample of key custodians' signed statements 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.	Interview key custodians to verify that they report to a different manager if the custodians together form a threshold to create a key. Interview key custodians to verify that key custodians do not report to the Key Manager if the Key Manager is also a key custodian—because that would form a threshold to create a key. Examine personnel organization charts to verify applicable key custodians report to different managers.
f) The Key Manager must not have the right to override operations of the key custodians or perform activities for other key custodians.	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.
7.4.3 Key Custodians	
a) 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.	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. Interview key custodian personnel to verify the documented roles and responsibilities allow performance of required activities on a step-by-step basis.
b) The identity of individual custodians must be restricted on a need-to-know basis and may not be made available in generally available documentation.	Interview personnel to verify that identification of key custodians is based on a need-to-know basis and not identified in general documentation.
c) The suitability of personnel must be reviewed on an annual basis.	Examine documentation to verify that primary and backup key custodians are reviewed annually for suitability to the role.
d) The key custodians must be employees of the vendor and never temporary staff or consultants.	Examine documentation to verify that key custodians and their backups are employees of the vendor. Interview a sample of key custodians to very they are employees of the vendor.

7.4 Key-Management Security Administration

Requirement	Test Procedure
e) They 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.	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. Examine a sample of signed statements for key custodians to verify they acknowledge understanding of their responsibilities for safeguarding key components, shares, or other keying materials entrusted to them.
f) Only fully trained key custodians and their backups may participate in key-management activities.	Examine policies/ procedures to verify that they require key custodians and their backups are fully trained in key-management activities. Interview key custodians (and backups) to ensure training was required prior to performing key-management activities.
g) Physical barriers must exist to ensure that no key custodian has access to sufficient components or shares to form the clear key.	Interview personnel to identify the physical barriers that exist to ensure no key custodian has access to sufficient components or shares to form the clear key. Observe physical barriers to ensure they are in place and active.
7.4.4 Key-Management Device PINs *In relation to PINs and pass-phrases used with key-management devices:*	
a) If PINs or pass-phrases are stored, a copy of any PIN or pass-phrase, needed to access any device required for any key-management activity, must be stored securely (for recovery purposes).	Interview personnel to identify secure storage requirements for PIN or pass-phrases. Examine locations where the PIN or pass-phrase is stored and ensure it is stored securely.
b) Only those individuals needing access to a device must have access to the PIN or pass-phrase for that device.	Interview personnel to ensure that access to the PIN or pass-phrase is limited to only those person(s) needing access to the device.
c) 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.	Examine policy regarding using PINs and pass-phrases to access key-management devices to verify that the policy includes the length and character-mix of such PINs and pass-phrases, and the frequency of change. Examine a sample of system settings to verify composition rules are enforced and the frequency of PIN/pass phrase change aligns with policy.

7.4 Key-Management Security Administration

Requirement	Test Procedure
d) All equipment associated with key-management activity, such as brass keys and smart cards, must not be in the control or possession of any one individual who could use those tokens to enable the key-management activity under single control. These tokens must be secured in a manner similar to key components, including the use of access-control logs for when removed or placed into secure storage.	Interview personnel to identify controls to prevent key-management activity under single control. Examine key-management activity audit logs to verify dual control was required for applicable activity.

7.5 Key Generation

Requirement	Test Procedure
a) Generate keys and key components 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) PUB 800-22.	Examine key-management documentation including, where necessary, documentation of the secure cryptographic devices 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.
b) Key generation must take place in a hardware security module (HSM) that has achieved PCI approval or FIPS 140-2 or 140-3 Level 3 or higher certification for physical security. *During operation, the HSM must utilize a security algorithm that complies with payment system requirements as defined in Annex A.*	Interview personnel to verify that: • Key generation takes place in a secure cryptographic device—e.g., HSM. • The HSM has achieved PCI approval or FIPS 140-2 Level 3 or higher certification for physical security. Examine key-management/device documentation to verify that: • Key generation takes place in a secure cryptographic device—e.g., HSM. • The HSM has achieved PCI approval or FIPS 140-2 Level 3 or higher certification for physical security. • During key-generation, the HSM utilizes a secure algorithm that complies with Annex A of this document.
c) Cables must be inspected under dual control to ensure disclosure of a plaintext key or key component or share is not possible.	Examine key-management documentation to verify that procedures are in place to inspect cables under dual control prior to key-management activity, to ensure disclosure of a clear-text key or key component is not possible. Observe personnel performing inspection of cables to verify that procedures are followed.

7.5 Key Generation

Requirement	Test Procedure
d) Use the principles of split knowledge and dual control during the generation of any cryptographic keys in component or share form.	Interview personnel to verify that split knowledge and dual control are required during the generation of any cryptographic keys in component or share form. Examine a sample of key-ceremony records and events to verify that split knowledge and dual control are required during the generation of any cryptographic keys in component or share form.
e) Key components, if printed, must be created in such a way that the key component cannot be tapped or observed during the process by other than the authorized key custodian. Additionally, the key components cannot be observed on final documents without evidence of tampering.	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. Examine procedures to verify that printed key components are created in such a way that the key component cannot be tapped or observed during the process by other than the authorized key custodian and cannot be observed on final documents without evidence of tampering.
f) Immediately destroy any residue from the printing or generation process that might disclose a component so that an unauthorized person cannot obtain it.	Examine key-management documentation to verify that any residue from the printing or generation process is immediately destroyed. Interview personnel to verify that procedures are followed.
g) Ensure that a generated key is not at any time observable or otherwise accessible in plaintext to any person during the generation process.	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. Observe a key-generation process (live or demonstration if necessary) to verify procedures are followed.
h) Key components or shares must be placed in pre-serialized, tamper-evident envelopes when not in use by the authorized key custodian.	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. Examine 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.
7.5.1 Asymmetric Keys Used for Payment Transactions	
a) Adhere to the public-key algorithm and ensure that the length of issuer RSA key pairs used for payment-transaction processing is in accordance with payment-system requirements.	Examine payment system requirements for public-key algorithms regarding the length of issuer key pairs and the vendor's key-management documentation for consistency.

7.5 Key Generation

Requirement	Test Procedure
b) Ensure that the generation of asymmetric key pairs ensures the secrecy of the private key and the integrity of the public key.	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; and • Their creation and management are in compliance with the payment system requirements for obtaining the issuer certificate.
c) Create and manage asymmetric keys in compliance with the payment system requirements for obtaining the issuer certificate.	Examine payment system requirements for the creation and management of asymmetric keys and the vendor's key-management documentation for consistency.

7.6 Key Distribution

Requirement	Test Procedure
a) Keys must be distributed only in their allowable forms.	Examine key-management documentation to verify that keys are distributed only in their allowable forms in accordance with Sections 7.2, "Symmetric Keys, and 7.3, "Asymmetric Keys."
b) When transmitted electronically, keys and key components or shares must be encrypted prior to transmission following all key-management requirements documented in this section.	Examine key-management documentation to verify that keys and key components or shares are encrypted prior to electronic transmission.
c) Ensure that private or secret key components or shares and keying data that are sent as plaintext 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.	Examine documentation for conveying key components to verify that the use of different communication channels, such as different courier services and not the same courier on different days, is required. Examine key-management activity audit logs to verify key components were sent according to required procedures.
ii. A two-part form that identifies the sender and the materials sent must accompany the keying data.	Examine procedures for key generation to ensure a two-part form is used and the form identifies the materials sent. Examine the two-part form to verify that it includes details of the sender and the material sent.
iii. The form must be signed by the sender and require that the recipient return one part of the form to the originator.	Examine a sample of recently generated key components and verify the forms were adequately signed and returned according to procedures.

7.6 Key Distribution

Requirement	Test Procedure
iv. Key components or shares must be placed in pre-serialized, tamper-evident envelopes for shipment.	Examine policies/procedures to verify that key components or shares are placed in pre-serialized TEE bags prior to shipment. Examine a sample of key-management activity logs and verify that pre-serialized numbers are logged as part of the process.
d) 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.	Examine key-management policies/procedures to verify that inspection of the shipping package received is required and that any signs of tampering require initiation of key-compromise procedures. Interview personnel to verify that procedures are followed.
ii. Verify the contents of the package with the attached two-part form.	Examine procedures for key-component receipt to verify a two-part form is used and the form identifies the materials sent. Interview personnel to verify that procedures are followed.
iii. Return one part of the form to the sender of the component or share, acknowledging receipt.	Examine procedures for key-component receipt to verify that one part of the form is returned to the sender of the component or share, acknowledging receipt. Interview personnel to verify that procedures are followed.
iv. Securely store the component or share according to the vendor's key-storage policy.	Examine procedures for key-component receipt to verify that the component or share is securely stored according to the vendor's key-storage policy. Interview personnel to verify that procedures are followed.
e) Before entities accept 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.	Examine key-management documentation to verify that prior to certificate acceptance a prearranged method to validate certificate status is in place and includes the valid period of usage and revocation status, if available. Interview personnel to verify that procedures are followed.

7.7 Key Loading

Requirement	Test Procedure
The following requirements relate to the loading of clear-text cryptographic key components/shares into HSMs.	
a) Any hardware used in the key-loading function must be dedicated, controlled, and maintained in a secure environment under dual control. Effective January 2018, all newly deployed key-loading devices must be SCDs, either PCI-approved or FIPS 140-2 or 140-3 Level 3 or higher certification for physical security.	Examine key-management documentation to verify that any hardware used in the key-loading function is dedicated, controlled, and maintained in a secure environment under dual control. 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. Examine documentation to verify that all newly deployed key-loading devices are SCDs and are either PCI-approved or FIPS 140-2 or 140-3 Level 3 or higher certification for physical security.
b) 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).	Examine key-management documentation to verify that the target cryptographic devices, cabling, and paper components are inspected for any signs of tampering prior to key loading. Observe personnel performing physical inspections of the target cryptographic devices, cabling, and paper components to verify processes are followed to detect signs of tampering prior to key loading.
c) Tokens, PROMs, or other key component/share mechanisms used for loading keys (or key components/shares) must only be in the physical possession of the designated custodian (or their backup), and only for the minimum practical time.	Examine key-management documentation 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 backup, and • Only for the minimum practical time.
d) 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.	Examine vendor/device documentation to verify that a device used to transfer keys between the cryptographic device that generated the key(s) and the cryptographic devices that will use those key(s), is itself 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.	Interview personnel to verify that residual information is not retained after key loading. Observe a key-loading ceremony and verify information is not retained after transferring the keying material.
e) All key-loading activities must be under the control of the Key Manager.	Examine key-management documentation and interview personnel to verify that all key-loading activities are performed under the control of the Key Manager. Observe key-loading activities to verify that all such activities are under control of the Key Manager.

7.7 Key Loading

Requirement	Test Procedure
f) Control and maintain any tokens, electronically erasable programmable read-only memory (EEPROM), physical keys, or other key component/share-holding devices used in loading keys in a secure environment under dual control.	Examine key-management documentation to verify that all key/key component/key share-holding device used for key loading are managed under dual control. Observe personnel performing key loading to verify that all key/key component/key share-holding mechanisms are handled under dual control.
g) Make certain that the key-loading process does not disclose any portion of a key component/share to an unauthorized individual.	Examine key-management documentation to verify that the key-loading process does not disclose any portion of a key component/share to an unauthorized individual. Interview personnel to verify that procedures are followed.
h) 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.	Examine key-management documentation 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. Interview personnel to verify that procedures are followed.
i) 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 used for this purpose, check values for key and key components 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.	Examine key-management documentation 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. Observe personnel performing validation processes to verify that they are conducted under dual control and the outcomes are reported to the Key Manager.
j) Once a key or its components/shares have been loaded and validated as operational, either: • Securely destroy or delete it from the key-loading materials as defined in Section 7.11, “Key Destruction”; or • Securely store it according to these requirements if preserving the keys or components/shares for future loading.	Examine key-management documentation 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. 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.

7.7 Key Loading

Requirement	Test Procedure
k) During the key-loading process, key custodians as well as the key manager must verify that the key usage set for the key being loaded matches the keys intended use. This information must be recorded in an audit trail of the key ceremony.	Examine key-management documentation to verify procedures are in place to validate key usage. Examine key ceremony audit logs to ensure they are complete and correct.

7.8 Key Storage

Requirement	Test Procedure
The following requirements relate to the secure storage of secret keys, private keys, and their plaintext key components or shares.	
a) Key components/shares must be stored in pre-serialized, tamper-evident envelopes in separate, secure locations (such as safes).	Examine key-management documentation and interview personnel to verify: • Key components/shares are stored in pre-serialized, tamper-evident envelopes; • The envelopes are stored in secure locations (such as safes); and • Removal of the envelopes from their secure location is detectable. Observe the envelopes used to verify that they are pre-serialized and tamper-evident. Observe storage locations to verify the envelopes are stored in separate, secure locations.
b) These envelopes must not be removable without detection.	Examine key-management documentation and interview personnel to verify removal of the envelopes from their secure location is detectable. Observe storage locations to verify the envelopes cannot be removed without detection.
c) An inventory of the contents of key storage safes must be maintained and audited quarterly.	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. Examine inventory and audit documentation to verify inventory is complete and audits are performed at least quarterly.

7.8 Key Storage

Requirement	Test Procedure
d) Where a secret or private key component/share is stored on a token—e.g., an integrated circuit card—and an access code—e.g., a personal identification number (PIN)) or similar access-control mechanism is used to access that token, only that token's owner (or designated backup) must be allowed possession of both the token and its corresponding access code.	Examine key-management documentation for secret or private key component/shares that are stored on a physical media to verify that the key custodian (or designated backup) is the only person allowed possession of both the media and its corresponding access code.
e) Ensure that access logs, at a minimum, include the following: • Date and time (in/out) • Names and signatures of the key custodians involved • Purpose of access • Serial number of envelope (in/out)	Examine key-management documentation to verify that access logs are maintained. 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)
f) Keep the access and destruction logs for master keys until after cards using keys protected by those master keys are no longer in circulation.	Examine key-management documentation to verify that logs for access and destruction of master keys are retained until at least after all keys protected by those master keys are retired and no longer in circulation.

7.9 Key Usage

Requirement	Test Procedure
a) Each key must be used for only one purpose and not shared between payment systems, issuers, or cryptographic zones, for example:	
i. Private keys shall be used only to create digital signatures OR to perform decryption operations. Private keys shall never be used to encrypt other keys.	Examine documentation to identify controls that ensure private keys are used only to create digital signatures or perform decryption and that private keys shall not be used to encrypt other keys. Examine evidence that verifies controls are in place and active.
ii. RSA signature (private) keys must be prohibited from being used for the encryption of either data or another key, and similarly RSA encryption (public) keys must be prohibited from being used to generate signatures.	Examine documentation to identify controls that ensure private keys are used only to create digital signatures or perform decryption; that private keys shall not be used to encrypt other keys; and RSA encryption (public) keys must be prohibited from being used to generate signatures. Examine evidence that verifies controls are in place and active.

7.9 Key Usage

Requirement	Test Procedure
iii. Public keys shall be used only to verify digital signature OR perform encryption operations.	Examine documentation to identify controls that ensure public keys can only be used to verify digital signatures OR perform encryption operations. Examine evidence that verifies controls are in place and active.
iv. Key-encrypting keys must never be used as working keys (session keys) and vice versa.	Examine policies/procedures to identify controls that KEKs are not used as working keys and vice versa. Examine evidence that verifies controls are in place and functioning.
b) Key-encipherment keys used to encrypt other keys for conveyance—e.g., KEK, ZCMK—must be unique per established key zone and, optionally, unique per issuer within that zone. These keys must only be shared between the two communicating entities and must not be shared with any third organization.	Examine documentation to verify it requires that key-encipherment keys are: • Unique per established key zone • Only shared between the two communicating entities Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.
c) The HSM must enforce a separation of keys to prevent keys from being used for purposes other than those for which they were intended.	Examine key-management documentation to verify that cryptographic keys are only used for the one, specific purpose for which they were defined. Observe HSM settings and configurations to verify they enforce a separation of keys.
d) All secret and private keys must have a predefined expiry date by which they must be retired from use. No key must be used for a period longer than the designated life span of that key. Issuer keys must not be used for longer than the issuer-specified expiry date.	Examine documented key-management policies and procedures to verify that they require that: • All secret and private keys have a predefined expiry date by which they must be retired from use and cannot be used for a period longer than the designated life span of that key. • Issuer-provided keys with a defined expiry date are not used after the issuer-specified expiry date. Observe issuer keys currently in use to verify they are within the issuer-specified expiry date.
e) There must be no process by which, once deployed, the life of a key can be extended beyond its original designated life span.	Examine key-management procedures to ensure a key cannot be extended beyond its original designated life span after deployment.
f) The vendor must:	
i. Prohibit any keys from being shared or substituted between production and test systems.	Examine key-management documentation to verify that cryptographic keys are never shared or substituted between production and test/development systems. Observe a demonstration of the processes for generating and loading keys into production systems to verify they have no association with test or development keys. Observe a demonstration of the processes for generating and loading keys into test systems to verify they have no association with production keys.

7.9 Key Usage

Requirement	Test Procedure
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.	Examine key-management documentation to verify that 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. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.
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.	Examine key-management documentation to verify that keys used for prototyping are not used in production. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.
iv. Make certain that the life of keys used to encrypt other keys is 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.	Examine documented procedures 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. Examine documented procedures to verify procedures require that only the algorithms and key lengths stipulated in Normative Annex A of this document be used. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.
v. Ensure that private and secret keys exist in the minimum number of locations consistent with effective system operation.	Examine documented procedures to verify that private and secret keys exist in the minimum number of locations consistent with effective system operation. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.
vi. Not use key variants except within the device with the original key.	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. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.
vii. Only use private keys to decipher or to create a digital signature; public keys must only be used to encipher or to verify a signature.	Examine documented procedures to verify that private keys are only used to decipher or to create a digital signature; and public keys are only used to encipher or to verify a signature.

7.9 Key Usage

Requirement	Test Procedure
viii. Maintain an inventory of keys under its management to determine when a key is no longer required—e.g., could include key label/name, effective date, expiration date, key purpose/type, key length, etc.	Examine documentation of key-inventory control and monitoring procedures to verify all keys are identified and accounted for in the inventory. Examine key inventory records to verify the following details are included: • Key label/name • Effective date • Expiration date (if applicable) • Key purpose/type • Key length Interview personnel to verify that key-inventory procedures are known and followed.
g) All derivation keys must be unique per issuer.	Examine key-management documentation to verify that all derivation keys are unique per issuer. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.
h) IC keys must be unique per IC.	Examine key-management documentation to verify that all IC keys are unique per IC. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.
i) Transport keys used for mobile provisioning must be unique per device.	Examine key-management documentation to verify that transport keys used for mobile provisioning are unique per device. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.

7.10 Key Back-up/Recovery

Requirement	Test Procedure
It is not a requirement to have backup copies of key components, shares, or keys. However, if backup copies are used, the requirements below must be met.	
a) Ensure that key back-up and recovery are part of the business recovery/resumption plans of the organization.	Examine documented procedures to verify that key back-up and recovery are part of the business recovery/resumption plans of the organization.
b) Require a minimum of two authorized individuals to enable the recovery of keys.	Examine documented recovery procedures to verify that recovery of keys requires dual control. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.
c) All relevant policies and procedures that apply to production keys must also apply to backup keys.	Examine documented procedures and backup records to determine whether any backup copies of keys or their components exist. Observe back-up processes to verify backup copies of secret and/or private keys are maintained in accordance with the same requirements as are followed for the production keys.
d) Vendor must prohibit the loading of backup keys into a failed device until the reason for that failure has been ascertained and the problem has been corrected.	Examine documented to verify the procedures ensure that the loading of backup keys into failed devices is not permitted until after the reason for that failure has been ascertained and the problem has been corrected. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.
e) The back-up of keys must conform to Information Security Policy.	Examine documented procedures to verify that the back-up of keys conforms to the organization's Information Security Policy. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.
f) All access to backup storage locations must be witnessed and logged under dual control.	Examine documented procedures to verify that all access to all backup storage locations is witnessed and logged under dual control. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.

7.11 Key Destruction

Requirement	Test Procedure
The following requirements relating to the destruction of clear keys, components, and shares must be met.	
a) Immediately destroy key components/shares that are no longer required after successful loading and validation as operational.	Examine documented procedures to verify processes are in place for destroying keys and their components/shares after successful loading and validation. Examine a sample of key-history logs and key-destruction logs to verify that all key components/shares have been destroyed immediately upon completion of loading. Examine storage locations for key components/shares that have been loaded to verify they are no longer present.
b) When a cryptographic device—e.g., HSM—is decommissioned, any data stored and any resident cryptographic keys must be deleted or otherwise destroyed.	Interview personnel 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. Observe processes for removing cryptographic devices 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.
c) Securely destroy all copies of keys that are no longer required for card production or provisioning.	Examine documented procedures to verify processes are in place for destroying all copies (including backups) of keys that are no longer required.
d) All key destruction must be logged, and the log retained for verification.	Examine a sample of key-destruction logs to verify that all copies of keys have been destroyed once the keys are no longer required.
e) Destroy keys and key components/shares so that it is impossible to recover them by physical or electronic means.	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. Observe key-destruction processes to verify that no part of the key or component can be recovered.
f) 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.	Examine documented procedures for removing HSMs from service to verify that if any key within the HSM cannot be destroyed, the device itself is destroyed in a manner that ensures it is irrecoverable. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.
g) Destroy all hard-copy key components/shares maintained on paper by cross-shredding, pulping, or burning. Strip shredding is not sufficient.	Examine documented procedures to verify all hard-copy key components/shares maintained on paper are destroyed by cross-shredding, pulping, or burning—and not by strip shredding. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.

7.11 Key Destruction

Requirement	Test Procedure
h) Electronically stored keys must either be overwritten with random data a minimum of three times or destroyed by smashing so they cannot be reassembled.	Examine documented procedures 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. Interview personnel to verify the implementation of the aforementioned.
i) Destroy all key components under dual presence with appropriate key-destruction affidavits signed by the applicable key custodian.	Examine documented procedures for destroying keys to verify that dual control is implemented and key-destruction affidavits are signed by the applicable key custodian for all key-component destruction processes. Observe a demonstration of processes for removing keys from service to verify that dual control is implemented. Examine a sample of key-destruction logs and verify that the key custodian signs an affidavit as a witness to the key destruction process.
j) 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. (This person may also fulfill the dual-presence requirement above or be a third person to the activity.)	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; or Examine a sample of 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.

7.12 Key-Management Audit Trail

Requirement	Test Procedure
a) 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., whether 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 • Pre-serialized key envelope number, if applicable	Examine 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) • Pre-serialized key envelope number, if applicable

7.12 Key-Management Audit Trail

Requirement	Test Procedure
b) Key-management logs must be retained for at least the life span of the key(s) to which they relate.	Examine documented procedures to verify procedures require key-management logs must be retained for the life span of the key(s) to which they relate. Examine a sample of 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.
c) The vendor must prohibit access to key-management logs by any personnel outside of the Key Manager or authorized individuals.	Examine documented procedures to ensure access to key-management logs is only permitted for the Key Manager or authorized individuals. Observe access to a sample of key-management logs to verify it is only permitted to authorized individuals.
d) Any facility to reset the sequence number generator or other mechanisms such as time and date stamps in the HSM must be restricted.	Examine documented procedures to ensure procedures restrict access to any capability to reset the sequence number generator or other mechanisms in the HSM. Examine access-control lists or other processes to verify that only authorized personnel have access to the sequence number generator.
e) The CISO or an authorized individual must investigate all audit log validation failures.	Examine documented procedures to verify the CISO (or equivalent) investigates all audit log validation failures. Interview personnel to verify the implementation of the aforementioned.
f) During the personalization process, an electronic log must be maintained to identify what keys were used.	Examine documentation to verify an electronic log is maintained to identify keys used during the personalization process. Examine a sample of logs to verify that they track what keys are used during the personalization process.
g) The vendor must ensure that the deletion of any audit trail is prevented.	Examine documented procedures to verify controls are defined for protecting audit trails from unauthorized deletion. Examine a sample of system configurations to verify controls are implemented to prevent unauthorized deletion of audit trails.

7.13 Key Compromise

Requirement	Test Procedure
The following requirements relate to the procedures for dealing with any known or suspected key compromise. Unless otherwise stated, the following applies to vendor-owned keys.	
a) The vendor 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, Key Manager, IT Security Manager, and the VPA.	Examine documented procedures for key compromise to verify they include who is to be notified; and at a minimum include the CISO (or equivalent), Key Manager, IT Security Manager, and the VPA. Interview personnel to verify that procedures are known and followed.
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.	Examine documented procedures for key compromise to verify they include 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. Interview personnel to verify that procedures are known and followed.
iii. An investigation into the cause of the compromise, including a documented analysis of how and why the event occurred and the damages suffered.	Examine documented procedures for key compromise to verify they include requiring an investigation into the cause of the compromise, including a documented analysis of how and why the event occurred and the damages suffered. Interview personnel to verify that procedures are known and followed.
iv. That the vendor will remove from operational use all compromised keys within a predefined time frame and provide a means of migrating to new key(s).	Examine documented procedures for key compromise to verify they include that the vendor will remove from operational use all compromised keys within a predefined time frame and provide a means of migrating to new key(s). Interview personnel to verify that procedures are known and followed.
v. Where keys are issuer-owned, the issuer must be notified immediately for further instruction.	Examine documented procedures for key compromise to verify they include that where keys are issuer-owned, the issuer must be notified immediately for further instruction. Interview personnel to verify that procedures are known and followed.
b) Ensure that the replacement key is not a variant of the compromised key.	Examine documented procedures to ensure replacement keys are not created from a variant of the compromise key. Interview personnel to verify the implementation of the aforementioned.
c) Where a key compromise is suspected but not yet proven, the Key Manager must have the ability to activate emergency key-replacement procedures.	Examine documented procedures to verify that in the event of a suspected key compromise, the Key Manager has authority to activate emergency key replacement procedures. Interview Key Manager to verify he/she is aware of their responsibility and understand the procedures to activate emergency key-replacement procedures.

7.13 Key Compromise

Requirement	Test Procedure
d) 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.	Examine documented procedures to verify they require that in the event of a suspected key compromise, all instances of the key must be immediately revoked pending the outcome of the investigation. Interview personnel to verify that procedures are understood and communicated to affected personnel.
e) All keys that are encrypted with a key that has been revoked must also be revoked.	Examine documented procedures to verify that all keys encrypted with a key that has been revoked are also revoked. Interview personnel to verify that procedures are understood and communicated to affected personnel.
f) In the event that a KEK has been compromised, all keys encrypted with the KEK must be replaced.	Examine documented procedures to verify that if a KEK is compromised, the KEK and all keys encrypted with that KEK are replaced. Interview personnel to verify that procedures are understood and communicated to affected personnel.
g) In the event that a MDK has been compromised, all keys derived from that master key must be replaced.	Examine documented procedures to verify that if a MDK is compromised, the MDK and all keys derived from that MDK are replaced. Interview personnel to verify that procedures are understood and communicated to affected personnel.
h) The payment system VPA must be notified within 24 hours of a known or suspected compromise.	Examine documented procedures to verify steps include notification of the VPA within 24 hours of a known or suspected compromise.
i) 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.	Examine documented procedures to verify data items that have been signed with a key that has been revoked are withdrawn as soon as possible and replaced. Interview personnel to verify that procedures are understood and communicated to affected personnel.

7.14 Key-Management Security Hardware

Requirement	Test Procedure
a) All key-management activity must be performed using an HSM.	Examine policies/procedures to verify all key-management activity uses an HSM.
b) When in its normal operational state:	
i. All of the HSM's tamper-resistant mechanisms must be activated.	Examine documented procedures to verify that when the HSM is in its normal operational state, all of the HSM's tamper-resistant mechanisms must be activated. 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.
ii. All physical keys must be removed.	Examine documented procedures to verify that when the HSM is in its normal operational state, all physical keys must be removed. Observe HSMs in normal operational state to verify they are configured according to the documented procedures, and that all physical keys are removed.
iii. All unnecessary externally attached devices must be removed (such as an operator terminal).	Examine documented procedures to verify that when the HSM is in its normal operational state, all unnecessary externally attached devices must be removed (such as an operator terminal). Observe HSMs in normal operational state to verify they are configured according to the documented procedures, and that all unnecessary externally attached devices are removed (such as an operator terminal).
c) HSMs used for key management or otherwise used for the protection of sensitive data must be approved by PCI or certified to FIPS 140-2 or 140-3 Level 3 or higher certification for physical security.	Examine documentation to ensure that all HSMs used for key management or otherwise used for the protection of sensitive data are: • Approved by PCI or certified to FIPS 140-2or 140-3 level 3 or higher. • Listed on the PCI SSC website with a valid PCI SSC listing number, as an Approved PCI PTS Device under the approval class "HSM." • Listed on the NIST Cryptographic Module Validation Program (CMVP) list with a valid listing number and approved to FIPS 140-2 or 140-3 Level 3 (overall), or higher. Refer to http://csrc.nist.gov.
d) 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.	Examine 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. 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.

7.14 Key-Management Security Hardware

Requirement	Test Procedure
e) The process for the installation and commissioning of the HSM must be documented and logged.	Examine documented procedures and logs for HSM installations to verify processes for installation and commissioning of HSMs are documented and logged.
f) When an HSM is removed from service permanently or for repair, all operational keys must be deleted from the device prior to its removal.	Examine documented procedures for removing HSMs from service to verify that all operational keys are deleted from the device (for example, zeroized) prior to its removal from service. Observe demonstration of processes for removing HSMs from service to verify all operational keys are deleted from the device.
g) The removal process for the repair or decommissioning of the HSM must be documented and logged.	Examine documented procedures and interview personnel to verify that processes for removal of an HSM for repair or decommissioning must be documented and logged. Observe processes and examine logs for HSM removal to verify processes for removal of an HSM for repair or decommissioning are documented and logged.
h) The HSM must be under physical dual control at all times.	Examine documented procedures to verify that HSMs must be under physical dual control at all times when accessed or when in any privileged mode. Interview personnel to verify that procedures are understood and communicated to affected personnel. Examine HSM storage locations and records to ensure they have been managed under dual control after receipt.

Section 8: Key Management: Confidential Data

8.1 General Principles

Requirement	Test Procedure
8.1 General Principles	
a) Key-encipherment keys must meet the minimum key sizes as delineated in Normative Annex A.	Examine the documented key hierarchy and verify keys meet the minimum key sizes as delineated in Normative Annex A.
b) All key-encrypting keys used to transmit or convey other cryptographic keys must be at least as strong as the key being transmitted or conveyed.	Examine documented key-management policies and procedures to verify a policy exists that requires key-encrypting keys (KEKs) used to transmit or convey other cryptographic keys be at least as strong as the key being transmitted or conveyed. Examine the documented key hierarchy to verify keys used to transmit or convey other cryptographic keys are at least as strong as the key being transmitted. Observe key-management operations and device configurations 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.
c) Cryptographic keys must not be hard-coded into software.	Examine documented key-management policies and procedures to verify a policy exists that prohibits hard-coded cryptographic in software. 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. Examine software configuration files (for example, shell scripts, command files, communication scripts, software code etc.) to verify that cryptographic keys are not embedded.
d) Audit trails must be maintained for all key-management activities.	Interview personnel to verify audit trails are maintained for all key-management activities. Examine a sample of key-management audit logs to verify their existence and that they address all key-management activities—e.g., generation, conveyance, destruction, etc.
e) Key-management activities must be performed by vendor or issuer staff.	Interview personnel to verify key-management activities are only performed by authorized personnel. Examine a sample of key-management audit logs to verify key-management activities are only performed by vendor or issuer staff.
f) Key-management activities must only be performed by fully trained and authorized personnel.	Examine the vendor's training requirements for individuals involved with key-management activities to verify training program and materials exist. Examine evidence that training has been provided for identified personnel.

8.1 General Principles

Requirement	Test Procedure
g) The vendor must generate keys and key components using a random or pseudo-random process using one of the following: • An approved key-generation function of a PCI–approved HSM • An approved key-generation function of a FIPS 140-2 or 140-3 Level 3 (or higher) for physical security HSM • An approved random number generator that has been certified by an independent qualified laboratory according to *NIST SP 800-22*	Examine key-management procedures to verify that it requires that all devices used to generate cryptographic keys meet one of the following: • An approved key-generation function of a PCI–approved HSM • An approved key-generation function of a FIPS 140-2 or 140-3 Level 3 (or higher) for physical security HSM An approved random number generator that has been certified by an independent qualified laboratory according to *NIST SP 800-22* Examine certification letters or technical documentation to verify that all devices used to generate cryptographic keys or key components meet one of the following: • An approved key-generation function of a PCI-approved HSM or POI • An approved key-generation function of a FIPS 140-2 or FIPS 140-3 Level 3 (or higher) HSM • An SCD that has an approved random number generator that has been certified by an independent qualified laboratory according to NIST SP 800-22
h) Before the vendor accepts a key, it must ensure that it knows its origin.	Interview personnel to verify that as part of key-acceptance procedures, the vendor knows the key's origin. Observe a demonstration of the key-acceptance process to verify the vendor knows the key's origin.
i) Keys must be stored in a manner that preserves their integrity.	Observe the storage locations for a sample of keys and verify the storage is adequate to preserve their integrity.
j) Keys must be used for only one purpose and not shared between cryptographic zones.	Examine documented key-management policies and procedures to verify keys must be used for only one purpose and are not shared between cryptographic zones. Examine a sample of key check values to verify they are unique except by chance.
k) All secret and private keys must have a predefined expiry date by which they must be retired from use. No key must be used for a period longer than the designated life span of that key. Issuer keys must not be used for longer than the issuer-specified expiry date.	Examine key-management policies and procedures to verify secret and private keys require a pre-defined expiry date. Examine a sample of keys to identify key expiry dates and verify that active secret and private keys and issuer keys have not expired.
l) There must be no process by which, once deployed, the life of a key can be extended beyond its original designated life span.	Examine key-management policies and procedures to verify that they prohibit the life of a key from being extended beyond its original designated life span. Interview personnel to verify that keys are not extended beyond their original designated life span.

8.1 General Principles

Requirement	Test Procedure
m) The vendor must prohibit any keys from being shared or substituted between production and test systems.	Interview personnel to identify controls that prohibit keys from being shared between test and production systems. Examine a sample of test and production configuration files to verify the same key check values are not present except by chance in both environments.
n) The vendor must make certain that the life of keys used to encrypt other keys is shorter than the time required to conduct an exhaustive search of the key space.	Examine the documented key hierarchy and verify keys meet the minimum key sizes as delineated in Normative Annex A.
o) The vendor must ensure that keys exist in the minimum number of locations consistent with effective system operation.	Interview personnel to verify it is known that keys may only exist in the minimum number of locations consistent with effective system operation and the vendor is able to identify the locations. Examine a sample of keys to identify storage locations and verify storage is limited to effective system operation.
p) The vendor must ensure that keys are accessible only to the minimum number of people required for effective operation of the system.	Interview personnel to verify keys are only accessible to the minimum number of people required for effective system operations.
q) The vendor must have a documented process for handling known or suspected key compromise that includes the revocation of the key.	Examine documented key-management policies and procedures to verify a process is defined for handling known or suspected key compromise that includes the revocation of the key. Interview personnel to verify the policies and procedures are known.
r) In the event of the compromise of a key, all instances of the key must be revoked.	Examine documented key-management policies and procedures to verify that in the event of key compromise, steps are defined to ensure all instances of the key are revoked.
s) All keys that are encrypted with a key that has been revoked must also be revoked.	Examine documented key-management policies and procedures to verify that in the event of key compromise, steps are defined to ensure all keys that are encrypted with a key that has been revoked are also revoked.
t) In the event that a KEK has been compromised, all keys encrypted with that KEK must be replaced.	Examine documented key-management policies and procedures to verify that in the event of key compromise, steps are defined to ensure all keys that are encrypted with a KEK are replaced.

Section 9: PIN Distribution via Electronic Methods

9.1 General Requirements

Requirement	Test Procedure
The following requirements apply for the distribution of PINs via electronic methods.	
a) The PIN distribution system must not communicate with any other system where associated cardholder data is stored or processed.	Examine system documentation and network diagrams to identify process flows and communication channels for the PIN distribution system (PDS) to verify the PDS cannot communicate with any other system where associated cardholder data is stored or processed. Examine interface rules or applicable controls to verify that other systems where cardholder data is stored or processed cannot communicate with the PIN distribution system.
b) The PIN distribution system must run on a dedicated computer and be isolated from any other network by a dedicated firewall.	Examine system documentation and network diagrams to verify that the PDS runs on a dedicated computer and is isolated from any other network by a dedicated firewall. Examine firewall configurations to verify the PIN distribution system runs on a dedicated computer and is isolated from other networks by a dedicated firewall.
c) The PIN distribution system must perform no other function than PIN distribution, and any sessions established during the distribution—e.g., a telephone call, an e-mail, or a SMS message—must be terminated once the PIN has been sent.	Interview personnel to identify controls that prohibit functions (other than PIN distribution) from being established during a PIN distribution process. Examine a sample of logs to verify that when a session is established during a distribution—e.g., a telephone call, e-mail, or SMS message—the session is terminated once the PIN has been sent.
d) During transmission to and storage in the PIN distribution system, all PIN and authentication values must be encrypted using key algorithms and sizes as stated in Normative Annex A.	Examine system documentation and configuration to verify that during transmission to and storage in the PDS, all PIN and authentication values are encrypted using cryptographic algorithms and key sizes in accordance with Annex A.
e) Communication of the PIN to the cardholder must only take place after verification of the identification value and associated authentication value.	Interview personnel to verify communication of the PIN occurs only after verification of the identification and authentication values. Observe demonstration of a cardholder PIN reset and verify that appropriate verification occurs prior to communicating the PIN.
f) The identification and authentication values must not disclose the account number.	Examine the identification and authentication values for a sample of PIN distribution requests to verify that account number is not present.
g) The authentication value must be different than the identification value and must not be a value easily associated with the cardholder.	Examine a sample of PIN distribution requests to verify the authentication value is different than the identification value and is not a value easily associated with the cardholder.

9.1 General Requirements

Requirement	Test Procedure
h) The authentication value must be communicated to the cardholder in such a way that access by anyone other than the cardholder is detected.	Examine evidence for communicating the authentication values to the cardholder to verify they prevent undetected access by anyone other than the cardholder.
i) The authentication value must be restricted to the PIN distribution system and not accessible by any other system.	Interview personnel to identify controls that restrict the authentication value to the PIN distribution system. Examine identified controls to verify they restrict the authentication value to the PDS and it is not accessible by any other system.
j) The PIN must only be distributed in response to the receipt of valid identification and authentication values.	Interview personnel to verify the PIN is only distributed after validation of identification and authentication values. Observe a demonstration of the process to ensure identification and authentication values are validated before the PIN is distributed.
k) The PIN distribution system must be able to identify the cardholder from the identification value in the request, and the request must contain the cardholder's authentication value.	Examine the documented PIN distribution system process flow to verify the request provides the information necessary to identify the cardholder based upon the identification value and includes the cardholder authentication value. Observe a demonstration of a cardholder request to verify identification and authentication values are present.
l) The distribution system must not have any way of associating an identification value or authentication value with a specific cardholder's name, address, or account number.	Examine evidence to verify controls are established to prevent the distribution system from associating an identification value or authentication value with a specific cardholder's name, address, or account number. Examine a sample of requests to verify the identification and authentication values do not correlate to a cardholder's name, address, or account number.
m) The PIN distribution system must limit the number of attempts to obtain a PIN and upon exceeding this limit must alert the vendor to take further action as defined by the issuer.	Examine evidence to verify that a threshold for invalid attempts exists and upon exceeding this limit the PDS alerts the vendor to take further action as defined by the issuer. Examine a sample of invalid attempts—e.g., a system log—where the threshold was exceeded to verify procedures were performed to take action as defined by the issuer.
n) The PIN must only be decrypted immediately before it is passed to the final distribution channel—e.g., the telephone or e-mail system.	Examine system documentation and PIN distribution flows to verify the PIN is only decrypted immediately before being passed to the final distribution channel.

9.1 General Requirements

Requirement	Test Procedure
o) The PIN distribution system must not contain any other cardholder data—e.g., PAN, cardholder name).	Interview system/database administrator to identify the PDS system locations in which cardholder data may exist. Examine a sample of the PIN distribution system data tables or other evidentiary material to verify other cardholder data does not exist.
p) The association of the PIN to a specific account must not be possible in the distribution system.	Examine documentation to identify the controls established to prevent the association of a PIN to a specific account in the PIN distribution system. Examine a sample of the PIN distribution system tables to verify cardholder data does not exist.
q) The identification value, PIN, and authentication value must not be logged and must be deleted immediately after successful delivery is confirmed.	Examine a sample of logs to verify the identification value, PIN, and authentication value are not captured and the data elements are deleted immediately after successful delivery is confirmed.
r) If the PIN is not delivered to the cardholder, it must be deleted from the system after a fixed period of time, which can be designated by the issuer.	Examine documentation to identify processes for when the PIN is not delivered to the cardholder to verify that it is deleted from the system after a fixed period of time, as designated by the issuer.

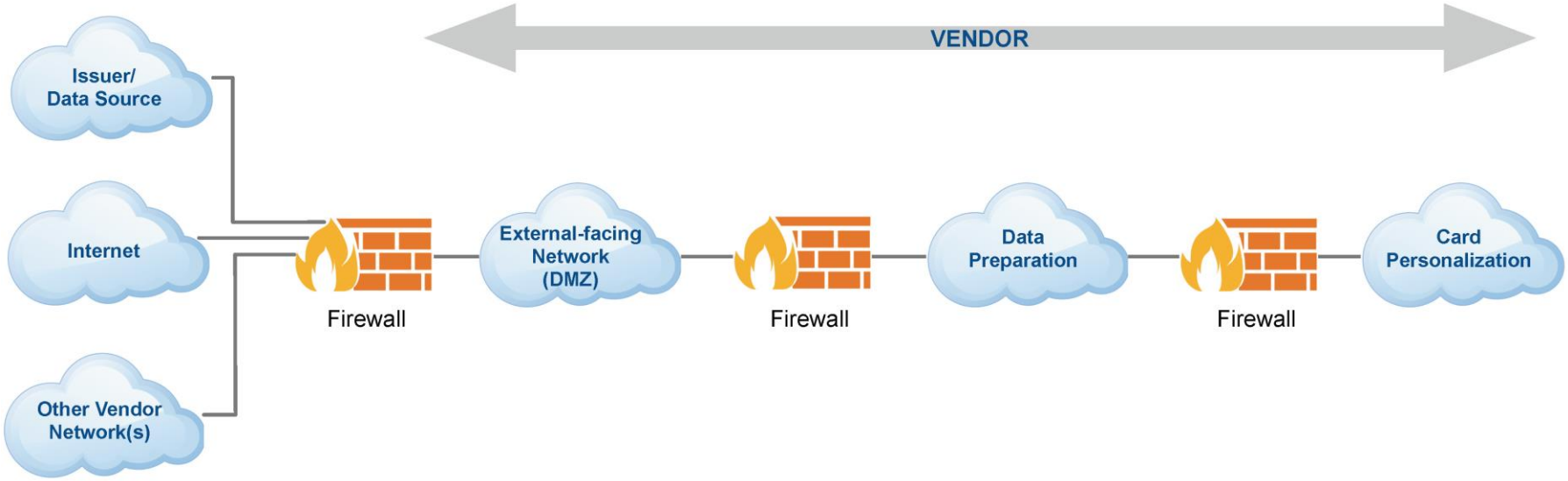
Appendix A: Applicability of Requirements

Logical Security Requirements				
Requirement	**Physical Cards**	**Mobile Provisioning**		**Conditions**
		SE	**HCE**	
Section 1 – Roles and Responsibilities				
All	X	X	X	All requirements applicable
Section 2 – Security Policy and Procedures				
All	X	X	X	All requirements applicable
Section 3 – Data Security				
3.1	X	X	X	
3.2	X	X	X	
3.3	X	X	X	
3.4	X	X	X	
3.5	X	X	X	
3.6	X	X	X	
3.7	X			
3.8	X	X	X	
3.9		X	X	
3.10	X	X	X	
Section 4 – Network Security				
All	X	X	X	All requirements applicable

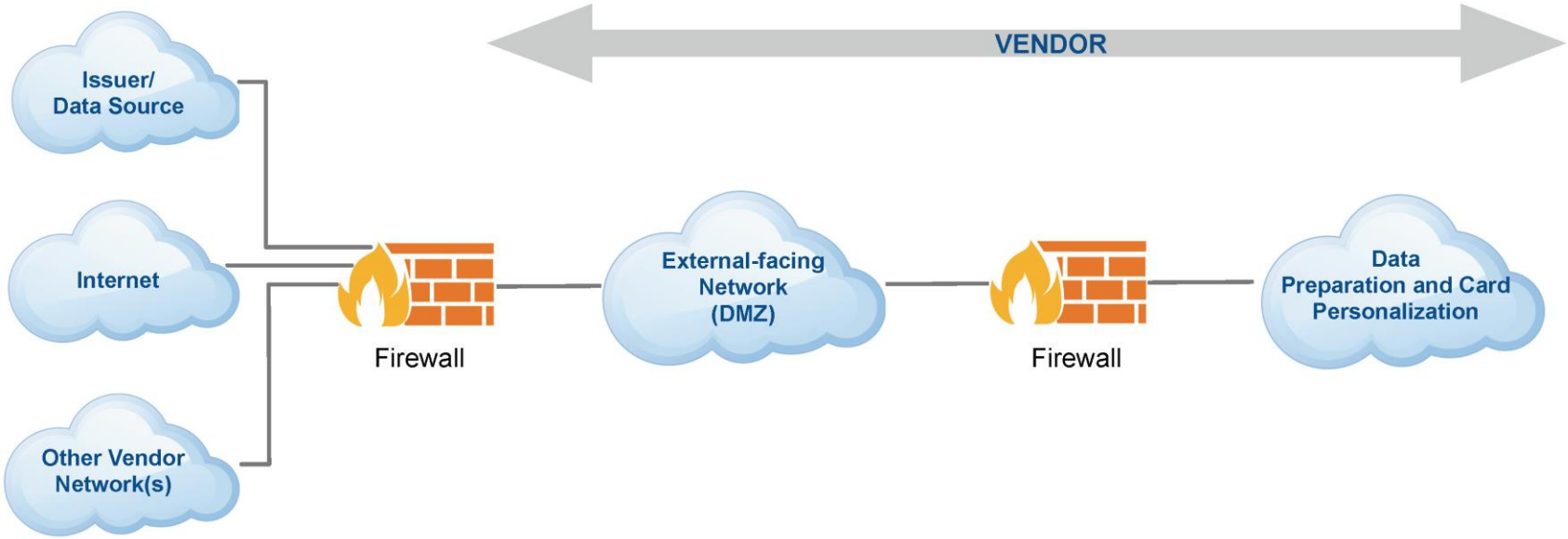
Logical Security Requirements				
Requirement	**Physical Cards**	**Mobile Provisioning**		**Conditions**
		SE	**HCE**	
Section 5 – System Security				
5.1	X	X	X	
5.2	X	X	X	
5.3	X	X	X	
5.4	X	X	X	
5.5		X	X	
5.6	X	X	X	
5.7		X	X	
5.8	X	X	X	
Section 6 – User Management and System Access Control				
All	X	X	X	All requirements applicable
Section 7 – Key Management: Secret Data				
All	X	X	X	All requirements applicable
Section 8 – Key Management: Confidential Data				
All	X	X	X	All requirements applicable
Section 9 – PIN Distribution via Electronic Methods				
All	X	X	X	All requirements applicable

Appendix B: Topology Examples

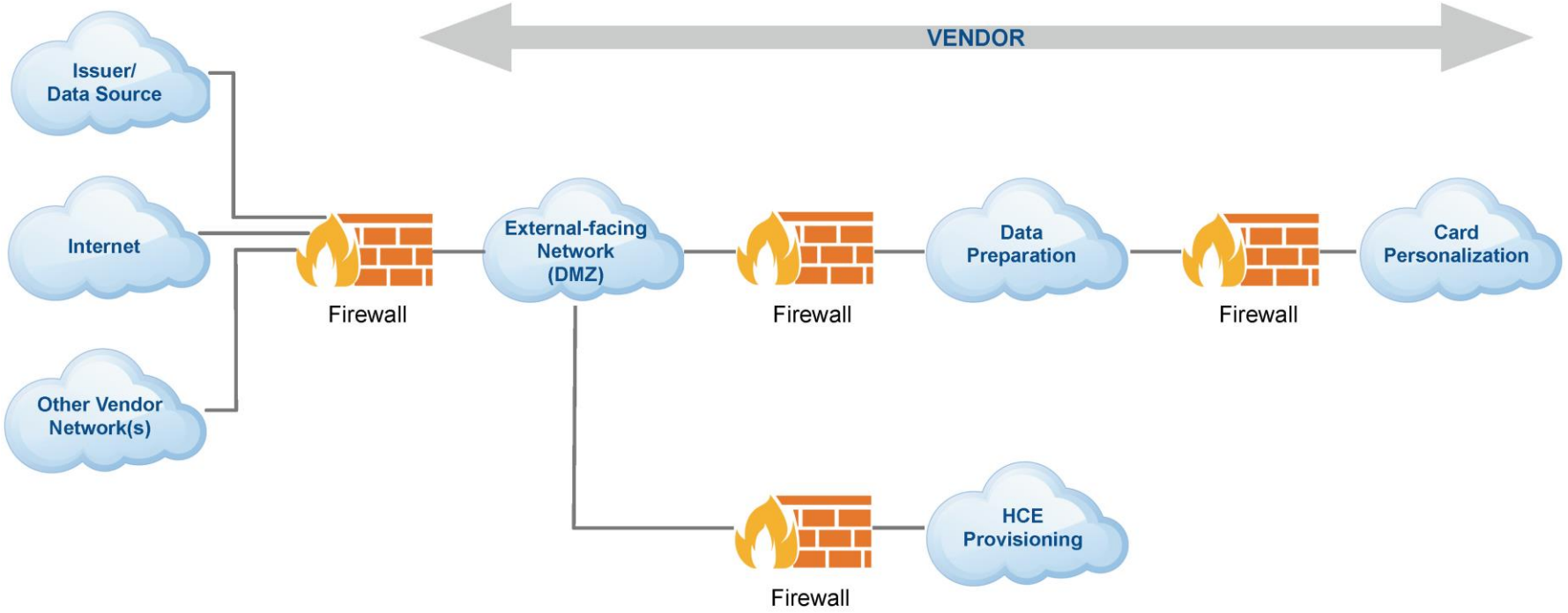
Example B1



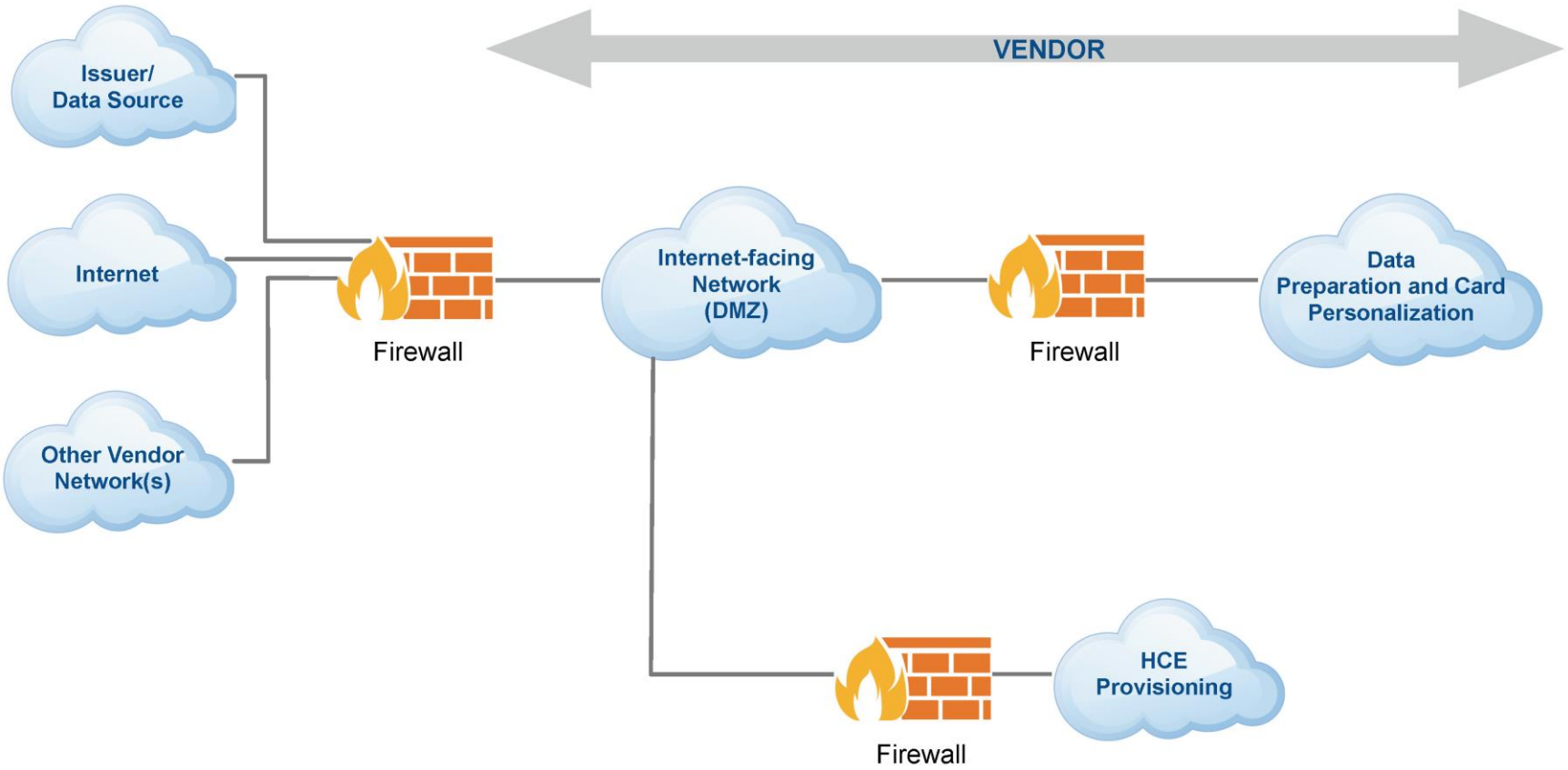
Example B2



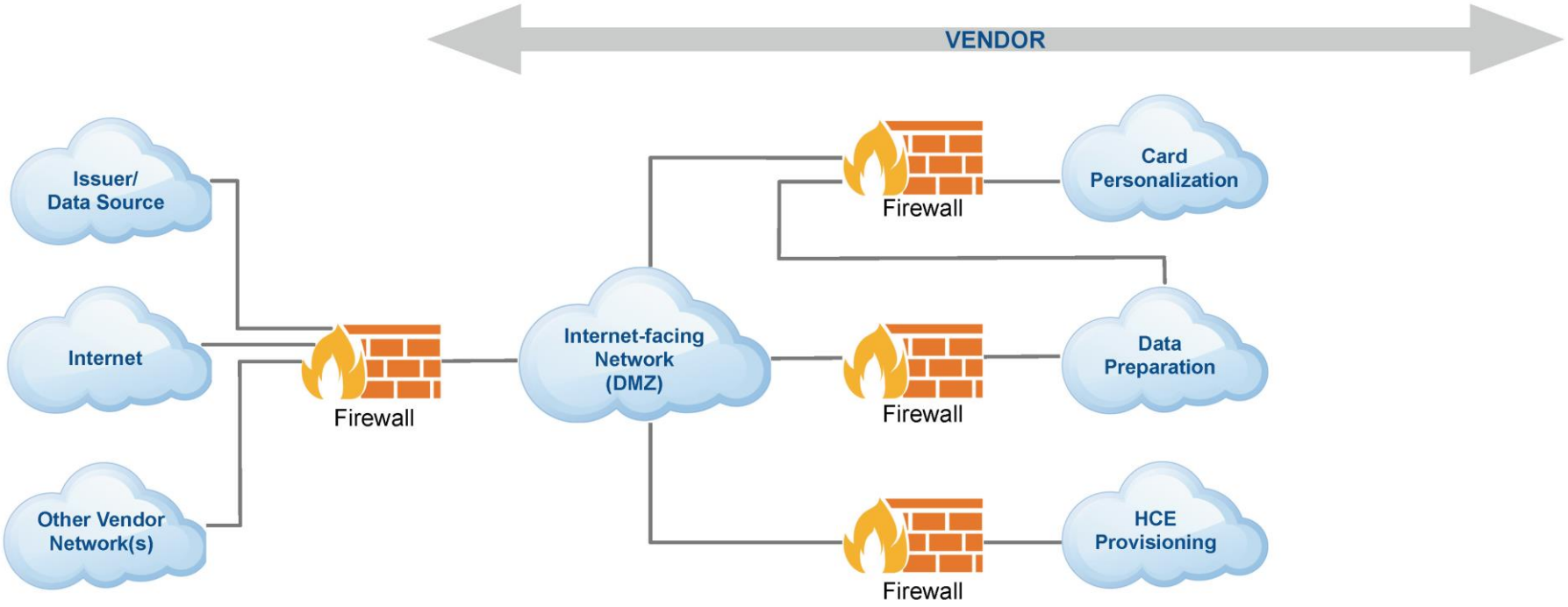
Example B3



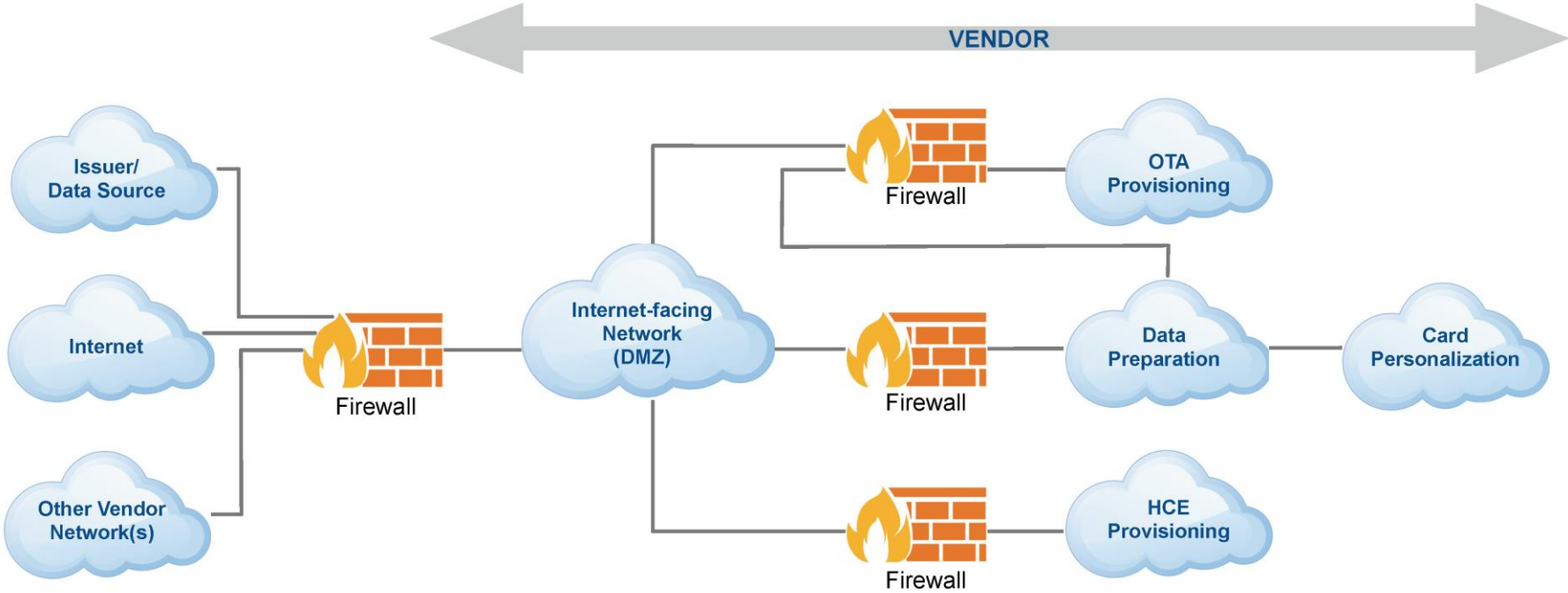
Example B4



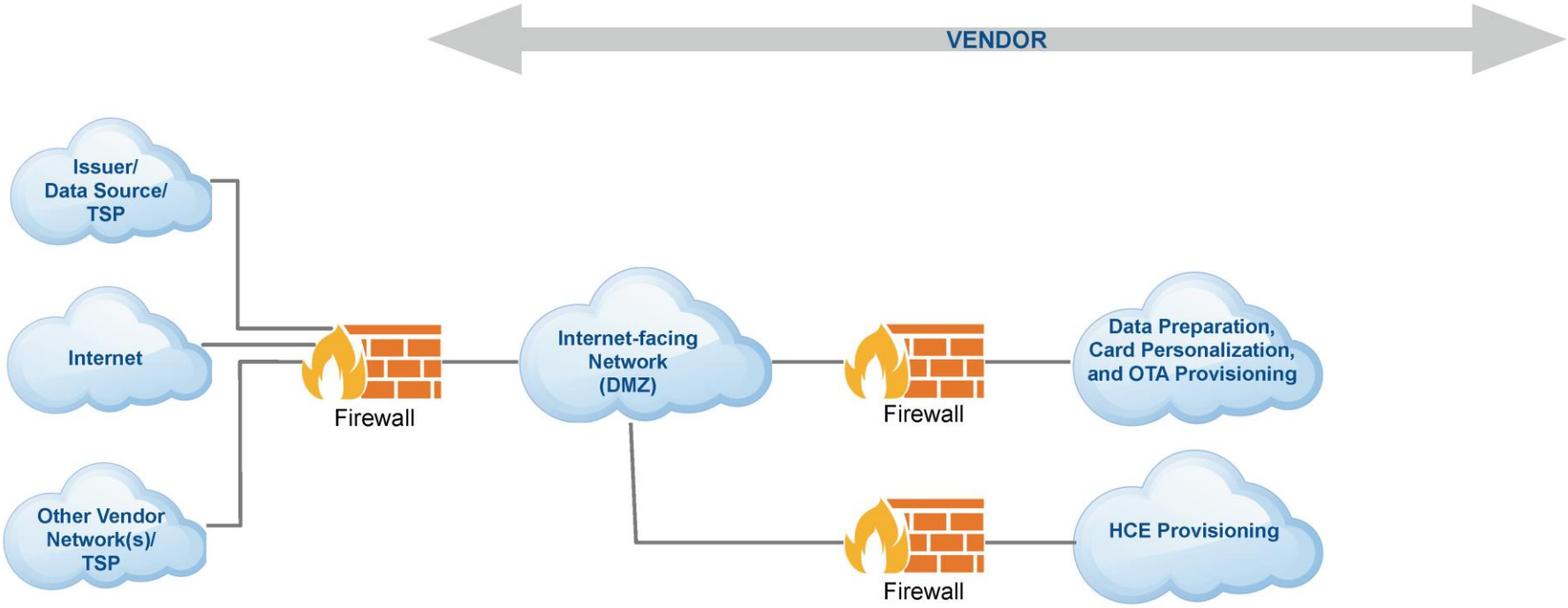
Example B5



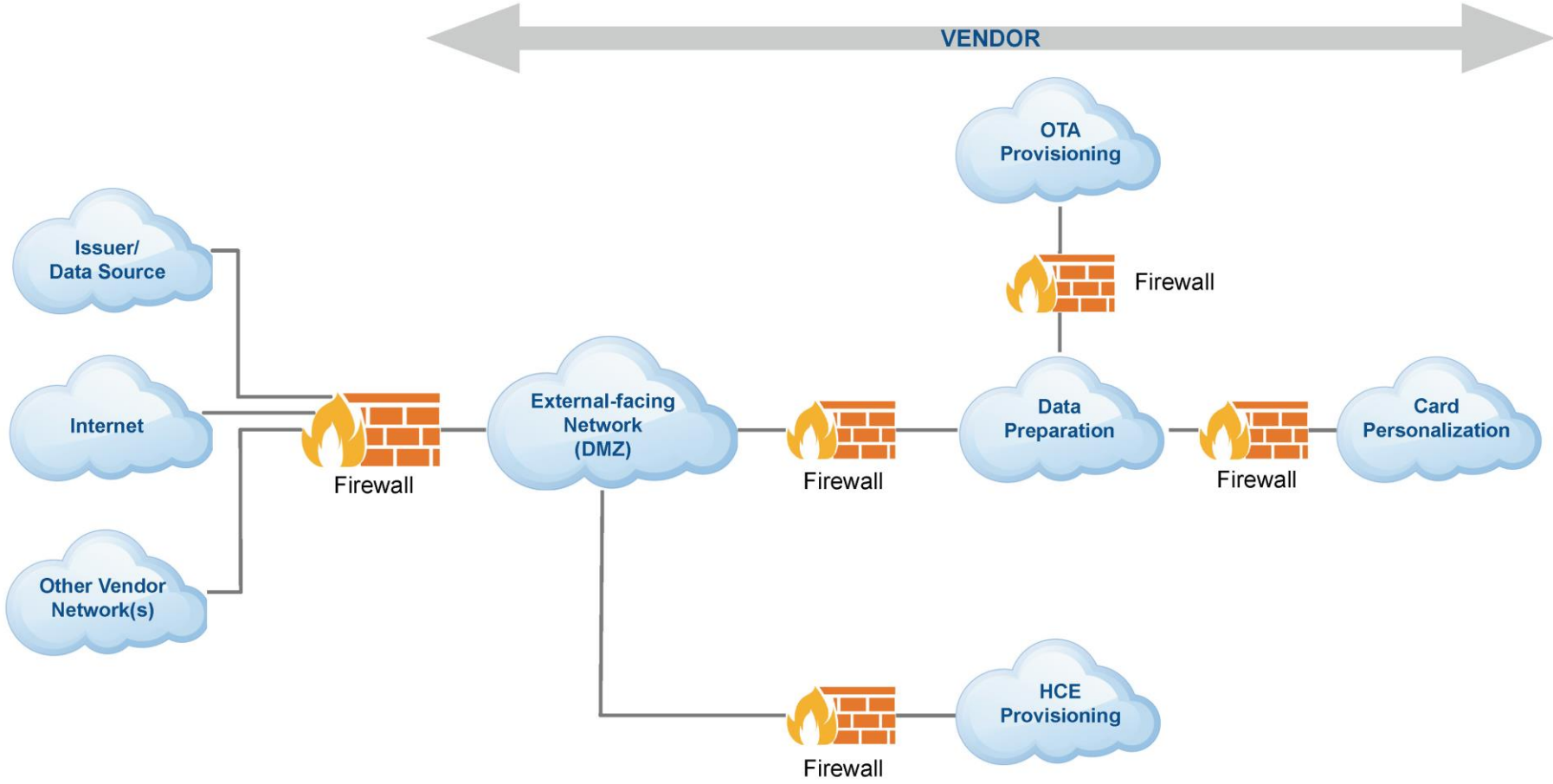
Example B6



Example B7



Example B8



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

The following are the minimum key sizes and parameters for the algorithm(s) in question that must be used in connection with key transport, exchange, or establishment and for data protection in connection with these requirements. Other key sizes and algorithms may be supported for non-PCI payment brand relevant purposes:

	Algorithm				
	DES	**IFC** (RSA)	**ECC** (ECDSA, EdDSA, ECDH, ECMQV)	**FFC** (DSA, DH, MQV)	**AES**
Minimum key size in number of bits:	112	2048	224	2048/224	128

Key-encipherment keys shall be at least of equal or greater strength than any key that they are protecting. This applies to any key-encipherment keys 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. For purposes of this requirement, the following algorithms and keys sizes by row are considered equivalent.

	Algorithm				
Bits of Security	**DES**	**IFC** (RSA)	**ECC** (ECDSA, EdDSA, ECDH, ECMQV)	**FFC** (DSA, DH, MQV)	**AES**
80	112	1024	160	1024/160	–
112	168	2048	224	2048/224	–
128	–	3072	256	3072/256	128
192	–	7680	384	7680/384	192
256	–	15360	512	15360/512	256

DES refers to TDES keys with non-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** must 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 must be at least 2048 bits long, and parameter *q* must be at least 224 bits long. Each entity shall generate a private key *x* and a public key *y* using the domain parameters (*p, q, g*).
- **ECDH implementations entities** must securely generate and distribute the system-wide parameters. Entities may generate the elliptic curve domain parameters or use a recommended curve (see *NIST SP 800-186*). The elliptic curve specified by the domain parameters must be at least as secure as P-224.

Each entity shall generate a private key *d* and a public key *Q* using the specified elliptic curve domain parameters. (See *NIST SP 800-186* for methods of generating *d* and *Q*).

- Each private key shall be statistically unique, unpredictable, and created using an approved random number generator as described in this document.

Entities must 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: MAC algorithm 1 using padding method 3, MAC algorithm 5 using padding method 4, should be used.

Glossary of Acronyms and Terms

Acronyms

Acronym	Term	Acronym	Term
ANSI	American National Standards Institute	**IVR**	Interactive Voice Response
AP	Access point	**KEK**	Key-encryption key
CA	Certificate Authority	**MAC**	Message authentication code
DES	Data Encryption Standard	**MDK**	Master Derivation Key
EEPROM	Electronically erasable programmable read-only memory	**NFC**	Near field communication
ESP	Encapsulating Security Payload	**PC**	Personal computer
FIPS	Federal Information Processing Standards	**PCI**	Payment Card Industry
HSA	High security area	**PIN**	Personal identification number
HSM	Hardware security module	**POTS**	Plain old telephone service
IC	Integrated Circuit	**PROM**	Programmable read-only memory
ID	Identification value	**RF**	Radio frequency
IDS	Intrusion-detection system	**RSA**	Rivest, Shamir, Adleman asymmetric algorithm
IKE	Internet Key Exchange	**SMS**	Short Message Service
IP	Internet Protocol	**SQL**	Structured Query Language
IPSec	Internet Protocol Security	**TDES**	Triple Data Encryption Algorithm
IRP	Incident response plan	**VPA**	Vendor Program Administrator
ISO	International Organization for Standardization	**VPN**	Virtual private network
ISP	Information security policy	**ZCMK**	Zone Control Master Key

Terms

Term	Definition
Advanced Encryption Standard (AES)	The Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES).
Application Keys	Keys used by the issuer application. Application keys include the MDK and keys that may be derived from the MDK to be loaded into the chips during personalization.
Asymmetric	In cryptography, "asymmetric" implies the use of two different keys: a public key and a private key.
Authentication	A cryptographic process that validates the source and integrity of data. Examples include Dynamic Data Authentication, Static Data Authentication, Online Card Authentication, and Online Issuer Authentication.
Authentication value	The data that the PIN-distribution system uses to authenticate the cardholder.
Bureau	A vendor performing card personalization and/or data preparation.
Cardholder Data	At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, and/or service code.
Card Production Staff	Card Production Staff applies to any employees or contractors who are involved in card production related activities that could impact security, including administration, support activities and IT infrastructure.
Certificate Authority	A trusted central administration that issues and revokes certificates according to an advertised policy and is willing to vouch for the identities of those to whom it issues certificates and their association with a given key.
Check value	A computed value which is the result of passing a data value through a non-reversible algorithm. Check values are generally calculated using a cryptographic transformation, which takes as input a secret key and an arbitrary string and gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key must not be feasible.
Chip	The integrated circuit that is embedded into a plastic card designed to perform processing or memory functions. See also *Chip card*.
Chip card	A card or device embedded with an integrated circuit or chip that communicates information to a point-of-transaction terminal. Chip cards offer increased functionality through the combination of significant computing power and substantial data storage.
Chip Initialization	See *Pre-personalization.*

Term	Definition
Clear text	Information in a state that is understandable and meaningful. Something unencrypted.
Cloud-Based Provisioning	Preparation and delivery of Host Card Emulation data to a device.
COTS	Commercial off-the-shelf (consumer-grade) devices such as mobile phones and tablets.
Cryptographic key	A value that is used in a cryptographic algorithm for encryption or decryption.
Data Encryption Standard (DES)	The symmetric key methodology defined in ANSI X.3.92.
Data Preparation	A process by which cardholder data is managed and processed by the vendor for subsequent use in the personalization process.
Decipher, decrypt	To produce clear text from encrypted data.
Dual control	A process of utilizing two or more separate persons operating together to protect sensitive functions or information whereby no single person is able to access or utilize the materials—e.g., a cryptographic key.
EEPROM	Electronically erasable programmable read-only memory.
Facility	Facility includes external and internal structures subject to the requirements of Section 2, "Premises," of the Card Production and Provisioning Physical Security Requirements, even if the vendor is leasing the space.
Hardware (host) security module	An HSM is a type of SCD, a physically and logically protected hardware device that provides a secure set of cryptographic services. It includes the set of hardware, firmware, software, or some combination thereof that implements cryptographic logic, cryptographic processes, or both, including cryptographic algorithms.
Host Card Emulation (HCE)	Technology that permits a device to perform the function of a payment card on a Near Field Communication (NFC)-enabled device or via In-Apps without the use of a secure element.
Integrated circuit card	A card or device embedded with an integrated circuit chip that communicates information to a point-of-transaction terminal.
Integrated circuit chip	An electronic component designed to perform processing or memory functions.
International Organization for Standardization (ISO)	The specialized international agency that establishes and publishes international technical standards.
Issuer	An entity that is licensed by the payment scheme to issue cards and enters into a contractual relationship with the cardholder.

Term	Definition
Key component	One of at least two parameters having the characteristics (for example, format, randomness) of a cryptographic key that is combined with one or more like parameters, for example, by means of modulo-2 addition, to form a cryptographic key.
Key exchange	The process of importing, exporting, and distributing cryptographic keys using formalized procedures to ensure the security and integrity of those keys.
Key-exchange key (KEK)	A key used to encrypt and decrypt other keys during transport between entities in a key zone or within a given entity. It may also be used for local storage of keys. Also known as key-encipherment or key-encryption key.
Key generation	Creation of a new key for subsequent use.
Key management	The activities involving the handling of cryptographic keys and other related security parameters—e.g., initialization vectors, counters—during the entire life cycle of the keys, including their generation, storage, distribution, loading and use, deletion, destruction, and archiving.
Key-management device	A device used anywhere in the key life cycle for the management of keys. It may or may not be an SCD. Where required in the document, it must be an SCD. Examples include devices used for key loading or key generation.
Keying material	The data—e.g., keys and initialization vectors—necessary to establish and maintain cryptographic keying relationships.
Key (secret) share	One of at least two parameters related to a cryptographic key generated in such a way that a quorum of such parameters can be combined to form the cryptographic key but such that less than a quorum does not provide any information about the key.
Local Master Key (LMK)	See *Master File Key*.
Master Derivation Key (MDK)	The master key used to derive the keys used for the processing associated with card authentication, issuer authentication, and dispute processing.
Master File Key (MFK)	This is a symmetric key used to encrypt other cryptographic keys that are to be stored outside of the hardware security module (HSM).
Media	Any storage device used to place, keep, and retrieve data. The format used can include but is not limited to physical—e.g., paper—and electronic devices—e.g., chips, USB devices, tapes, disks.
Message authentication code (MAC)	A value cryptographically generated from some data using Triple DES in CBC mode.

Term	Definition
Mobile Provisioning	The personalization (provisioning) of a commercial off-the-shelf (COTS) device, such as an NFC-equipped mobile phone with appropriate cardholder account information. The information is transmitted to the device by a process called over-the-air (OTA) provisioning or alternatively, over-the-internet (OTI).
Multi-factor Authentication	Method of authenticating a user when two or more factors are verified. These factors include something the user has (such as a smart card or dongle), something the user knows (such as a password, passphrase, or PIN), or something the user is or does (such as fingerprints, other forms of biometrics, etc.).
Near field communication	A short-range wireless technology that enables data exchange over a distance of less than 10 cm. Also referred to as "contactless."
Office network	A collection of systems used for administrative purposes and removed from the production environment.
OTA	Over-the-air (OTA) refers to any process that involves the transfer of data (including applications) to the mobile device or any component within the mobile device via a mobile network.
OTI	Over-the-Internet (OTI): A remote connection from a security domain in the secure element to a backend server, using TLS over HTTP.
Non-console access	Refers to logical access to a system component that occurs over a network interface rather than via a direct, physical connection to the system component. Non-console access includes access from within local/internal networks as well as access from an external, or remote, network.
Participating Payment Brand	A payment card brand that, as of the time in question, is then formally admitted as (or an affiliate of) a member of PCI SSC pursuant to its governing documents. At the time of this publication, Participating Payment Brands include PCI SSC's Founding Members and Strategic Members.
Personalization	The process of applying the account and, when required for the product, cardholder-specific data to the card, uniquely tying the card to a given account. This includes encoding the magnetic stripe, embossing the card (if applicable), and loading data on to the chip. Personalization uses technology such as: Embossing Laser engraving Thermal transfer Indent printing
Personalization file	A file created by the issuer or issuer's processor that has all of the necessary information to personalize a card.

Term	Definition
Personalization Keys	Keys (loaded to the chip during pre-personalization) are used to provide authentication and confidentiality during personalization and to lock and unlock the chip before and after personalization. The keys are derived from the issuer Master Keys. The master keys may be the property of the issuer or the vendor.
PIN	A personal identification number that identifies a cardholder in an authorization request.
Plaintext	See *Clear text.*
Pre-personalization (Chip Initialization)	The process of replacing a transport key on a chip with an issuer-specific key and (optionally) activating the application.
Private Key	A cryptographic key, used with a public-key cryptographic algorithm, that is uniquely associated with an entity and is not made public. In the case of an asymmetric signature system, the private key defines the signature transformation. In the case of an asymmetric encipherment system, the private key defines the decipherment transformation.
Private Network	Network established by an organization that uses private IP address space. Private networks are commonly designed as local area networks. Private network access from public networks should be properly protected with the use of firewalls and routers. See also *Public Network*.
PROM	Programmable read-only memory.
Pseudorandom	The process of generating values with a high level of entropy and that satisfy various qualifications, using cryptographic and other non-hardware means.
Public key	A cryptographic key, used with a public-key cryptographic algorithm, uniquely associated with an entity, and that may be made public. In the case of an asymmetric signature system, the public key defines the verification transformation. In the case of an asymmetric encipherment system, the public key defines the encipherment transformation. A key that is "publicly known" is not necessarily globally available. The key may only be available to all members of a pre-specified group.

Term	Definition
Public Network	Network established and operated by a third-party telecommunications provider for the specific purpose of providing data transmission services for the public. Data over public networks can be intercepted, modified, and/or diverted while in transit. Examples of public networks include, but are not limited to: The Internet, Wireless technologies, including 802.11 and Bluetooth, Cellular technologies, for example, Global System for Mobile, communications (GSM), code division multiple access (CDMA), General Packet Radio Service (GPRS), Satellite communications. See also *Private Network.*
Random	The process of generating values with a high level of entropy and which satisfy various qualifications, using cryptographic and hardware-based means.
Remote Access	Access to a computer network from a location outside of that network. Remote access connections can originate either from inside the company's own network or from a remote location outside the company's network. An example of technology for remote access is VPN. For these requirements remote access is access from outside the HSA.
Secret key	A cryptographic key used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public. A secret key (symmetrical) cryptographic algorithm uses a single secret key for both encryption and decryption. The use of the term "secret" in this context does not imply a classification level; rather the term implies the need to protect the key from disclosure or substitution.
Secure cryptographic device (SCD)	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.
Secure Element	Tamper-resistant module in a mobile device capable of hosting/embedding applications in a secure manner. A secure element may be an integral part of the mobile device or may be a removable element that is inserted into the mobile device for use.
Segregation of Duties	Practice of dividing steps in a function among different individuals so as to keep a single individual from being able to subvert the process.
Sensitive data	Data that must be protected against unauthorized disclosure, alteration, or destruction—especially plain-text PINs and cryptographic keys—and includes design characteristics, status information, and so forth.

Term	Definition
Service Set Identifier (SSID)	SSID is a 32-character sequence that uniquely identifies a wireless LAN (WLAN). The SSID is the name of the wireless network.
Session key	A key established by a key-management protocol, which provides security services to data transferred between the parties. A single protocol execution may establish multiple session keys—e.g., an encryption key and a MAC key.
Simple Network Management Protocol (SNMP)	An Internet-standard protocol for managing devices on IP networks, such as routers, switches, servers, workstations, printers, and modem racks.
Split knowledge	A condition under which two or more persons separately and confidentially have custody of components of a single key that individually convey no knowledge of the resultant cryptographic key.
SQL injection	SQL injection is a code-injection technique that exploits a security vulnerability in a website's software. This is done by including portions of SQL statements in a web form entry field in an attempt to get the website to pass a newly formed rogue SQL command to the database—e.g., dump the database contents to the attacker.
Symmetric	In cryptography, where the same key is used for both encryption and decryption.
Topology Diagram	A visual representation of the network. It shows all the components that make up the network, including routers, devices, hubs, firewalls, etc. and how they interact.
Triple Data Encryption Standard (TDES)	An algorithm specified in *ISO/IEC 18033-3: Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*.
Trusted Certification Authority (CA)	Either a commercial CA or a PKI operated by the vendor. If the PKI is operated by the vendor, the CA must have been validated to comply with an industry standard, such as ETSI TS 101 456: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified authorities.
Variant of a key	A new key formed by a process (which need not be secret) with the original key, such that one or more of the non-parity bits of the new key differ from the corresponding bits of the original key.
Vendor	The legal entity and its associated premises that is approved by the payment scheme.
Vendor Program Administrator (VPA)	The payment system contact person or team that manages vendor compliance with the security requirements defined in this document.

Term	Definition
Virtual Private Network (VPN)	A technology that extends a (virtual) remote network to the VPN initiating source system. Upon successful connection, the default gateway of the source system points to the (virtual) remote network. Products based on current industry standards such as IPsec or OpenVPN protocols are acceptable VPN technologies.
Wireless site survey	A process that uses software and tools to analyze the RF output of a particular area and to adjust access point placement and signal strength output to optimize RF signal for a specific area. Wireless site survey applications take into account building materials, floor plans, windows and doors, furniture, and other physical and electronic data to determine the strength of a signal within and beyond the desired coverage area and to assess placement and parameters of the access point(s).
Working Key	A key used to cryptographically process the transaction. A working key is sometimes referred to as a data key, communications key, session key, or transaction key.
Zone Control Master Key	A key-encryption key used to encrypt other keys conveyed between nodes in a key zone.