Payment Card Industry (PCI)

Card Production and Provisioning

Logical Security Requirements

Version 2.0

December 2016

Document Changes

Date	Version	Author	Description
December 2012	1.x	PCI	RFC version
May 2013	1.0	PCI	Initial Release
March 2015	1.1	PCI	Enhancements for clarification
July 2016	2.x	PCI	RFC Version
December 2016	2.0	PCI	Addition of Mobile Provisioning and other changes. See Summary of Changes from v1.1 to v2.

Table of Contents

1 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 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.

1.1 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 out of scope for this document but can be found separately, in the *Payment Card Industry (PCI) Card Production and Provisioning Physical Security Requirements.*

1.2 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.

1.3 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.

1.4 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.

1.5 Limitations

For the purpose of this document, the scope will only cover the systems and environment used by the vendor in the process of data preparation, pre-personalization, and personalization. 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 payment brands are responsible for defining and managing compliance programs associated with these requirements. Contact the Payment Brand(s) of interest for any additional criteria.

2 Roles and Responsibilities

This section defines requirements that apply for the various roles and responsibilities relating to the management of the vendor's security policies and procedures. These requirements relate to:

- Information security personnel
- Assignment of security duties

2.1 Information Security Personnel

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").

b) The CISO must be an employee of the vendor.

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.

2.2 Assignment of Security Duties

a) The CISO must:

   i. Be responsible for compliance to these requirements.

   ii. Have sufficient authority to enforce the requirements of this document.

   iii. Not perform activities that they have the responsibility for approving.

   iv. Designate a back-up person who is qualified and empowered to act upon critical security events in the event the CISO is not available.

   v. Identify an IT security manager (if not themselves) responsible for overseeing the vendor's security environment.

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.

c) Where managers have security compliance responsibilities, the activities for which the manager has responsibility must be 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.

3 Security Policy and Procedures

3.1 Information Security Policy

a) The vendor must define and document an information security policy (ISP) for the facility.

b) Senior management must review and endorse the validity of the ISP at least once each year.

c) The ISP must include a named individual assigned as the “policy owner” and be responsible for management and enforcement of that policy.

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.

3.2 Security Procedures

a) The vendor must maintain procedures for each function associated with the ISP to support compliance with these requirements.

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.

c) Security procedures must describe the groups, roles, and responsibilities for all activities that protect cardholder data.

3.3 Incident Response Plans and Forensics

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.

b) Ensure staff report any unexpected or unusual activity relating to production equipment and operations.

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:

   i. Name of issuer

   ii. Type of data

   iii. Name and address of the vendor

   iv. Identification of the source of the data

   v. 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)

d) Investigate the incident and provide at least weekly updates about investigation progress.

e) Supply a final incident report providing the investigation results and any remediation.

f) Identify and preserve specific logs, documents, equipment, and other relevant items that provide evidence for forensic analysis.

4 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.

4.1 Classification

4.1.1 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 8 of this document, “Key Management: Secret Data.”

Examples:

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

4.1.2 Confidential Data

Confidential data is considered as 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. These are confidential data and must be managed in accordance with Section 9 of this document, “Key Management: Confidential Data.”

Examples:

- PAN, expiry, service code, cardholder name
- 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)

4.1.3 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.

4.1.4 Protections

Documented security requirements must exist that define the protection controls commensurate to the classification scheme.

All payment data must have an identifiable owner who is responsible for classification and for ensuring protection controls are implemented and working.

4.2 Encryption

All secret and confidential data must be:

a) Encrypted using algorithms and key sizes as stated in Normative Annex A.

b) Encrypted at all times during transmission and storage.

c) Decrypted for the minimum time required for data preparation and personalization.

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.

4.3 Access to Cardholder Data

The vendor must:

a) Document and follow procedures describing the vendor's data access requirements.

b) Prevent direct access to cardholder data from outside the cloud-based provisioning network or the personalization network.

c) Prevent physical and logical access from outside the high security area (HSA) to the data-preparation or personalization networks.

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.

e) Establish proper user authentication prior to access.

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.

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. PANs must be encrypted at all other times and decrypted only for the minimum time required for processing.

h) Apply appropriate measures to ensure that any third-party access meets the following requirements:

   i. Third-party access to cardholder or cloud-based provisioning data must be based on a formal contract referencing applicable security policies and standards.

   ii. 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.

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.

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.

k) Ensure that application (program) IDs used for cloud-based processes are used only for their intended purposes and not for individual user access.

4.4 Transmission of Cardholder Data

The requirements in this section apply to data transmitted to or from the issuer or authorized processor.

a) Data transmission procedures must incorporate the maintenance of a transmission audit log that includes, at a minimum:

   i. Date and time of transmission

   ii. Identification of the data source

b) 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.

c) The vendor must establish mechanisms that ensure the authenticity and validate the integrity of data transmitted and received.

d) The vendor must protect the integrity of cardholder data against modification and deletion at all times.

e) The vendor must accept data only from pre-authorized sources.

f) The vendor must log and inform the card brands of all issuers sending the vendor cardholder data in clear text.

g) If the file is not successfully transmitted, or only part of the data is received, the recipient must contact the sender to resolve. The vendor must inform the issuer or authorized processor as soon as possible that the file was not successfully received. Any incomplete data transmission received must be deleted under dual control and logged accordingly.

4.5 Retention and Deletion of Cardholder Data

The vendor must:

a) Ensure that procedures that define the vendor's data-retention policy are documented and 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.

   i. Ensure that the authorized retention period does not exceed six months from the date the card is personalized.

   ii. Ensure each issuer authorization to retain data is valid for no longer than two years.

c) Delete data on the personalization machine as soon as the job is completed.

d) Confirm the deletion of manually deleted data including sign-off by a second authorized person.

e) Conduct quarterly audits to ensure that all data beyond the data retention period has been deleted.

f) Ensure that all secret or confidential data has been irrecoverably removed before the media is used for any other purpose.

g) Ensure media destruction is performed 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.

h) Ensure data is always stored within the high security area (HSA).

i) Ensure that 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.

4.6 Media Handling

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.

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.

c) All removable media must be securely stored, controlled, and tracked.

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.

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:

   i. Unique identifier

   ii. Date and time

   iii. Name and signature of current custodian

   iv. Name and signature of recipient custodian

   v. Reason for transfer

f) Transfers of custody between two individuals must be authorized and logged.

g) Transfer of removable media to and from the HSA must be 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.

4.7 Contactless Personalization

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.

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.

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.

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.

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.

4.8 Data Used for Testing

a) Test (non-production) keys and test (non-production) data cannot be used with production equipment.

b) Cards used for final system validation or user acceptance that use production keys and/or data must be produced using production equipment.

4.9 Mobile Provisioning Activity Logs

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.

4.10 Decommissioning Plan

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.

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.

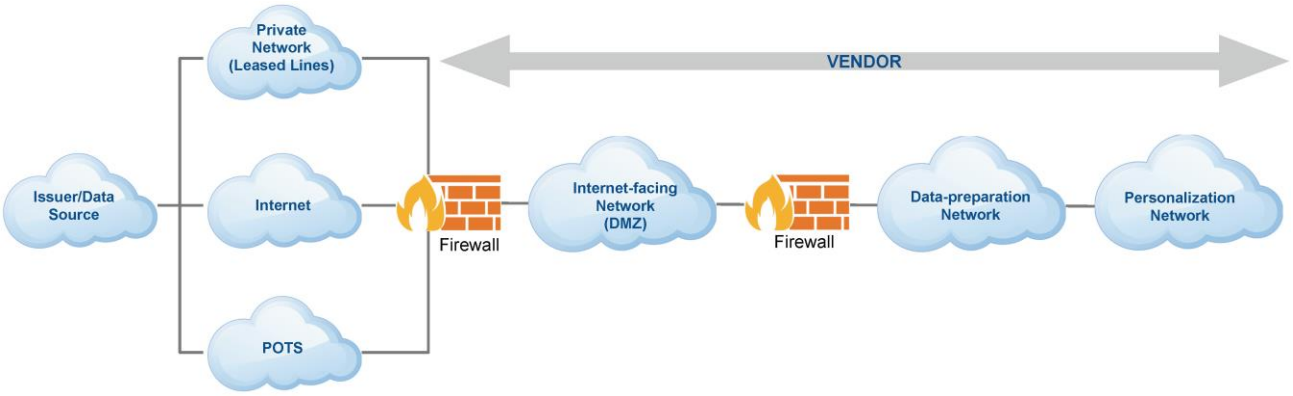
c) The disposition expectations for each identified item must be defined. For example, items may be returned to the owner, transported to an authorized user, or destroyed.

5 Network Security

5.1 Typical Vendor Network

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.

Figure 5-1



The diagram above shows a typical network setup of a vendor environment and a generic connection from the data source to the machines on the production floor.

Note: *The data-preparation and personalization systems may be on the same network.*

The following is a brief description of each of the network clouds:

5.1.1 Issuer / Data Source

This is the issuer that owns the cardholder data or that sends it to the vendor on behalf of the issuer.

5.1.2 Private Network (Leased lines), Internet, POTS

Cardholder data are typically sent over these three main types of network to the personalization vendor.

5.1.3 Card Production and Provisioning DMZ

This is the network segment that contains servers and applications that are accessible by an external network (i.e., any network that is outside the card-production network or its DMZ).

a) The DMZ must be dedicated to card production/provisioning activities.

b) The card production and provisioning network must be 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

d) The DMZ must be located in the Server Room of the HSA.

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.

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.

The following diagrams illustrate acceptable placement of the DMZ and associated firewalls:

Figure 5-2

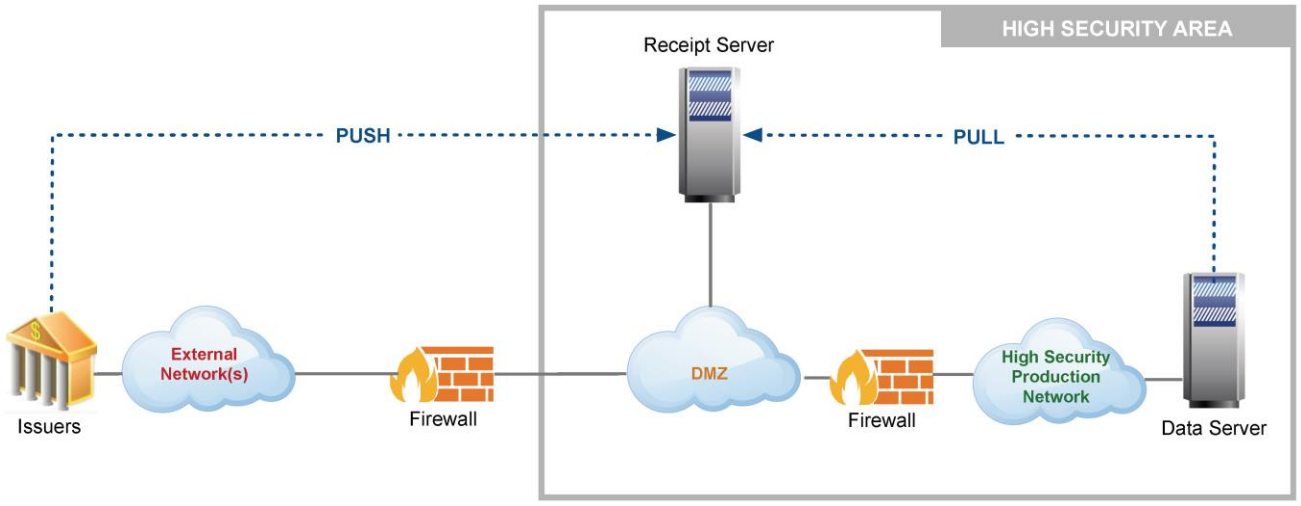
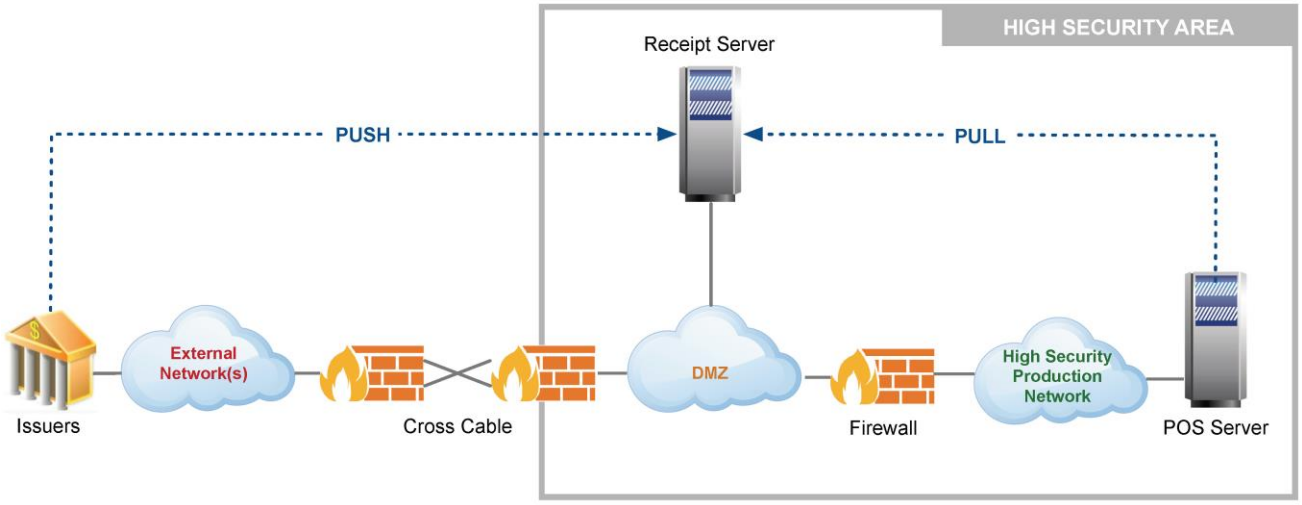


Figure 5-3



5.1.4 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.

5.1.5 Personalization Network

This is the network that contains the card personalization machines.

5.1.6 Mobile Provisioning Networks

HCE provisioning must be on its own network, but SE based provisioning is not required to be separated from other personalization networks.

Note: *See Appendix B for other topology examples.*

5.2 General Requirements

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.

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.

c) Ensure that the CISO accepts, by formal signature, the security implications of the current network topology.

d) Document the flow of cardholder and cloud-based provisioning data within the environment from the receipt/generation to end of its lifecycle.

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.

f) Systems and applications that make up the cloud-based provisioning network must be physically and logically segregated 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.

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.”

h) Be able to immediately assess the impact if any of its critical nodes are compromised.

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.

j) Control at all times the physical connection points leading into the personalization network and cloud-based provisioning network.

k) Prevent data from being tampered with or monitored by protecting the network cabling associated with personalization-data movement.

l) Transfer required issuer data and keys into the personalization network or the cloud-based provisioning network via a defined and documented process.

m) Ensure a process is in place for updates and patches and identification of their criticality, as detailed in Section 6.3.

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.

5.3 Network Devices

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.

b) Document the current network device configuration settings, rules set and justification for each device.

c) Ensure all available services are approved by an authorized security manager.

d) Implement logical and physical security controls that protect the integrity of network devices used.

e) Implement mechanisms to effectively monitor the activity on network devices.

f) Implement patches in compliance with Section 6.3, “Configuration and Patch Management.”

g) Maintain an audit trail of all changes and the associated approval.

h) Implement unique IDs for each administrator.

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.

j) Implement a mechanism to ensure that only authorized changes are made to network devices.

5.4 Firewalls

The requirements in this section apply to firewalls protecting the data-preparation and personalization networks.

5.4.1 General

The vendor must:

a) Ensure all documents relating to firewall configurations are stored securely.

b) Deploy an external firewall outside the HSA to protect the HSA’s DMZ (see figures 2 and 3 above for acceptable configurations).

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.

d) Deploy a firewall between the external network and the DMZ and between the DMZ and the cloud-based provisioning network.

e) Utilize physically separate firewalls for the aforementioned.

f) 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.

g) Implement appropriate operating-system controls on firewalls.

h) Review firewall rule sets and validate supporting business justification either:

- Monthly, or
- Quarterly with review after every firewall configuration change.

i) Restrict physical and logical access to firewalls to only those designated personnel who are authorized to perform firewall or router administration activities.

j) 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.

k) Ensure that only authorized individuals can perform firewall administration.

l) Run firewalls and routers on dedicated hardware. All non-firewall-related software such as compilers, editors, and communication software must be deleted or disabled.

m) Implement daily, automated analysis reports to monitor firewall activity.

n) Use unique administrator passwords for firewalls used by the personalization system and those passwords used for other network devices in the facility.

o) Implement mechanisms to protect firewall and router system logs from tampering, and procedures to check the system integrity monthly.

p) 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.

5.4.2 Configuration

The firewalls must:

a) Be configured to permit network access to required services only.

b) Be hardened in accordance with industry best practices, if the firewall is implemented on a commercial off-the-shelf (COTS) operating system.

c) Prohibit direct public access between any external networks and any system component that stores cardholder data.

d) Implement IP masquerading or Network Address Translation (NAT) on the firewall between the DMZ and personalization and the cloud-based provisioning networks.

e) If managed remotely, be managed according to Section 5.6, “Remote Access.”

f) Be configured to deny all services not expressly permitted.

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.

h) Disable source routing on the firewall.

i) Notify the administrator in real time of any items requiring immediate attention.

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

k) The vendor must perform baseline security configurations checks in the cloud- based provisioning environment either:

- Monthly or
- Quarterly with review after every configuration change

5.5 Anti-virus software or programs

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

b) Deploy anti-virus software on all systems potentially affected by malicious software—e.g., personal computers and servers.

c) Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.

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.

5.6 Remote Access

For purposes of this section, this applies to remote administration by the vendor, and not issuer connections.

5.6.1 Connection Conditions

a) Remote access is permitted only for the administration of the network or system components.

b) Access from outside the facility to the badge access system is not permitted.

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.

d) Access using personally owned hardware is prohibited.

e) Remote access is not permitted where qualified employees are temporarily off-site and remote access is a convenience.

f) The remote access process must be fully documented and include at least the following components:

   i. System components for which remote access is permitted

   ii. The location from which remote access is permitted

   iii. The conditions under which remote access is acceptable

   iv. Users with remote access permission

   v. The access privileges applicable to each authorized user

g) All access privileges must be validated on a quarterly basis by an authorized individual.

h) Remote access is prohibited 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.

j) The vendor must:

   i. Ensure that systems allowing remote connections accept connections only from preauthorized source systems.

   ii. Ensure remote administration is predefined and preauthorized by the vendor.

   iii. Ensure remote changes comply with change-management requirements as outlined in Section 6.2, “Change Management.”

   iv. Ensure that 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.

k) Ensure that non-vendor staff performing remote administration maintains liability insurance to cover potential losses. All 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.

5.6.2 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.

b) For remote access to DMZ components, the VPN must terminate at the target device.

c) SSL and TLS 1.0 are expressly prohibited in connection with the aforementioned.

d) Traffic on the VPN must be encrypted using Triple DES with at least double-length keys or Advanced Encryption Standard (AES).

e) Modifications to the VPN must be in compliance with the change-management requirements as outlined in Section 6.2, “Change Management.”

f) Mechanisms (e.g., digital signatures, checksums) must exist to detect unauthorized changes to VPN configuration and change-control settings.

g) Multi-factor authentication must be used for all VPN connections.

h) Access must be declined after three consecutive unsuccessful access attempts.

i) Access counters must only be 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.

k) Remote access must be logged, and the log must be reviewed weekly for suspicious activity. Evidence of log review must be maintained.

l) VPN traffic using Internet Protocol Security (IPSec) must meet the following additional requirements:

   i. Tunnel mode must be used except where communication is host-to-host.

   ii. Aggressive mode must not be used for tunnel establishment.

   iii. The device authentication method must use certificates obtained from a trusted Certificate Authority.

   iv. Encapsulating Security Payload (ESP) must be used to provide data confidentiality and authentication.

   v. The Perfect Forward Secrecy (PFS) option of Internet Key Exchange (IKE) must be used to protect against session key compromise.

5.7 Wireless Networks

5.7.1 General

The vendor must:

a) Implement a documented policy regarding wireless communications and clearly communicate this policy to all employees.

b) Not use wireless communications 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.

d) Use a wireless intrusion-detection system (WIDS) capable of detecting hidden and spoofed networks for all authorized wireless networks.

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.

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.

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.

5.7.2 Management

If wireless communication channels are used to transport any non-personalization data within 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.

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.

c) The vendor must deploy a firewall to segregate the wireless network and the wired network.

d) All wireless gateways must be protected with firewalls.

e) All wireless access points must be configured to prevent remote administration over the wireless network.

f) All wireless traffic must be encrypted with Triple DES or AES (see Annex A) and an encryption key of at least 128 bits, using WPA, WPA2, or 802.11x (or an equivalent protocol).

WEP encryption must not be used and must be disabled.

g) The service set identifier (SSID) must not be broadcast.

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.

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.

j) The vendor must disable the SNMP at all wireless access points.

k) Static passwords used to join wireless networks must be compliant with the requirements in Section 7.2, “Password Control,” but may be shared with other individuals in the organization on a need-to-know basis.

5.7.3 Additional Requirements for using Wi-Fi

If the wireless network uses Wi-Fi based on IEEE 802.11, the vendor must ensure that the following requirements are met:

a) Default SSID must be changed upon installation and must be at least 8 characters.

b) A log of media access-control addresses and associated devices (including 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.

c) A media access control address-based access-control list (ACL) must be used for access control of clients.

d) Wi-Fi Protected Access (WPA) must be enabled if the wireless system is WPA-capable.

e) Default passwords on the AP must be 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.

g) The AP must be assigned unique Internet protocol (IP) addresses instead of relying on Dynamic Host.

5.8 Security Testing and Monitoring

5.8.1 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).

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.

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.

d) Retain evidence of successful remediation and make this evidence available during site compliance evaluations upon request.

5.8.2 Penetration

The vendor must:

a) Perform internal and external penetration tests at least once a year and after any significant infrastructure changes.

   i. The internal penetration test must not be performed remotely.

   ii. Penetration tests must be performed on the network layer and include all personalization network components as well as operating systems.

   iii. Penetration tests must be performed on the application layer and must include:

      - Injection flaws (e.g., SQL injection)
      - Buffer overflow
      - Insecure cryptographic storage
      - Improper error handling
      - All other discovered 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.

c) Retain evidence of successful remediation and make this evidence available during site compliance evaluations upon request.

5.8.3 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 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. For networks where clear-text PINs traverse, the systems must not be configured to allow capture of clear PIN values.

b) Ensure 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.

6 System Security

6.1 General Requirements

The vendor must:

a) Document security controls that protect cardholder data and the cloud-based provisioning network.

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.

c) Change supplier provided default parameters prior to or during installation in the production environment.

d) Encrypt non-console administrative access when it takes place from within the personalization network.

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).

f) Restrict and secure access to system files at all times.

g) Ensure that virtual systems do not span different network domains.

h) Ensure that all components of the personalization network physically reside within the HSA.

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.

j) Ensure that the badge access-control system complies with the system security requirements in this document.

k) Ensure that the badge access is compliant to Section 7 of this document, “User Management and System Access Control.”

6.2 Change Management

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

b) Ensure that network and system changes follow a documented change-management process and the process is validated at least every 12 months.

c) Ensure all changes are approved by the CISO or authorized individual prior to deployment.

d) Ensure that the change-management process includes procedures for emergency changes.

e) Implement version identification and control for all software and documentation.

f) Ensure that the 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.

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.

6.3 Configuration and Patch Management

The vendor must:

a) Implement a documented procedure to determine 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.

c) Ensure 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.

e) Ensure that the configuration of 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 or 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).

h) Verify the integrity and quality of the patches before application, including source authenticity.

i) Make a backup of the system being changed before applying any patches. The backup must be securely stored.

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.

k) Ensure that emergency hardware and software implementations comply with the procedures and validation requirements established for emergency implementations.

l) Ensure that emergency hardware and software implementations follow the configuration and patch management requirements in this section.

6.4 Audit Logs

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 or product logs and application logs containing security events.

b) Ensure that audit logs include at least the following components:

i. User identification
ii. Type of event
iii. Valid date and time stamp
iv. Success or failure indication
v. Origination of the event
vi. Identity or name of the affected data, system component, or resources
vii. Access to audit logs
viii. Changes in access privileges

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, application, and operating systems.

d) Verify at least once a month that all systems are meeting log requirements.

e) Ensure that logs for all critical systems 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.

f) Protect and maintain the integrity of the audit logs from any form of modification.

g) Implement a security-incident and event-logging framework for its organization.

6.5 Backup and Recovery for Mobile Provisioning Networks

a) The backup and recovery procedures for mobile provisioning must be documented.

b) The procedures must include 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.

d) The vendor must protect backup copies from intentional or unintentional modifications or destruction.

e) Backups, whether stored within or outside of the HSA, must be encrypted and protected equivalent to the primary data as delineated in Section 4.1, “Classification.”

f) Controls must be established to prohibit creating 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.

6.6 Software Design and Development

6.6.1 General

The vendor must:

a) Document the design, development, and maintenance processes.

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.

c) Document all software components for each system and describe the functionality provided.

d) Protect any software backup copies from accidental destruction.

6.6.2 Design

The vendor must document the flow of personalization data within the environment from the receipt/generation to end of lifecycle.

6.6.3 Development

The vendor must:

a) Ensure access to source code for applications used on the personalization network is restricted to authorized personnel only.

b) Ensure that in-house-developed personalization software logs any restart (and details associated with that restart event).

c) Ensure that 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.

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.

6.7 Use of Web Services for Issuer Interfaces

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 5.6.2.

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.

c) All web services client and servers that are exposed to untrusted networks are protected by a suitably configured application firewall supporting message validation.

d) Implement controls to ensure message integrity.

6.8 Software implementation

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.

b) For internally developed software, ensure that security testing includes verification that temporary code, hard-coded keys, and suspicious code are removed.

c) Ensure all software implementation complies with Section 6.2, “Change Management.”

d) Test software prior to implementation to ensure correct operation.

e) Prevent debugging within production environment.

f) Have a predefined PC device configuration for PC devices used within the HSA.

g) Implement an approval process for all software beyond the standard PC device configuration for PC devices used within the HSA.

h) Ensure no unauthorized software can be installed.

i) Ensure all software is transferred from development to production in accordance with the change-control process.

7 User Management and System Access Control

7.1 User Management

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.

b) Restrict approval and level of access to staff with a documented business need before access is granted. At a minimum, documented approvals must be retained while the account is active.

c) Restrict systems access by unique user ID to only those individuals who have a business need.

d) Only grant individuals the minimum level of access sufficient to perform their duties.

e) Make certain that systems authentication requires at least the use of a unique ID and password.

f) Restrict administrative access to the minimum number of individuals required for management of the system.

g) Ensure that group, shared, and generic accounts and passwords are disabled wherever the system supports unique values.

h) 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.

i) 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 7.2 below.

j) Validate all system access at least quarterly.

k) Revalidate employee access to any systems upon a change of duties.

l) Ensure that access controls enforce segregation of duties.

m) For cloud-based provisioning, restrict issuer access and privileges to only the issuer's own cardholder data.

n) Strictly limit privileged or administrative access and ensure such access is approved by both the user's manager and the IT security manager.

o) Establish management oversight of privileged access to ensure compliance with segregation of duties.

p) Ensure that all privileged administrative access is logged and reviewed weekly.

7.2 Password Control

7.2.1 General

The vendor must:

a) Implement a policy and detailed procedures relating to the generation, use, renewal, and distribution of passwords.

b) Implement procedures for handling lost, forgotten and compromised passwords.

c) Distribute password procedures and policies to all users who have access to cardholder information or any system used as part of the personalization process.

d) Ensure that only users with administrative privileges can administer other users' passwords.

e) Not store passwords in clear text.

f) Change all default passwords.

7.2.2 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.

b) Newly issued passwords are changed on first use.

c) "First use" passwords expire if not used within 24 hours of distribution.

d) Systems enforce password lengths of at least eight characters.

e) Passwords consist of a combination of at least three of the following:

   i. Upper-case letters
   ii. Lower-case letters
   iii. Numbers
   iv. Special characters

f) Passwords are not the same as the user ID.

g) Passwords are not displayed during entry.

h) Passwords are encrypted during transmission and rendered unreadable when stored.

i) Passwords have a maximum life not to exceed 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.

k) The user's identity is verified prior to resetting a user password.

l) Authentication credentials to the tokenization process are secured to prevent unauthorized disclosure and use.

7.3 Session Locking

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.

b) Enforce a manual log-out process where manufacture and personalization equipment does not have the ability to automatically log off a user.

7.4 Account Locking

a) Accounts that have been inactive for a specified period (with a maximum of 90 days) must be removed from the system.

b) Systems must enforce the locking of a user account after a maximum of six unsuccessful authentication 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.

d) A user's account must be locked immediately upon that user leaving the vendor's employment until it is removed.

e) A user's account must be locked immediately if that user's 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:

   i. Remote access

   ii. Database

   iii. Application

   iv. OS

8 Key Management: Secret Data

8.1 General Principles

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.

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.

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.

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 dedicated and be 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 Appendix 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.

g) Cryptographic keys must not be hard-coded into software.

h) Audit trails must be maintained for all key-management activities.

i) Key-management activities must be performed by vendor or issuer staff.

j) Key-management activities must only be performed by fully trained and authorized personnel.

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.

l) All key-management activities must be documented, and all activities involving clear key components must be logged. The log must include:

   i. Unique identification of the individual that performed each function

   ii. Date and time

   iii. Function

   iv. Purpose

8.2 Symmetric Keys

Ensure that symmetric keys only exist in the following forms:

a) As plaintext inside the protected memory of a secure cryptographic device

b) As a cryptogram

c) 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.

   i. 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).

ii. No single person shall be able to access or use all components or a quorum of shares of a single secret cryptographic key.

8.3 Asymmetric Keys

Ensure that:

a) Private keys exist only in the following forms:

   i. As plaintext inside the protected memory of a secure cryptographic device

   ii. As a cryptogram

   iii. As two or more components or as part of an “m of n” sharing scheme where the value of “m” is at least two; managed using the principles of dual control and split knowledge

   iv. 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).

   v. No single person shall be able to access or use all components or a quorum of shares of a single private cryptographic key.

b) 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:

   i. Within a certificate,

   ii. Within a PKCS#10,

   iii. Within a SCD, or

   iv. With a MAC (message authentication code) created using the algorithm defined in ISO 16609.

c) Asymmetric keys also adhere to:

   i. The payment system requirements for obtaining the issuer certificate

   ii. The payment system specification for asymmetric keys

8.4 Key-Management Security Administration

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.

8.4.1 General Requirements

a) The vendor must define procedures for the transfer of key-management roles between individuals.

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.

8.4.2 Key Manager

a) There must be a nominated Key Manager with overall responsibility for all activities relating to key management.

b) CISO must approve the Key Manager for the position within the vendor.

c) The Key Manager must:

   i. Have a nominated deputy.

   ii. Be responsible for ensuring that all key-management activity is fully documented.

   iii. Be responsible for ensuring that all key-management activity is carried out in accordance with the documented procedures.

   iv. In collaboration with the personnel department, vet all key custodians to ensure their suitability for the role.

   v. Be an employee of the vendor

d) The Key Manager must be informed immediately of any security breach or loss of integrity relating to key activities.

e) The Key Manager must be responsible for ensuring that:

   i. All key custodians have been trained with regard to their responsibilities, and this forms part of their annual security training.

   ii. Each custodian signs a statement, or is legally bonded, acknowledging that they understand their responsibilities.

   iii. Key custodians who form the necessary threshold to create a key must not report directly to the same manager. If the Key Manager is also a key custodian, other key custodians must not report to the Key Manager if, in conjunction with the Key Manager, that would form a threshold to create a key.

f) The Key Manager must not have the right to override operations of the key custodians or perform activities for other key custodians.

8.4.3 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.

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.

c) The suitability of personnel must be reviewed on an annual basis.

d) They must be employees of the vendor and never temporary staff or consultants.

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.

f) Only fully trained key custodians and their backups may participate in 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.

8.4.4 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).

b) Only those person(s) who need access to a device must have access to the PIN or pass-phrase for that 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.

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.

8.5 Key Generation

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.

b) Key generation must take place in a hardware security module (HSM) that has achieved PCI approval or FIPS 140-2 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 Appendix A.

c) Cables must be inspected to ensure disclosure of a plaintext key or key component or share is not possible.

d) Use the principles of split knowledge and dual control 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 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.

f) Immediately destroy any residue from the printing or generation process that might disclose a component so that an unauthorized person cannot obtain it.

g) Ensure that a generated key is not at any time observable or otherwise accessible in plaintext to any person during the generation process.

h) Key components or shares must be placed in pre-serialized, tamper-evident envelopes when not in use by the authorized key custodian.

8.5.1 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.

b) Ensure that the generation of asymmetric key pairs ensures the secrecy of the private key and the integrity of the public key.

c) Create and manage asymmetric keys in compliance with the payment system requirements for obtaining the issuer certificate.

8.6 Key Distribution

a) Keys must be distributed only in their allowable forms.

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.

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.

   ii. A two-part form that identifies the sender and the materials sent must accompany the keying data.

   iii. The form must be signed by the sender and require that the recipient return one part of the form to the originator.

   iv. Key components or shares must be placed in pre-serialized, tamper-evident envelopes for shipment.

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.

   ii. Verify the contents of the package with the attached two-part form.

   iii. Return one part of the form to the sender of the component or share, acknowledging receipt.

   iv. Securely store the component or share according to the vendor's key storage policy.

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.

8.7 Key Loading

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 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).

c) Tokens, PROMs, or other key component/shares 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.

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.

   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.

e) All key loading activities must be under the control of the Key Manager.

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.

g) Make certain that the key-loading process does not disclose any portion of a key component/share to an unauthorized individual.

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.

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.

j) Once a key or its components/shares have been loaded and validated as operational, either:

   i. Securely destroy or delete it from the key-loading materials as defined in Section 8.11, “Key Destruction”; or

   ii. Securely store it according to these requirements if preserving the keys or components/shares for future loading.

8.8 Key Storage

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).

b) These envelopes must not be removable without detection.

c) An inventory of the contents of key storage safes must be maintained and audited quarterly.

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.

e) Ensure that access logs include, at a minimum, the following:

   i. Date and time (in/out)

   ii. Names and signatures of the key custodians involved

   iii. Purpose of access

   iv. 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.

8.9 Key Usage

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.

   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.

   iii. Public keys shall be used only to verify digital signature OR perform encryption operations.

   iv. Key-encrypting keys must never be used as working keys (session keys) and vice versa.

b) Transport 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.

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.

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.

e) There must be no process by which, once deployed, the life of a key can be extended beyond its original designated life span.

f) The vendor must:

   i. Prohibit any keys from being shared or substituted between production and test systems.

   ii. Prohibit keys used for pilots (i.e., limited production—for example via time, capabilities or volume) from being used for full product rollout unless the keys were managed to the same level of security compliance as required for production.

   iii. Ensure that any keys used for prototyping (i.e., using cards for proof of concept or process where production keys are not used) are not used in production.

   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.

   v. Ensure that private and secret keys exist in the minimum number of locations consistent with effective system operation.

   vi. Not use key variants except within the device with the original key.

   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.

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.

g) All derivation keys must be unique per issuer.

h) IC keys must be unique per IC.

i) Transport keys used for mobile provisioning must be unique per device.

8.10 Key Backup/Recovery

It is not a requirement to have back-up copies of key components, shares, or keys. However, if back-up copies are used, the requirements below must be met:

a) Ensure that key backup 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.

c) All relevant policies and procedures that apply to production keys must also apply to back-up keys.

d) Vendor must prohibit the loading of back-up keys into a failed device until the reason for that failure has been ascertained and the problem has been corrected.

e) The backup of keys must conform to Information Security Policy.

f) All access to back-up storage locations must be witnessed and logged under dual control.

8.11 Key Destruction

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.

b) When a cryptographic device (e.g., HSM) is decommissioned, any data stored and any resident cryptographic keys must be deleted or otherwise destroyed.

c) Securely destroy all copies of keys that are no longer required for card production or provisioning.

d) All key destruction must be logged and the log retained for verification.

e) Destroy keys and key components/shares so that it is impossible to recover them by physical or electronic means.

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.

g) Destroy all hard-copy key components/shares maintained on paper by cross-shredding, pulping, or burning. Strip shredding is not sufficient.

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.

i) Destroy all key components under dual presence with appropriate key-destruction affidavits signed by the applicable key custodian.

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.)

8.12 Key-Management Audit Trail

a) Key-management logs must contain, at a minimum, for each recorded activity:
   i. The date and time of the activity took place
   ii. The action taken (e.g., whether key generation, key distribution, key destruction)
   iii. Name and signature of the person performing the action (may be more than one name and signature if split responsibility is involved)
   iv. Countersignature of the Key Manager or CISO
   v. Pre-serialized key envelope number, if applicable

b) Key-management logs must be retained for at least 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.

d) Any facility to reset the sequence number generator or other mechanisms such as time and date stamps in the HSM must be restricted.

e) The CISO or an authorized individual must investigate all audit log validation failures.

f) During the personalization process, an electronic log must be maintained to identify what keys were used.

g) The vendor must ensure that the deletion of any audit trail is prevented.

8.13 Key Compromise

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
   ii. The actions to be taken to protect and/or recover system software and/or hardware, symmetric and asymmetric keys, previously generated signatures, and encrypted data
   iii. An investigation into the cause of the compromise, including a documented analysis of how and why the event occurred and the damages suffered.
   iv. 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).
   v. Where keys are issuer-owned, the issuer must be notified immediately for further instruction.

b) Ensure that the replacement key is not a variant of the compromised key.

c) Where a key compromise is suspected but not yet proven, the Key Manager must have the ability to activate emergency key replacement procedures.

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.

e) All keys that are encrypted with a key that has been revoked must also be revoked.

f) In the event that a KEK has been compromised, all keys encrypted with the KEK must be replaced.

g) In the event that a MDK has been compromised, all keys derived from that master key must be replaced.

h) The payment system VPA must be notified 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.

8.14 Key-Management Security Hardware

a) All key-management activity must be performed using a HSM.

b) When in its normal operational state:

   i. All of the HSM's tamper-responsive mechanisms must be activated.

   ii. All physical keys must be removed.

   iii. All unnecessary externally attached devices must be 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 Level 3, or higher.

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.

e) The process for the installation and commissioning of the HSM must be documented and logged.

f) When a HSM is removed from service permanently or for repair, all operational keys must be deleted from the device prior to its removal.

g) The removal process for the repair or decommissioning of the HSM must be documented and logged.

h) The HSM must be under physical dual control at all times.

9 Key Management: Confidential Data

9.1 General Principles

a) Key-encipherment keys must 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.

c) Cryptographic keys must not be hard-coded into software.

d) Audit trails must be maintained for all key-management activities.

e) Key-management activities must be performed by vendor or issuer staff.

f) Key-management activities must only be performed by fully trained and authorized personnel.

g) The vendor must generate keys and key components using a random or pseudo-random process.

h) Before the vendor accepts a key, it must ensure that it knows its origin.

i) Keys must be stored in a manner that preserves their integrity.

j) Keys must be used for only one purpose and not shared between cryptographic zones.

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.

l) There must be no process by which, once deployed, the life of a key can be extended beyond its original designated life span.

m) The vendor must prohibit any keys from being shared or substituted between production and test systems.

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.

o) The vendor must ensure that keys exist in the minimum number of locations consistent with 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.

q) The vendor must have a documented process for handling known or suspected key compromise that includes the revocation of the key.

r) In the event of the compromise of a key, all instances of the key must be revoked.

s) All keys that are encrypted with a key that has been revoked must also be revoked.

t) In the event that a KEK has been compromised, all keys encrypted with that KEK must be replaced.

10 PIN Distribution via Electronic Methods

10.1 General Requirements

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.

b) The PIN distribution system must run on a dedicated computer and be isolated from any other network 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.

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.

e) Communication of the PIN to the cardholder must only take place after verification of the identification value and associated authentication value.

f) The identification and authentication values must not disclose the account number.

g) The authentication value must be different than the identification value and must not be a value easily associated with the cardholder.

h) The authentication value must be communicated to the cardholder in such a way that access by anyone other than the cardholder is detected.

i) The authentication value must be restricted to the PIN distribution system and not accessible by any other system.

j) The PIN must only be distributed in response to the receipt of valid identification and authentication values.

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.

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.

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.

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).

o) The PIN distribution system must not contain any other cardholder data (e.g., PAN, cardholder name).

p) The association of the PIN to a specific account must not be possible in the distribution system.

q) The identification value, PIN, and authentication value must not be logged and must be 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.

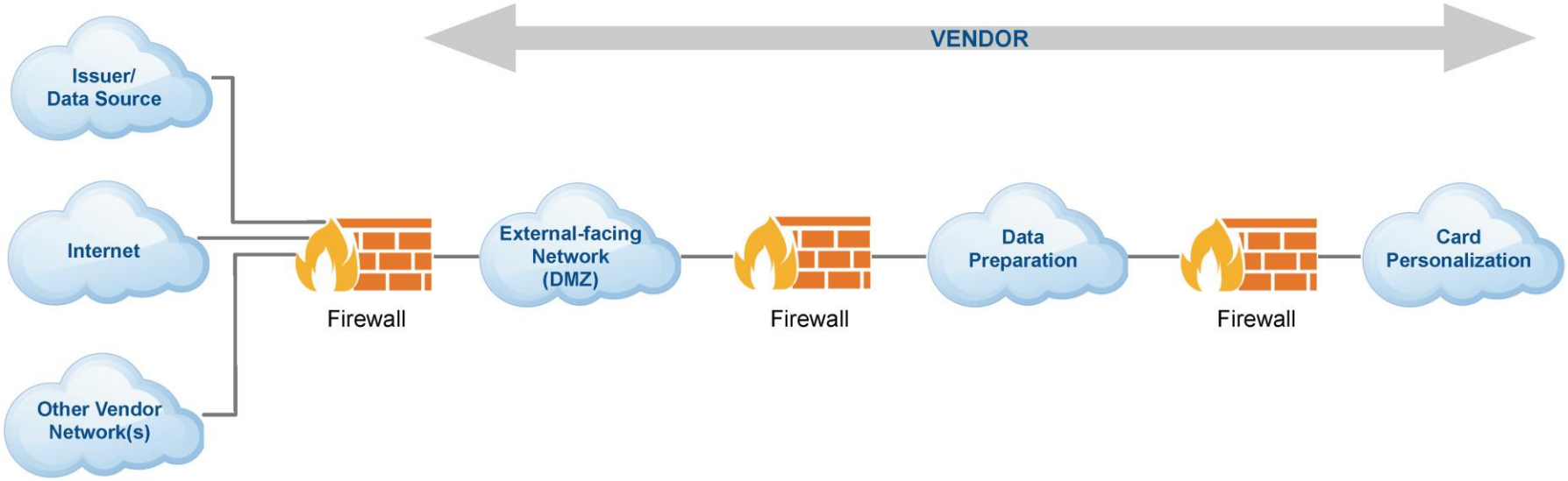
Appendix A: Applicability of Requirements

Logical Security Requirements				
Requirement	**Physical Cards**	**Mobile Provisioning**		**Conditions**
		SE	**HCE**	
Section 2 – Roles and Responsibilities				
All	X	X	X	All requirements applicable
Section 3 – Security Policy and Procedures				
All	X	X	X	All requirements applicable
Section 4 – Data Security				
4.1	X	X	X	
4.2	X	X	X	
4.3	X	X	X	
4.4	X	X	X	
4.5	X	X	X	
4.6	X	X	X	
4.7	X			
4.8	X	X	X	
4.9		X	X	
Section 5 – Network Security				
All	X	X	X	All requirements applicable
Section 6 – System Security				
6.1	X	X	X	
6.2	X	X	X	
6.3	X	X	X	
6.4	X	X	X	
6.5		X	X	
6.6	X	X	X	
6.7		X	X	
6.8	X	X	X	

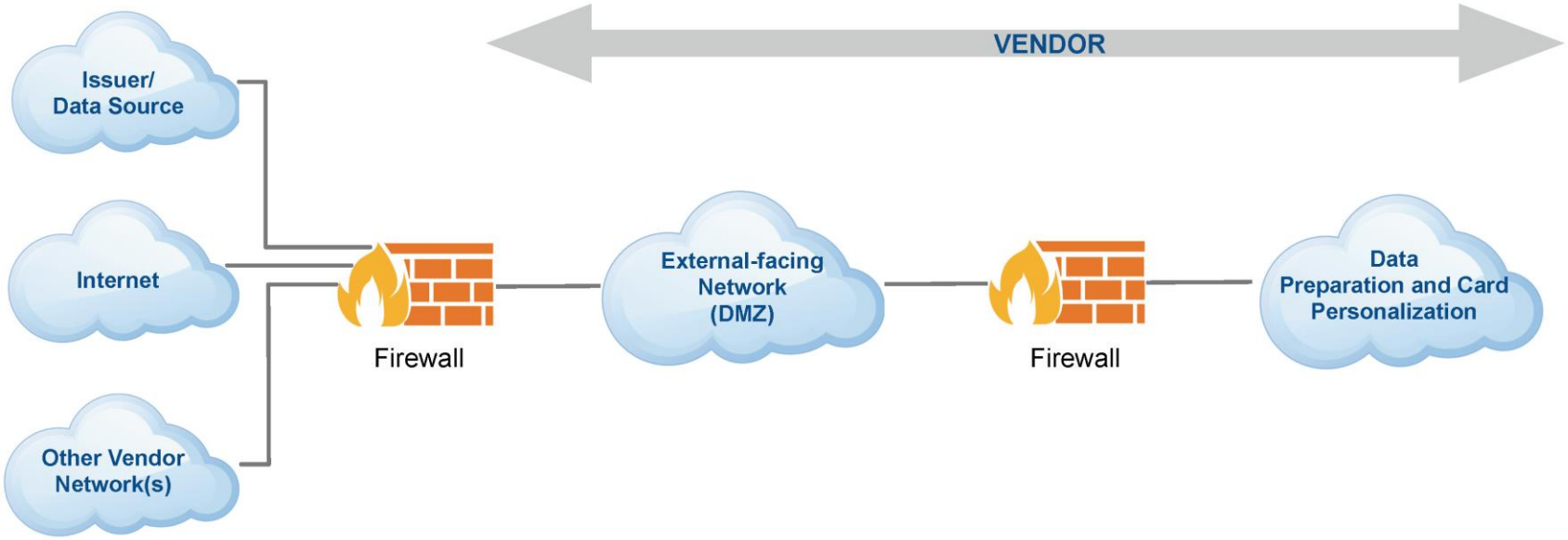
Logical Security Requirements				
Requirement	**Physical Cards**	**Mobile Provisioning**		**Conditions**
		SE	**HCE**	
Section 7 – User Management and System Access Control				
All	X	X	X	All requirements applicable
Section 8 – Key Management: Secret Data				
All	X	X	X	All requirements applicable
Section 9 – Key Management: Confidential Data				
All	X	X	X	All requirements applicable
Section 10 – PIN Distribution via Electronic Methods				
All	X	X	X	All requirements applicable

Appendix B: Topology Examples

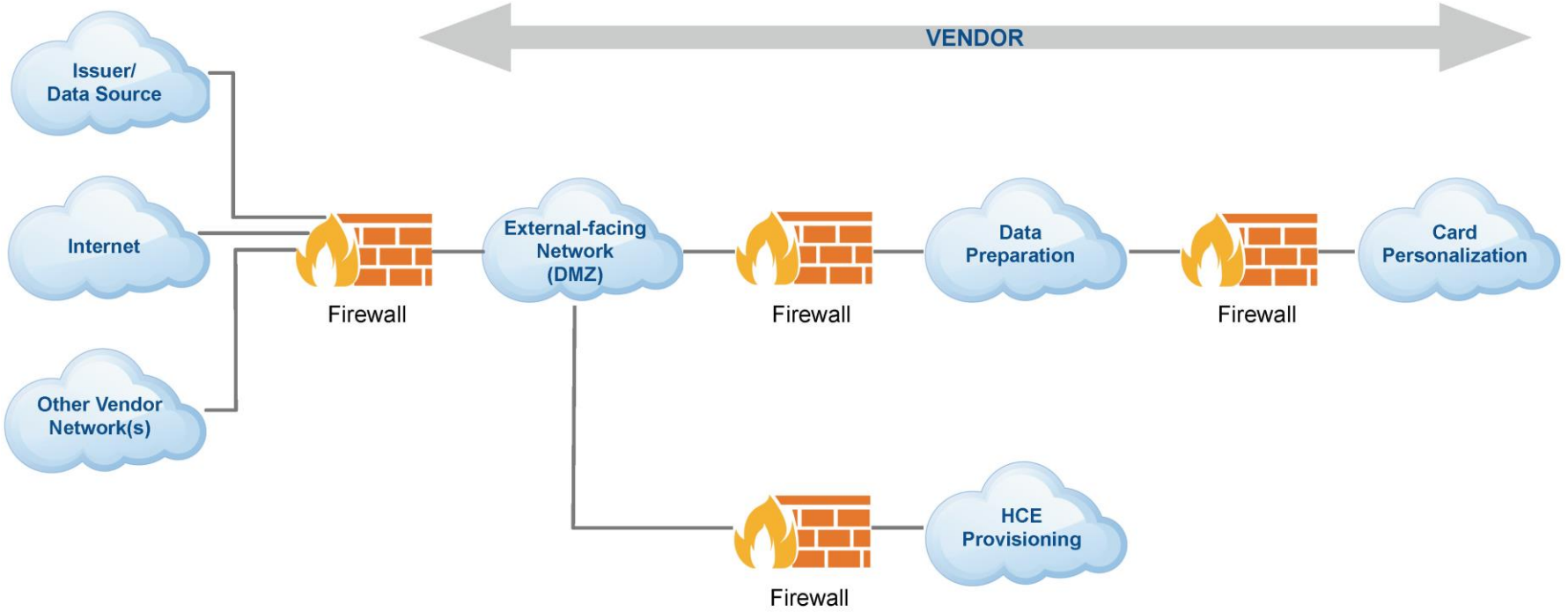
Example B1



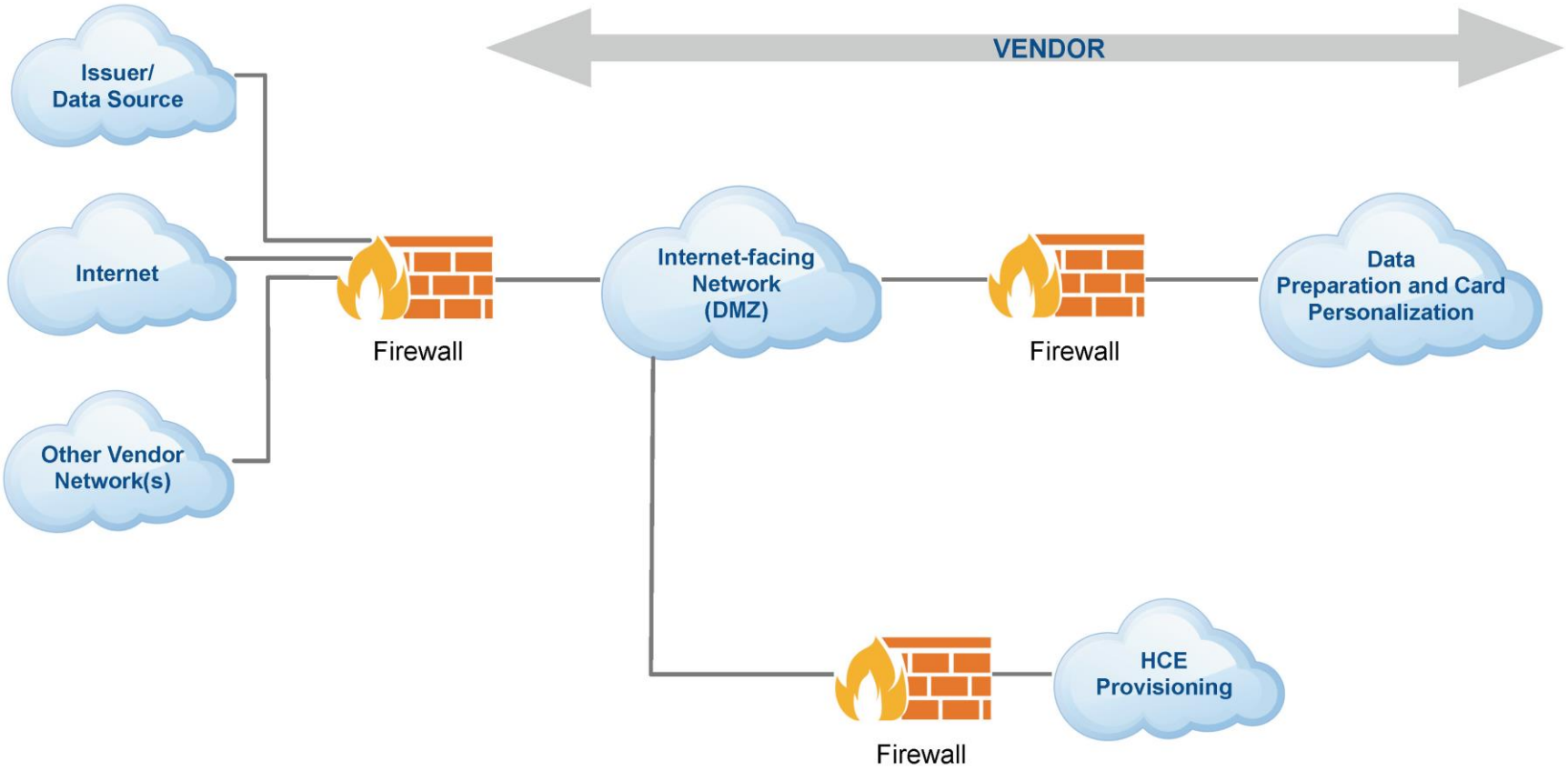
Example B2



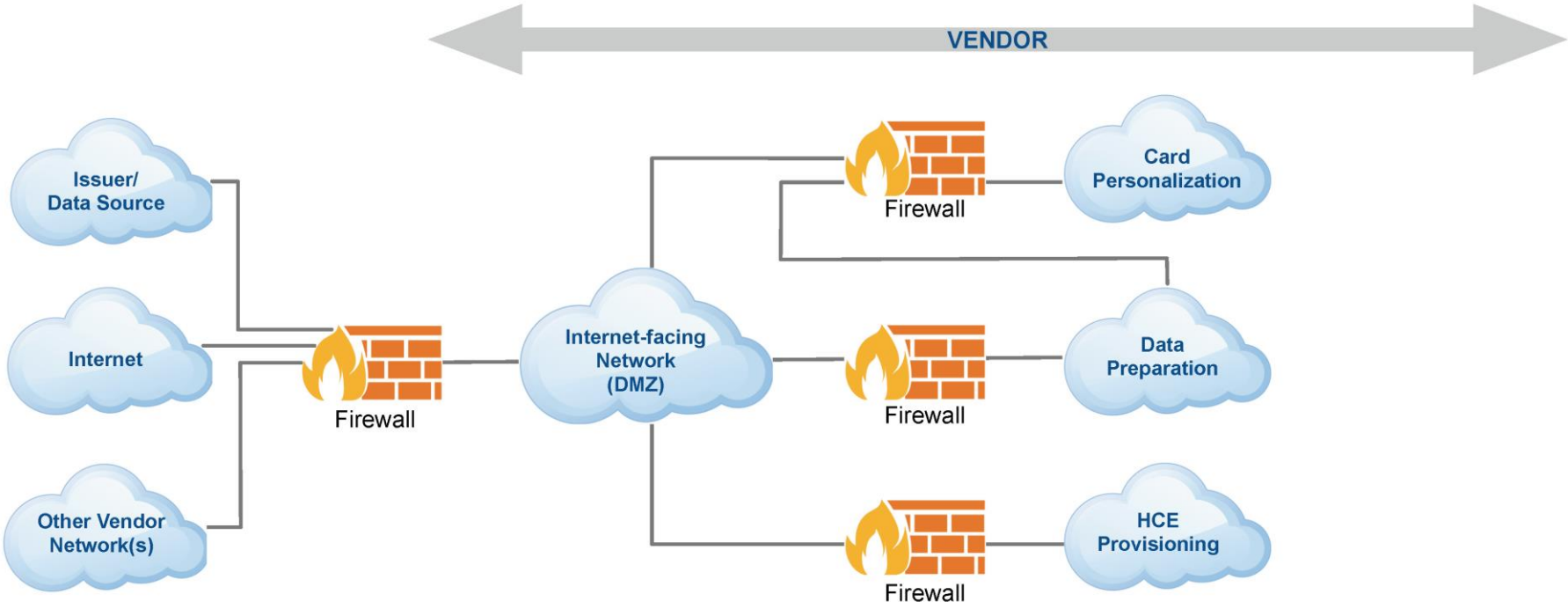
Example B3



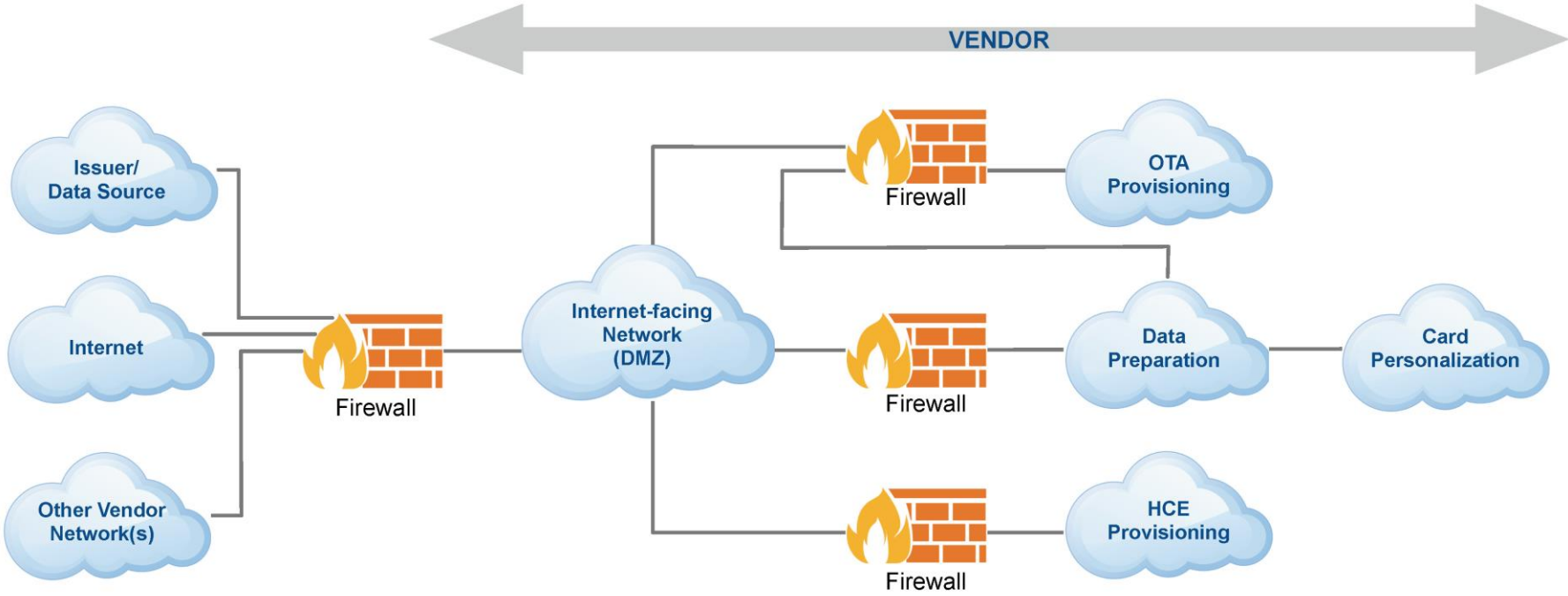
Example B4



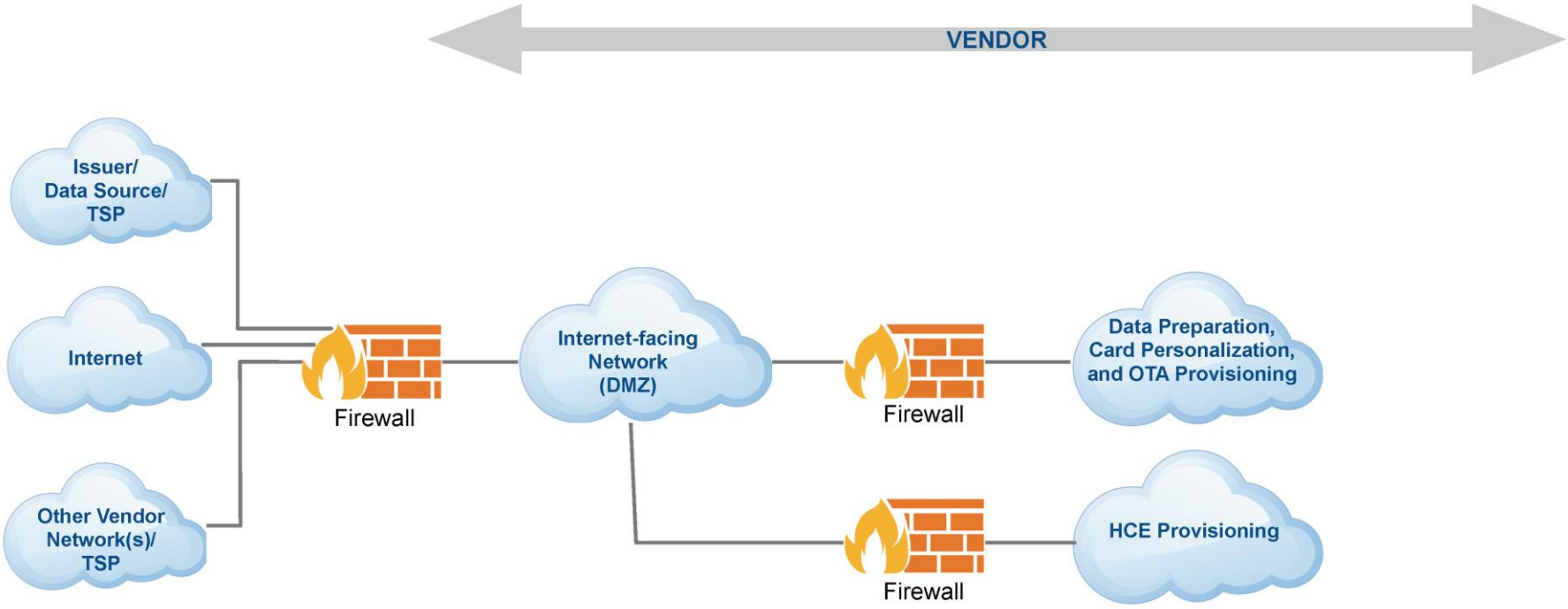
Example B5



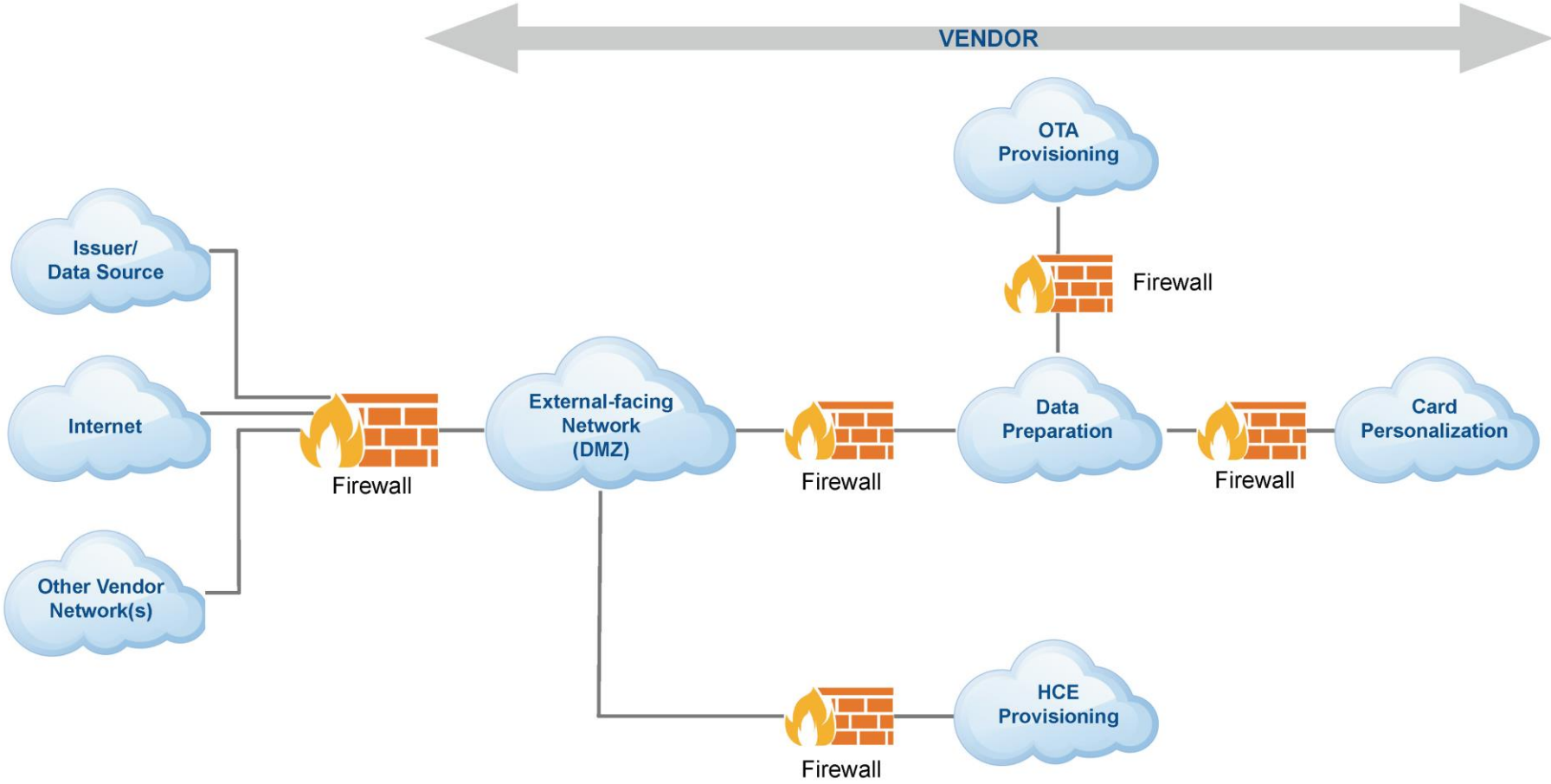
Example B6



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:

Algorithm	DES	RSA	Elliptic Curve	DSA	AES
Minimum key size in number of bits:	112	1024	160	1024/160	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	DES	RSA	Elliptic Curve	DSA/D-H	AES
Minimum key size in number of bits:	112	1024	160	1024/160	–
Minimum key size in number of bits:	168	2048	224	2048/224	–
Minimum key size in number of bits:	–	3072	256	3072/256	128
Minimum key size in number of bits:	–	7680	384	7680/384	192
Minimum key size in number of bits:	–	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 Diffie-Hellman 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*,). 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 Diffie-Hellman public keys using either DSA, a certificate, or a symmetric MAC (based on TDES—see *ISO 16609 – Banking – Requirements for message authentication using symmetric techniques;* Method 3 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.
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.*
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.

Term	Definition
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.
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.
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.

Term	Definition
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).
Message authentication code (MAC)	A value cryptographically generated from some data using Triple DES in CBC mode.
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).
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.
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: a) Embossing b) Laser engraving c) Thermal transfer d) Indent printing

Term	Definition
Personalization file	A file created by the issuer or issuer's processor that has all of the necessary information to personalize a card.
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.
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.
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 specific network from a different network.
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.

Term	Definition
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.
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.
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.