



Payment Card Industry (PCI)

Card Production and Provisioning Report on Compliance

Enter company name

Enter city name, Enter country name

Enter Assessor company name

For use with Logical Security Requirements v3.0.1

ROC Version 3.01

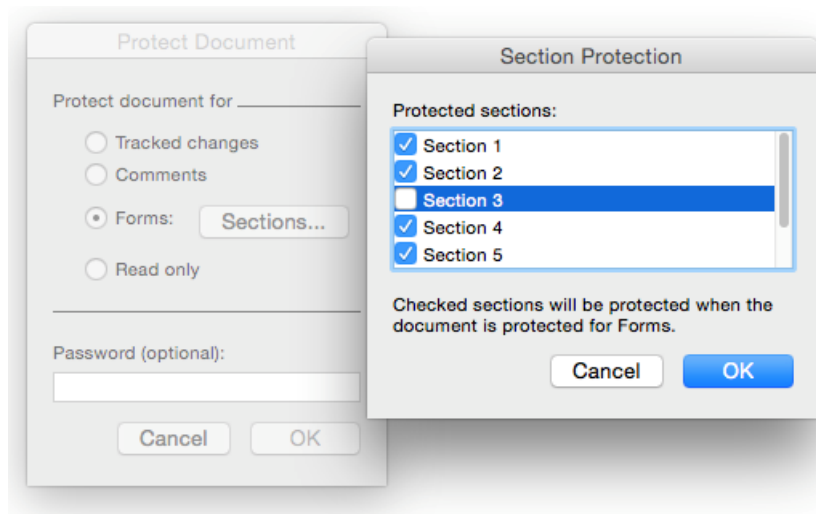
November 2023

Document Changes

Date	Version	Description
July 2015	1.0	Initial version
December 2015	1.0a	Minor errata
June 2016	1.0b	Expanded sections 2.2, 3.3 and 3.4
April 2017	2.0	Updated for changes incorporated into v2 of the Security Requirements, including Mobile Provisioning.
December 2017	2.1	Updated with addition of Test Procedures
June 2022	3.0	Updated for new requirements release
November 2023	3.0.1	Minor errata

Note to Assessors

When protecting this document for use as a form, leave Section 3 (page 11 of this document) unprotected to allow for insertion of network diagrams. Select “Sections,” then un-check Section 3 as illustrated below.



Contents

Document Changes	ii
Note to Assessors	iii
Introduction to the ROC Template.....	1
ROC Sections	2
ROC Vendor Self-Evaluation	2
ROC Summary of Assessor Findings.....	3
ROC Reporting Details.....	4
Do's and Don'ts: Reporting Expectations.....	4
ROC Template for PCI Card Production and Provisioning Security Requirements v3.0.1	5
1. Contact Information and Assessment Specifics.....	5
1.1 Contact Information	5
1.2 Location, Date, and Timeframe of Assessment.....	6
1.3 Card Production Activities.....	6
1.4 Mobile Provisioning Activities	7
2. Summary of Non-Compliance Findings.....	8
2.1 Non-Compliance Findings – Example.....	8
2.2 Non-Compliance Findings – Detail.....	9
3. Inspection Overview	9
3.1 Facility Description	13
3.2 High-level Network Diagram(s).....	13
3.3 Documentation Reviewed.....	16
3.4 Individuals Interviewed	16
4. Cryptographic Key Life Cycles (See Annex A for Examples)	22
Validating the Requirements	24
5. Findings and Observations	25
Section 1: Roles and Responsibilities	25
Section 2: Security Policy and Procedures	28
Section 3: Data Security	32
Section 4: Network Security.....	48
Section 5: System Security.....	82
Section 6: User Management and System Access Control.....	101
Section 7: Key Management: Secret Data	112
Section 8: Key Management: Confidential Data	158
Section 9: PIN Distribution via Electronic Methods	164
Annex A – Cryptographic Key Life Cycles – Examples	169

Introduction to the ROC Template

This document, the *PCI Card Production and Provisioning Report on Compliance* for use with *PCI Card Production and Provisioning Logical Security Requirements v3.0.1* ("ROC Reporting Template"), is the template for Payment Brand Assessors completing a Report on Compliance (ROC) for assessments against the *PCI Card Production and Provisioning Logical Security Requirements v3.0.1*.

The ROC Reporting Template serves two purposes:

- It serves as a declaration of the results of the card vendor's assessment of compliance with the *PCI Card Production and Provisioning Logical Security Requirements v3.0.1*
- It provides reporting instructions and the template for assessors to use. This can help provide reasonable assurance that a consistent level of reporting is present among assessors.

Contact the requesting payment brand for reporting and submission procedures.

Use of this reporting template is subject to payment brand stipulations for all Card Production and Provisioning v3.0.1 submissions.

Tables have been included in this template to facilitate the reporting process for certain lists and other information as appropriate. Additional appendices may be added if the assessor feels there is relevant information to be included that is not addressed in the current format. However, the assessor must not remove any details from the tables provided in this document.

Do not delete any content from any place in this document, including this section and the versioning above. These instructions are important for the assessor as the report is written and for the recipient in understanding the context from which the responses and conclusions are made. Addition of text or sections is applicable within reason, as noted above.

The Report on Compliance (ROC) is originated by the card vendor and further refined by the payment brand-designated assessor during the onsite card production vendor assessment as part of the card vendor's validation process. The ROC provides details about the vendor's environment and assessment methodology, and documents the vendor's compliance status for each Card Production and Provisioning Security Requirement. A PCI Card Production and Provisioning Security compliance assessment involves thorough testing and assessment activities, from which the assessor will generate detailed work papers. These work papers contain comprehensive records of the assessment activities including observations, results of system testing, configuration data, file lists, interview notes, documentation excerpts, references, screenshots, and other evidence collected during the course of the assessment. The ROC is effectively a **summary of evidence** derived from the assessor's work papers to describe how the assessor performed the validation activities and how the resultant findings were reached. At a high level, the ROC provides a comprehensive **summary of testing activities performed and information collected** during the assessment against the *PCI Card Production and Provisioning Logical Security Requirements v3.0.1*. The information contained in a ROC must provide enough detail and coverage to verify that the assessed entity is compliant with all PCI Card Production and Provisioning Security Requirements.

ROC Sections

The ROC includes the following sections and appendices:

- Section 1: Summary of Findings
- Section 2: Contact Information and Report Date
- Section 3: Summary Overview
- Section 4: Cryptographic Key Life Cycle
- Section 5: Findings and Observations

Note: Sections 1 through 4 must be thoroughly and accurately completed in order for the assessment findings in Section 5 to have the proper context. The reporting template includes tables with reporting instructions built-in to help assessors provide all required information throughout the document. Responses should be specific but efficient. Information provided should focus on concise quality of detail, rather than lengthy, repeated verbiage. Parroting the testing procedure within a description is discouraged, as it does not add any level of assurance to the narrative. Use of template language for summaries and descriptions is discouraged and details should be specifically relevant to the assessed entity.

ROC Vendor Self-Evaluation

The card vendor is asked to complete the card vendor self-evaluation in Section 5: Findings and Observations, for all requirements.

- Only one response should be selected at the sub-requirement level, and reporting of that should be consistent with other required documents.
- Select the appropriate response for “Compliant to PCI CP Requirement” for each requirement.
- In the “Comments/Remediation Date and Actions” section, the vendor may enter an explanation regarding its compliance that provides the payment brand assessor with additional information to be considered for the compliance assessment. In the event “No” is entered in the Compliance column, the vendor must state the planned remediation action and the date for the remediation. In the event "Not Applicable" is entered in the Compliance column, the vendor must explain why they believe the requirement does not apply for their situation.

ROC Summary of Assessor Findings

At each sub-requirement, under “Assessor Compliance Evaluation,” there is a column in which to designate the result. There are five options to summarize the assessor’s conclusion: Yes, New, Open, Closed, and Not Applicable.

The following table is a helpful representation when considering which selection to make and when to add comments. Remember, only one “Result” response may be selected at the sub-requirement level, and reporting of that should be consistent with other required documents.

Response	When to use this response:
Yes	Indicates the vendor is in compliance with this requirement
New	Indicates that this is a new non-compliance finding identified by the assessor for the first time.
Open	Indicates that this item was previously reported as a non-compliance finding, and action (if any) taken by the vendor does not resolve the original condition. The "Non-Compliance Description" column must explicitly state when this finding was first reported, the non-compliance condition observed, and the action (or lack thereof) taken by the vendor to resolve the finding. Findings for which the vendor has taken corrective action that resolved the original finding but introduced new non-compliance condition are reported as new findings for the applicable requirement.
Closed	Indicates that this item was previously reported as a non-compliance finding, and vendor corrective action has resolved the finding. The "Non-Compliance Description" column must describe the action the vendor has taken to resolve the finding.
Not Applicable	Indicates that the assessor’s assessment confirms that the requirement does not apply to for the vendor. Not Applicable responses are only expected if the requirement applies to an activity that the vendor does not perform.
Comment/ Non-Compliance Assessment	<p>Use this column to indicate:</p> <ul style="list-style-type: none"> ▪ Clarification describing the conditions observed in support of the assessor’s conclusion of compliance, or ▪ If non-compliance, a description of the reason for non-compliance. <p>Note that specific payment brands may require additional supporting details where compliance is noted.</p>

ROC Reporting Details

The reporting instructions in the Reporting Template explain the intent of the response required. There is no need to repeat the requirement or the reporting instruction within each assessor response. As noted earlier, responses should be specific and relevant to the assessed entity. Details provided should focus on concise quality of detail, rather than lengthy, repeated verbiage and should avoid parroting of the requirement without additional detail or generic template language.

Do's and Don'ts: Reporting Expectations

DO:	DON'T:
<ul style="list-style-type: none">▪ Use this Reporting Template when assessing against v3.0.1 of the Card Production and Provisioning Security Requirements.▪ Complete all sections in the order specified.▪ Read and understand the intent of each requirement and testing procedure.▪ Provide a response for every security requirement.▪ Provide sufficient detail and information to support the designated finding, but be concise.▪ Describe <i>how</i> a Requirement was verified per the Reporting Instruction, not just that it <i>was</i> verified.▪ Ensure all parts of the Reporting Instructions are addressed.▪ Ensure the response covers all applicable system components.▪ Perform an internal quality assurance review of the ROC for clarity, accuracy, and quality.▪ Provide useful, meaningful diagrams, as directed.	<ul style="list-style-type: none">▪ Don't simply repeat or echo the security requirement in the response.▪ Don't copy responses from one requirement to another.▪ Don't copy responses from previous assessments.▪ Don't include information irrelevant to the assessment.

ROC Template for PCI Card Production and Provisioning Security Requirements v3.0.1

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

1. Contact Information and Assessment Specifics

1.1 Contact Information

Client		
▪ Company name:		Payment Brand Identification Code:
▪ Company address:		
▪ Company URL:		
▪ Company contact:	Name:	
	Phone number:	E-mail address:
Assessor Company		
▪ Company name:		
▪ Company address:		
▪ Company URL:		
Assessor		
▪ Primary Assessor:	Name:	
	Phone number:	E-mail address:
▪ Secondary Assessor:	Name:	
	Phone number:	E-mail address:
▪ Secondary Assessor:	Name:	
	Phone number:	E-mail address:
Assessor Quality Assurance (QA) Primary Reviewer for this specific report <i>(not the QA Contact for the CPSA)</i>		
▪ QA Reviewer:	Name:	
	Phone number:	E-mail address:

1.2 Location, Date, and Timeframe of Assessment

▪ Address of facility where assessment was performed:		
▪ Date of Report (yyyy/mm/dd):		
▪ Timeframe of assessment (start date to completion date):	Start date (yyyy/mm/dd):	Completion date (yyyy/mm/dd):
▪ Was the review done onsite or remotely:	Select	
▪ If remote, state the rationale:		
▪ If applicable, identify date(s) spent onsite at the entity:	Start date (yyyy/mm/dd):	Completion date (yyyy/mm/dd):

1.3 Card Production Activities

Identify the functions for which a security assessment was performed and whether the function was added/discontinued since previous inspection.

▪ Card Manufacturing	Select	▪ Chip Embedding	Select
▪ Data Preparation	Select	▪ Card Personalization	Select
▪ Pre-Personalization	Select	▪ Chip Personalization	Select
▪ Fulfillment	Select	▪ Mailing	Select
▪ Packaging	Select	▪ Shipping	Select
▪ Storage	Select		
▪ PIN Printing and Mailing (personalized, credit or debit)	Select		
▪ PIN Printing (non-personalized prepaid cards)	Select		
▪ Electronic PIN Distribution	Select		
▪ Other (describe)			

1.4 Mobile Provisioning Activities

▪ Secure Element Provisioning Services		Select	▪ Cloud-based (HCE) Provisioning Services		Select
--	--	--------	---	--	--------

Secure Element Provisioning Services		
1. Select	Product/Solution	
	Description	
2. Select	Product/Solution	
	Description	
3. Select	Product/Solution	
	Description	
4. Select	Product/Solution	
	Description	
5. Select	Product/Solution	
	Description	

Cloud-based (HCE) Provisioning Services		
1. Select	Product/Solution	
	Description	
2. Select	Product/Solution	
	Description	
3. Select	Product/Solution	
	Description	
4. Select	Product/Solution	
	Description	
5. Select	Product/Solution	
	Description	

2. Summary of Non-Compliance Findings

Please use the table on the following page to report, covering all sections under each heading. Write up findings and list non-compliances—including the section reference number each non-compliance relates to—within the findings text as each non-compliance occurs. List all non-compliances in order, including the relevant section reference number the non-compliance—for example:

2.1 Non-Compliance Findings – Example

Requirement	New	Previous		Non-Compliance Findings Description
		Open	Closed	
1.1.b	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The CISO is not an employee of the vendor.
3.5.b	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Cardholder data is not deleted within 30 days of the date the card file is personalized.
4.1.1.a	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The DMZ is not dedicated to card production/provisioning activities.

Notes for Consideration

- Please ensure non-compliances are written exactly as the examples above and be as specific as possible down to the exact bullet that covers the non-compliance.
- Also list items that are **not** non-compliances but are items that either the assessor is unsure of, or the vendor has discussed with the assessor and questions arising from this discussion can only be answered by the applicable payment brand(s). This section is optional, so if not required, please delete it from the report.

3. Inspection Overview

3.1 Facility Description

The auditor must provide a general description of the vendor facility and card production environment. For example, “The facility consists of multiple buildings, and card production activities are performed in one building consisting of a High Security Area for card production. Administration functions are performed external to the HSA. The vendor being audited is the only occupant of this building.”

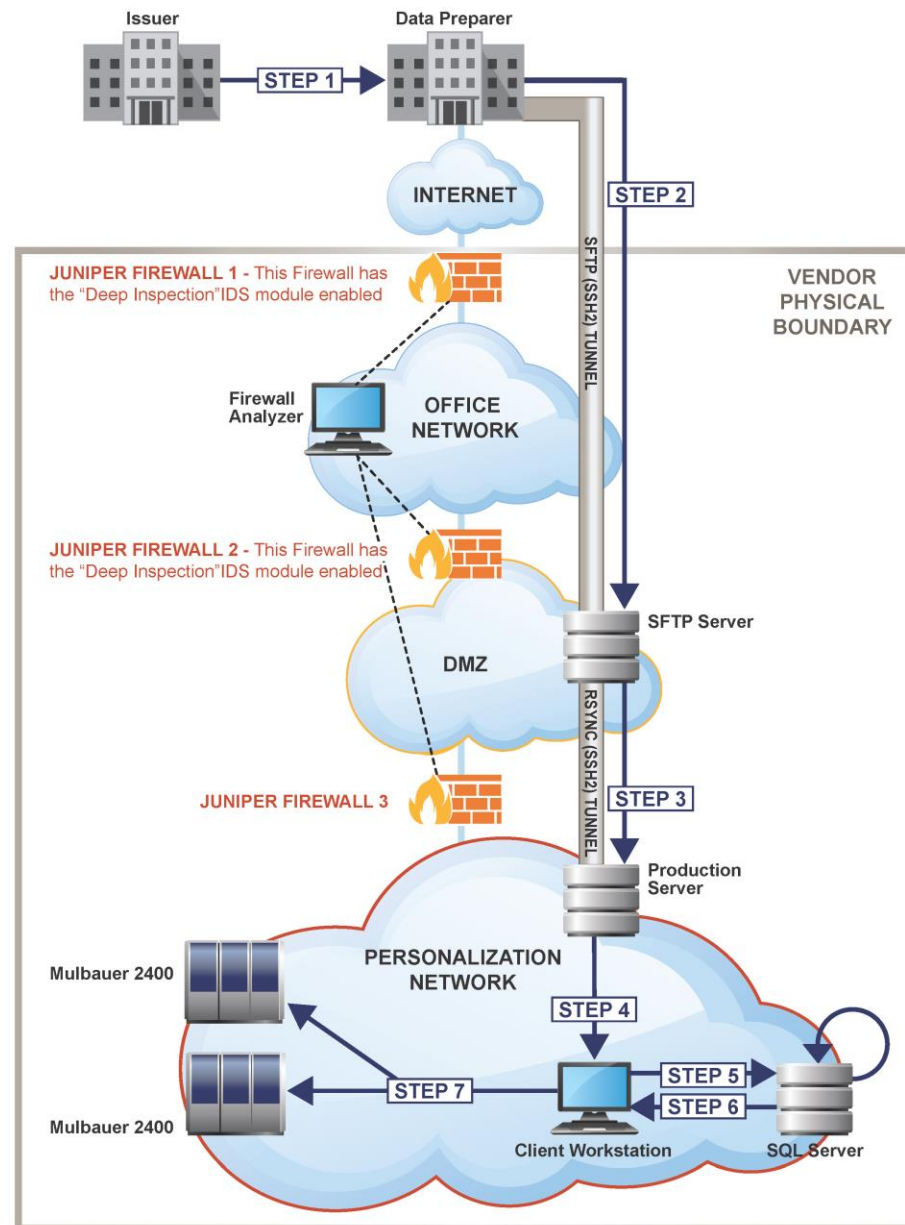
The introduction must also include any unusual conditions that may impact the audit scope or compliance assessment process. For example, “First audit after relocation, significant expansion / reconfiguration of the HAS, significant changes to key personnel, introduction of new technologies,” and any other unusual conditions.

<ul style="list-style-type: none"> Vendor Facility and Card Production and Provisioning Environment 	
<ul style="list-style-type: none"> Conditions that may Impact Audit Scope 	

3.2 High-level Network Diagram(s)

Provide a **high-level** network diagram (either obtained from the entity or created by assessor) of the entity’s networking topography, showing the overall architecture of the environment being assessed. This high-level diagram should demonstrate the data life-cycle using arrows and numbers similar to the example below. If more than one data path exists, this should be accounted for in the diagram and each should be clearly distinguishable.

Network Diagram Example





<Insert high-level network diagram(s)>

3.3 Documentation Reviewed

Identify and list all reviewed documents. Include the following:

Reference Number	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version)
Doc-1			
Doc-2			
Doc-3			
Doc-4			
Doc-5			
Doc-6			
Doc-7			
Doc-8			
Doc-9			
Doc-10			
Doc-11			
Doc-12			
Doc-13			
Doc-14			
Doc-15			
Doc-16			
Doc-17			
Doc-18			
Doc-19			
Doc-20			
Doc-21			
Doc-22			
Doc-23			
Doc-24			

Reference Number	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version)
Doc-25			
Doc-26			
Doc-27			
Doc-28			
Doc-29			
Doc-30			
Doc-31			
Doc-32			
Doc-33			
Doc-34			
Doc-35			
Doc-36			
Doc-37			
Doc-38			
Doc-39			
Doc-40			
Doc-41			
Doc-42			
Doc-43			
Doc-44			
Doc-45			
Doc-46			
Doc-47			
Doc-48			
Doc-49			
Doc-50			

Reference Number	Document Name (including version, if applicable)	Brief description of document purpose	Document date (latest version)
Doc-51			
Doc-52			
Doc-53			
Doc-54			
Doc-55			
Doc-56			
Doc-57			
Doc-58			
Doc-59			
Doc-60			
Doc-61			
Doc-62			
Doc-63			
Doc-64			
Doc-65			
Doc-66			
Doc-67			
Doc-68			
Doc-69			
Doc-70			
Doc-71			
Doc-72			
Doc-73			
Doc-74			
Doc-75			
Doc-76			

3.4 Individuals Interviewed

Identify and list the individuals interviewed. Include the following:

Reference Number	Employee Name	Role/Job Title	Organization	Summary of Topics Covered / Areas or Systems of Expertise (high-level summary only)
Int-1				
Int-2				
Int-3				
Int-4				
Int-5				
Int-6				
Int-7				
Int-8				
Int-9				
Int-10				
Int-11				
Int-12				
Int-13				
Int-14				
Int-15				
Int-16				
Int-17				
Int-18				
Int-19				
Int-20				
Int-21				
Int-22				
Int-23				
Int-24				

Reference Number	Employee Name	Role/Job Title	Organization	Summary of Topics Covered / Areas or Systems of Expertise (high-level summary only)
Int-25				
Int-26				
Int-27				
Int-28				
Int-29				
Int-30				
Int-31				
Int-32				
Int-33				
Int-34				
Int-35				
Int-36				
Int-37				
Int-38				
Int-39				
Int-40				
Int-41				
Int-42				
Int-43				
Int-44				
Int-45				
Int-46				
Int-47				
Int-48				
Int-49				
Int-50				

Reference Number	Employee Name	Role/Job Title	Organization	Summary of Topics Covered / Areas or Systems of Expertise (high-level summary only)
Int-51				
Int-52				
Int-53				
Int-54				
Int-55				
Int-56				
Int-57				
Int-58				
Int-59				
Int-60				
Int-61				
Int-62				
Int-63				
Int-64				
Int-65				
Int-66				
Int-67				
Int-68				
Int-69				
Int-70				
Int-71				
Int-72				
Int-73				
Int-74				
Int-75				
Int-76				

4. Cryptographic Key Life Cycles (See Annex A for Examples)

[illegible]

[illegible]

Validating the Requirements

The validation methods identified for each requirement describe the expected activities to be performed by the assessor to validate whether the entity has met the requirement. The intent behind each validation method is described as follows:

- **Examine:** The assessor critically evaluates data evidence. Common examples include documents (electronic or physical), screenshots, configuration files, audit logs, and data files.
- **Observe:** The assessor watches an action or views something in the environment. Examples of observation subjects include personnel performing a task or process, system components performing a function or responding to input, system configurations/settings, environmental conditions, and physical controls.
- **Interview:** The assessor converses with individual personnel. Interview objectives may include confirmation of whether an activity is performed, descriptions of how an activity is performed, and whether personnel have particular knowledge or understanding.
 - The validation methods are intended to allow the assessed entity to demonstrate how it has met a requirement. They also provide the assessed entity and the assessor with a common understanding of the assessment activities to be performed. The specific items to be examined or observed and personnel to be interviewed should be appropriate for the requirement being assessed, and for each entity's particular implementation.
 - When documenting the assessment results, the assessor identifies the validation activities performed and the result of each activity. While it is expected that an assessor will perform all the validation methods identified for each requirement, it is also possible for an implementation to be validated using different or additional methods. In such cases, the assessor should document why they used validation methods that differed from those identified in this document.

5. Findings and Observations

Section 1: Roles and Responsibilities

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
1.1 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").	Select		Examine applicable policies and procedures to verify that a senior manager has been designated as CISO and has IT security knowledge and responsibility of IT security management and cloud-based provisioning platform. Interview the CISO to determine their understanding of their roles and responsibilities.	Select	
b) The CISO must be an employee of the vendor.	Select		Examine employment documentation to verify employment and position.	Select	
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.	Select		Examine documented processes and verify reports or meeting minutes to ensure that monthly security compliance status or issues that pose potential risks are being reported by CISO to executive management.	Select	
1.2 Assignment of Security Duties					
a) The CISO must:					
i. Be responsible for compliance to these requirements.	Select		Interview the CISO and examine documentation to determine scope of responsibility.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
ii. Have sufficient authority to enforce the requirements of this document.	Select		Examine applicable policies and procedures to verify that a senior manager has been designated as CISO and has IT security knowledge and responsibility of IT security management and cloud-based provisioning platform.	Select	
iii. Not perform activities that he or she has the responsibility for approving.	Select		Examine logs or similar documentation to confirm the CISO does not perform activities related to the approval process for the vendor's Information Security Management and security of the cloud-based provisioning platform for which they have responsibility for approving.	Select	
iv. Designate a backup person who is empowered to act upon critical security events in the event the CISO is not available.	Select		Examine documentation that identifies the designated backup person who is empowered to act upon critical security events in the absence of the CISO. Interview the backup person to determine his or her understanding of his or her roles and responsibilities.	Select	
v. Identify an IT Security Manager (if not themselves) responsible for overseeing the vendor's security environment.	Select		Interview the CISO and examine documentation to conclude the individual or an appropriate designee has responsibility the vendor security environment.	Select	
vi. The back-up CISO and the IT Security Manager must be employees of the vendor.	Select		Interview the back-up CISO to verify role. Examine employment documentation to verify employment and position.	Select	

Section 1 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine logs or similar documentation to confirm the backup CISO does not perform activities related to the approval process for the vendor's Information Security Management and security of the cloud-based provisioning platform for which they have approval responsibility.	Select	
c) Where managers have security compliance responsibilities, the activities for which the manager has responsibility must be clearly defined.	Select		Examine documentation to authenticate the manager's security roles and responsibilities are clearly defined.	Select	
d) Staff responsible for day-to-day production activities must not be assigned security compliance assessment responsibility for the production activities that they perform.	Select		Interview security personnel or examine documentation—e.g., reviewing accounts on personalization machines and in the production workflow—to determine independence exists between day-to-day production operations and personnel performing security compliance assessments for those same production activities.	Select	

Section 2: Security Policy and Procedures

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.1 Information Security Policy					
a) The vendor must define and document an information security policy (ISP) for the facility and disseminate to all relevant personnel (including vendors, sub-contractors, and business partners).	Select		Examine the information security policy and verify that the policy is published. Interview a sample of relevant personnel to verify they are aware of the policy and that they have access to it.	Select	
b) Senior management must review and endorse the validity of the ISP at least once each year.	Select		Examine evidence—e.g., formal sign-off—that the information security policy has been reviewed and endorsed by senior management within the most recent 12-month period.	Select	
c) The ISP must include a named individual assigned as the “policy owner” and be responsible for management and enforcement of that policy.	Select		Examine the ISP to verify that: <ul style="list-style-type: none">• The information security policy designates a specific policy owner by name.• The policy owner is responsible for management and enforcement of that policy. Interview the policy owner to verify that the policy owner: <ul style="list-style-type: none">• Has acknowledged his or her responsibility.• Ensures that the policy is updated and changes communicated as needed.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		<p>Examine audit trails to verify they exist and:</p> <ul style="list-style-type: none"> • ISP updates are communicated to relevant staff. • Evidence of staff reviews and acceptance is maintained—e.g., automated systems for policy disbursement. <p>Interview a sample of staff to ensure that they are aware of the current ISP.</p>	Select	
2.2 Security Procedures					
a) The vendor must maintain procedures for each function associated with the ISP to support compliance with these requirements.	Select		Examine procedural documents to ensure procedures have been defined for each function described in the ISP—e.g., password policy, remote access policy.	Select	
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.	Select		<p>Interview a sample of staff to determine that procedures are followed to support compliance with these Security Requirements.</p> <p>Examine evidence that the procedures are reviewed, validated, and where necessary, updated annually.</p>	Select	
c) Security procedures must describe the groups, roles, and responsibilities for all activities that protect cardholder data.	Select		<p>Examine policies to verify that they clearly define information security responsibilities for all personnel.</p> <p>Interview a sample of responsible personnel to verify they understand the security policies.</p>	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
2.3 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.	Select		Examine the incident response plan and related procedures to verify the entity has a documented IRP addressing known or suspected compromise of any classified data. Interview personnel to determine that the IRP is communicated to relevant parties.	Select	
b) Ensure staff report any unexpected or unusual activity relating to production equipment and operations.	Select		Interview staff to determine that they report any unexpected or unusual activity relating to production equipment and operations. Examine evidence of existence of reported incidents.	Select	
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: (continued)	Select		Examine ISP documentation to verify notification procedures for suspected compromise of confidential or secret data to the VPA and impacted issuers are in place and requires reporting within 24 hours. Examine reported incidences to verify that law enforcement agencies were included in the written notification. Each notification must include at minimum the information outlined in Requirement 3.3c. Examine written notifications to determine weekly updates were issued during the investigation process.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
<p>2.3.c (cont.)</p> <ul style="list-style-type: none"> • Name of issuer • Type of data • Name and address of the vendor • Identification of the source of the data • Description of the incident including: <ul style="list-style-type: none"> – 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.	Select		Examine reports to determine a final report was provided and that the report contains results and any remediation.	Select	
e) Supply a final incident report providing the investigation results and any remediation.	Select		Examine incident response procedures to identify what logs, documents, equipment, or other relevant information is being preserved. Validate identified information is being preserved.	Select	

Section 2 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) Identify and preserve specific logs, documents, equipment, and other relevant items that provide evidence for forensic analysis.	Select		Examine incident response procedures to identify what logs, documents, equipment, or other relevant information is being preserved. Validate identified information is being preserved.	Select	

Section 3: Data Security

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

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
Definitions					
Secret Data					
<i>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.</i>					
<i>All symmetric (e.g., Triple DES, AES) and private asymmetric keys (e.g., RSA)—except keys used only for encryption of cardholder data—are secret data and must be managed in accordance with Section 7 of this document, “Key Management: Secret Data.”</i>					
<i>Examples:</i>					
<ul style="list-style-type: none">• Chip personalization keys• PIN keys and keys used to generate CVVs, CVCs, CAVs, or CSCs• PINs					

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
Confidential Data <i>Confidential data is considered any information that might provide the vendor with a competitive advantage or could cause business harm or legal exposure if the information is used or disclosed without restriction. Confidential data is data restricted to authorized individuals. This includes cardholder data and the keys used to encrypt cardholder data.</i> <i>Examples:</i> <ul style="list-style-type: none">• PAN, expiry, service code, cardholder name, Track 2 or Track 2 equivalent• TLS keys• Vendor evidence preserving data• Authentication credentials for requesting tokens• Mobile Station International Subscriber Directory Number (number used to identify a mobile phone number)					
Unrestricted/Public Data <i>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.</i>					
3.1.1 Protection Controls					
a) Documented security requirements must exist that define the protection controls commensurate to the classification scheme.	Select		Examine documentation to verify that data-protection controls are documented, and that the data-classification scheme differentiates between secret, confidential, and public data.	Select	
b) All payment data must have an identifiable owner who is responsible for classification for ensuring protection controls are implemented and working.	Select		Examine documentation to verify that data ownership identification is included in the data-protection controls. Examine a sample of stored data to verify that the data owner and security classification are identifiable.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
3.2 Encryption					
All secret and confidential data must be:					
a) Encrypted using algorithms and key sizes as stated in Normative Annex A.	Select		Examine key-management policies and procedures to verify that cryptographic keys used for secret and confidential data use algorithms and keys sizes that are in accordance with Annex A. Examine evidence for a sample of keys to verify that the key algorithms (select at least one asymmetric and one symmetric) and sizes used for secret and confidential data conform to the values defined in Annex A.	Select	
b) Encrypted at all times during transmission and storage.	Select		Interview personnel to identify controls in place for the transmission and storage of secret and confidential data. Examine transmission channels and data storage areas to verify that encryption is enabled and operating effectively for secret and confidential data.	Select	
c) Decrypted for the minimum time required for data preparation and personalization.	Select		Examine data flow and storage documentation and other supporting evidence to verify secret and confidential data is encrypted during storage and only decrypted for the minimum time needed to prepare data for personalization and perform personalization.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		<p>Examine documentation that describes the data flow to verify secret and confidential cardholder data:</p> <ul style="list-style-type: none"> Is decrypted only on the data-preparation, personalization, or cloud-based provisioning systems. Is never decrypted while the data is on an Internet- or public-facing network. Remains encrypted in the DMZ. Additional validation and assurance can be provided through checking the DMZ network for decryption/encryption software. 	Select	
3.3 Access to Cardholder Data					
The vendor must:					
a) Document and follow procedures describing the vendor's data access requirements.	Select		<p>Examine documentation to verify that the cardholder data access policy and procedure are documented.</p> <p>Observe a demonstration showing authorized access to cardholder data and that access attempted by an unauthorized user is declined.</p>	Select	
b) Prevent direct access to cardholder data from outside the cloud-based provisioning network or the personalization network.	Select		Examine access-control settings to verify cardholder data cannot be accessed from outside the cloud-based provisioning and personalization networks and systems.	Select	
c) Prevent logical access from outside the high security area (HSA) to the data-preparation or personalization networks.	Select		Examine access-control settings to verify logical access to the data preparation and personalization networks is prevented from outside the high security area (HSA).	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine a sample of access-control settings to verify that: <ul style="list-style-type: none"> The access rights for the individual are known. The reason for the access permission is available and access is justified. The individual does not have access permissions beyond those sufficient to perform his or her job. 	Select	
e) Establish proper user authentication prior to access.	Select		Examine documentation to determine whether user authentication procedures are defined. Observe a demonstration of the user authentication process to verify it conforms to procedures and provides confidence that the user was authenticated.	Select	
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.	Select		Examine a sample of audit trails to verify they exist for individual access to cardholder data and provide sufficient detail to identify the individual user.	Select	
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.	Select		Examine evidence that PANS are masked such that only the first six and last four digits are visible when displayed or printed. Examine evidence to verify that when a PAN is not masked the issuer has authorized the visible PAN and that the business justification is documented.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
<p>h) Apply appropriate measures to ensure that any third-party access meets the following requirements:</p> <ul style="list-style-type: none"> Third-party access to cardholder or cloud-based provisioning data must be based on a formal contract referencing applicable security policies and standards. Access to cardholder or cloud-based provisioning data and the processing facilities must not be provided until the appropriate access controls have been implemented and a contract defining terms for access has been signed. 	Select		<p>For all third-party service providers that have access to cardholder or provisioning data:</p> <ul style="list-style-type: none"> Examine evidence that a formal contract with the service provider exists and that it includes identification of and compliance with the applicable security policies and standards. Examine evidence to verify that access to cardholder and cloud-based provisioning data is not provided until a formal contract defining access terms is signed. 	Select	
<p>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.</p>	Select		<p>Examine database-access policies and procedures to verify that only authorized database administrators are granted direct access to cardholder or cloud-based provisioning databases while all other access is controlled through programmatic processes.</p> <p>Examine a sample of access-control settings to verify that only authorized database administrators are granted direct access to cardholder or cloud-based provisioning databases while all other access is controlled through programmatic processes.</p>	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine evidence that data access activity logs exist and that the logs are reviewed at least weekly. Observe a demonstration that direct access to data contained in databases is limited to authorized database administrators.	Select	
k) Ensure that application (program) IDs used for cloud-based processes are used only for their intended purposes and not for individual user access.	Select		Examine evidence to verify that application IDs for cloud-based processes cannot be used for individual user access and the IDs can only be used for their intended purpose. Observe a demonstration to verify that application IDs used for cloud-based processes cannot be used for individual user access.	Select	
3.4 Transmission of Cardholder Data					
<i>The requirements in this section apply to data transmitted to or from the issuer or authorized processor.</i>					
a) Cardholder data transmission procedures must incorporate the maintenance of a transmission audit log that includes, at a minimum: <ul style="list-style-type: none"> • Date and time of transmission • Identification of the data source 	Select		Examine a sample of cardholder data transmission logs to verify they exist and at a minimum contain the date/time of transmission and identification of the data source.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Cardholder data transmitted to or received from an external source or transferred on the cloud-based provisioning network must be encrypted and decrypted per the encryption requirements of this document.	Select		Interview DBAs to identify where cardholder data is encrypted and decrypted when transmitted to or received from an external source or transferred on the cloud-based provisioning network. Examine network and/or data-flow diagrams or other evidentiary documentation to verify that provisioning cardholder data transmitted to / received from an external source is only encrypted/decrypted as per the encryption requirements in this document—e.g., encryption strengths, algorithms, locations, durations, etc.	Select	
c) The vendor must establish mechanisms that ensure the authenticity and validate the integrity of cardholder data transmitted and received.	Select		Examine policies and procedures to verify that cardholder data transmitted and received is authenticated and validated. Interview personnel to verify that upon transmission or receipt the cardholder data authentication and validation process complies with the defined procedure.	Select	
d) The vendor must protect the integrity of cardholder data against modification and deletion at all times.	Select		Examine procedures and the production data flow to verify that cardholder data integrity is protected against modification and deletion.	Select	
e) The vendor must accept cardholder data only from pre-authorized sources that are defined and documented.	Select		Examine documentation to verify that authorized cardholder data sources are defined. Examine data transmission logs to verify that cardholder data is received from and sent only to pre-authorized locations.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) The vendor must log and inform the card brands of all issuers sending the vendor cardholder data in clear text.	Select		Examine policy and procedure documentation to verify a process is in place to identify clear-text cardholder data sent by an issuer and report it to the VPA. Examine evidence to verify that any identified clear-text cardholder sent by an issuer was reported to the VPA.	Select	
g) If the file is not successfully transmitted, or only part of the cardholder data is received, the recipient must contact the sender to resolve. The vendor must inform the issuer or authorized processor upon discovery that the file was not successfully received. Any incomplete cardholder data transmission received must be deleted under dual control and logged accordingly.	Select		Examine documentation to verify the vendor has procedures to: <ul style="list-style-type: none"> Resolve cardholder data transmission errors. Notify the issuer or authorized processor upon discovery that the file was not successfully received. Delete under dual control and log any incomplete cardholder data transmissions. 	Select	
3.5 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.	Select		Examine policies and procedures to verify that a data-retention policy exists. Examine evidence that the retention policy is followed.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Delete cardholder data within 30 days of the date the card file is personalized unless the issuer has authorized longer retention in writing. <ul style="list-style-type: none"> • Ensure that the authorized retention period does not exceed six months from the date the card is personalized. • Ensure each issuer authorization to retain cardholder data is valid for no longer than two years. 	Select		Examine a sample of retained cardholder data to verify that it is not retained longer than 30 days after personalization unless the issuer has authorized longer retention in writing. Verification of data deletion must include any data backups and return files in the DMZ that contain cardholder data. Examine evidence of issuer authorization for personalization data retained longer than 30 days after personalization. Examine issuer authorization that allows for cardholder data retention longer than 30 days to verify that the authorization is less than two years old. Examine a sample of cardholder data authorized for retention longer than 30 days and verify that: <ul style="list-style-type: none"> • Cardholder data is deleted in compliance with the authorized retention period. • Cardholder data is not retained longer than the six-month maximum. 	Select	
c) Delete data on the personalization machine as soon as the job is completed.	Select		Examine a sample of completed batches to verify that cardholder data is deleted from the personalized machine once the job is completed.	Select	
d) Confirm the deletion of manually deleted cardholder data including sign-off by a second authorized person.	Select		Examine evidence for a sample to verify that any cardholder data manually deleted was deleted with sign-off by an authorized secondary party.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Conduct quarterly audits to ensure that all cardholder data beyond the data retention period has been deleted.	Select		Examine evidence for a sample to verify that quarterly audits were conducted to ensure all cardholder data was deleted if it was retained beyond its authorized retention period.	Select	
f) Ensure that all cardholder data has been irrecoverably removed before the media is used for any other purpose.	Select		Examine evidence for a sample to verify that all cardholder data was irrecoverably removed before the media was used for another purpose.	Select	
g) Ensure media destruction is performed under CCTV surveillance according to industry standards (see <i>ISO 9564-1: Personal Identification Number Management and Security</i>) under dual control, and that a log is maintained and signed confirming the destruction process.	Select		Observe CCTV recordings for an example to verify that: <ul style="list-style-type: none"> Media is destroyed in accordance with industry standards and under dual control; and a log is maintained and signed confirming the destruction process. 	Select	
h) Ensure cardholder data is always stored within the high security area (HSA).	Select		Examine the data storage policy and procedures to verify cardholder data is being stored within the designated high security area. Observe the cardholder data storage location to verify it is a high security area.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
i) Ensure that cardholder data retained for longer than 30 days after personalization complies with the following additional requirements. This data must: <ul style="list-style-type: none"> • Be removed from the active production environment. • Be stored on a separate server or media • Be accessible only under dual control. 	Select		Observe the cardholder data storage area utilized for data retained longer than 30 days after personalization to verify that the data: <ul style="list-style-type: none"> • Is removed from the active production environment. • Is stored on a separate server or media. • Can only be accessed under dual control. 	Select	
3.6 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.	Select		Examine the vendor's policies and procedures for removable media documentation to verify it exists and includes devices such as laptops, mobile devices, USB devices, tapes, and disks.	Select	
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.	Select		Observe a sample of removable media within the HSA to verify it is clearly labeled with a unique identifier and data classification.	Select	
c) All removable media must be securely stored, controlled, and tracked.	Select		Observe the removable media storage location to verify the area is secure. Examine the removable media check-in/out process to verify an audit trail is maintained and that it provides an accurate record of media possession.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		<p>Examine a sample of checked-out, removable media within the HSA or the cloud-based provisioning environment to verify:</p> <ul style="list-style-type: none"> • The media is in the custody of the person to whom the media was issued. • The individual is authorized to possess the media. • That individual does not have the ability to decrypt any sensitive or confidential data contained on that media other than in compliance with procedures for handling sensitive or confidential data. • The media does not contain clear-text confidential data. 	Select	
<p>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:</p> <ul style="list-style-type: none"> • Unique identifier • Date and time • Name and signature of current custodian • Name and signature of custodian recipient • Reason for transfer 	Select		<p>Examine the media audit trail documentation to verify that it contains at least the following data points:</p> <ul style="list-style-type: none"> • Unique media identifier • Date and time logged out and returned • Name and signature of the current custodian • Name and signature of custodian recipient • Reason for transfer 	Select	
f) Transfers of custody between two individuals must be authorized and logged.	Select		Examine evidence that any transfer of checked out media is authorized and logged.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) Transfer of removable media to and from the HSA must be authorized and logged.	Select		Examine a sample of media that was removed from the HSA to verify that the removal was authorized and logged.	Select	
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.	Select		Examine evidence that media containing secret or confidential media is destroyed in a manner that makes it impossible to recover the data.	Select	
3.7 Contactless Personalization					
<i>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.</i>					
The vendor must:					
a) Ensure personalization signals cannot be detected beyond the HSA.	Select		Examine evidence to verify testing was performed showing that contactless personalization signals cannot be detected external to the HSA.	Select	
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.	Select		Examine evidence to verify that testing for personalization signals outside the HSA was performed after the last significant change to the personalization environment. Significant changes include but are not limited to: <ul style="list-style-type: none"> • The introduction of new personalization equipment • Modification of personalization equipment shielding • Structural changes to the HSA perimeter 	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine evidence that encrypted personalization signals comply with the encryption requirements defined in Normative Annex A.	Select	
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.	Select		Examine evidence that manual or automated scans for rogue RF devices are performed at least twice per month.	Select	
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.	Select		Examine evidence to verify personalized contactless cards are stored and handled: <ul style="list-style-type: none"> • As batches of two or more cards, or • Enclosed within protective packaging that restricts reading card emissions 	Select	
3.8 Data Used for Testing					
a) Test (non-production) keys and test (non-production) data cannot be used with production equipment.	Select		Examine documented policies and procedures to verify test keys and test data are restricted from use in production. Observe the location of the test environment to verify that it is separate from production. Interview personnel to verify testing is performed using test keys, data, equipment, and environment.	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Cards used for final system validation or user acceptance that use production keys and/or data must be produced using production equipment.	Select		Examine evidence to verify cards using production keys were produced for final system validation and user-acceptance testing in the production environment using production equipment.	Select	
3.9 Mobile Provisioning Activity Logs					
a) The vendor must maintain an electronic log for both when cards are successfully and unsuccessfully provisioned. The log must be maintained for a minimum of 45 days.	Select		Examine a sample of electronic logs to verify that successful and unsuccessful provisioning activity is logged. Examine evidence that provisioning activity logs are retained for at least 45 days.	Select	
3.10 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.	Select		Examine policies and procedures to verify that there is a decommissioning plan by which assets associated with card production and provisioning activities are secured in the event production activities are discontinued.	Select	
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.	Select		Examine the decommissioning plan to verify it includes the process by which the following items, at a minimum, are secured: <ul style="list-style-type: none"> • Cardholder data • Card design materials • Cryptographic keys • Production hardware • Physical keys 	Select	

Section 3 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine the decommissioning plan to verify that the disposition expectation is defined for each item covered in the plan.	Select	

Section 4: Network Security

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
4.1 Typical Vendor Network <i>The requirements in this section do not apply to vendors that only perform key management or pre-personalization activities on a stand-alone wired system (not connected to any network) and do not perform data preparation or personalization within their facilities. See Appendix B, “Topology Examples,” for network examples.</i>					
Definitions Issuer/Data Source <i>This is the issuer that owns the cardholder data or that sends it to the vendor on behalf of the issuer.</i> Private Network (Leased lines), Internet, POTS <i>Cardholder data is typically sent over these three main types of network to the personalization vendor.</i> Data Preparation Network <i>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.</i> Personalization Network <i>This is the network that contains the card personalization machines.</i>					

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
4.1.1 Card Production and Provisioning DMZ					
a) The DMZ must be dedicated to card production/provisioning activities.	Select		Examine network diagrams and system configurations to verify that a DMZ dedicated to card production/provisioning activities is established.	Select	
b) The card production and provisioning network must be segregated from other parts of an organization's network.	Select		Examine network diagrams and system configurations to verify that card production and provisioning network(s) are segregated from other parts of an organization's network.	Select	
c) All connections to and from the personalization network must be through a system in the DMZ.	Select		Examine network diagram to verify all communication to and from the personalization network is exchanged via a system in the DMZ.	Select	
d) The DMZ must be located in the server room of the HSA.	Select		Observe the system components comprising the DMZ to verify it is located in the server room within the HSA.	Select	
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.	Select		Observe the DMZ system components to verify they are located in dedicated rack(s) capable of restricting individual access. Examine policies and procedures regarding access to the dedicated rack(s) and verify the list of individuals with access is restricted to the minimum number of individuals required for effective operations.	Select	
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.	Select		Observe DMZ switches and cabling to verify they are all stored within the same rack. Observe the DMZ cable connections to verify that only the minimum number of cable connections required to provide connectivity to firewalls are entering/exiting the rack.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
4.1.2 Mobile Provisioning Networks					
a) HCE provisioning must be on its own network, but SE based provisioning is not required to be separated from other personalization networks.	Select		Examine network diagrams to verify that the HCE provisioning system is separated from other personalization network systems. Examine logical configuration settings—e.g., firewall rules—to verify segmentation.	Select	
4.2 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.	Select		Examine network topology diagram to verify it exists, clearly defines the boundaries for all networks, and includes all system components that reside in the HSA.	Select	
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.	Select		Interview network administration personnel to verify the policy and procedures require topology review and update upon making changes to the network and at least annually. Examine evidence that the network topology diagram was reviewed and updated when the network configuration was changed and at least within the last 12 months if there were no changes.	Select	
c) Ensure that the CISO accepts, by formal signature, the security implications of the current network topology.	Select		Examine evidence that the CISO has accepted the security implications of the current network topology and that the document includes his or her formal signature.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Document the flow of cardholder and cloud-based provisioning data within the environment from its receipt/generation to end of its lifecycle. The diagram(s) are kept current and updated as needed upon changes to the environment and must undergo an overall review for accuracy at least every 12 months.	Select		Examine the cardholder and cloud-based provisioning data-flow diagram to verify that cardholder data flows across systems and networks from its receipt/generation to end of its lifecycle. Interview the IT Manager to verify the diagram(s) are kept current and updated as needed and that it undergoes an overall review for accuracy at least every 12 months. .	Select	
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.	Select		Examine network configurations to verify personalization and data-preparation systems are on dedicated network(s) independent of the back office—e.g., through the use of a firewall(s) and not a VLAN between the personalization/data-preparation systems and the back office and Internet-connected networks.	Select	
f) Physically and logically segment systems and applications that make up the cloud-based provisioning network from other vendor networks and Internet-connected networks. For example, in a traditional card vendor environment this could be a separate rack in a server room, or in a provisioning-only entity, housed in a separate room or cage in a data center. It cannot be in the same rack as other servers used for different purposes.	Select		Examine network diagrams and other relevant materials to verify that any cloud-based provisioning network is physically and logically segmented from the broader environment. Observe where the cloud-based provisioning network components are housed to verify they are separate from other vendor networks and Internet-connected networks. For example, they cannot be in the same rack as other servers used for different purposes.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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”.	Select		<p>Examine policies and procedures to verify that:</p> <ul style="list-style-type: none"> Access to the cloud-based and personalization networks is restricted, and unauthorized access is prevented and detected. Access from within the high security area to anything other than the personalization or cloud-based networks is “read-only.” <p>Examine a sample of access rules to verify that access from within the high security area to anything other than the personalization or cloud-based networks is “read-only.”</p>	Select	
h) Be able to immediately assess the impact if any of its critical connecting points are compromised.	Select		Examine documented incident response procedures to verify processes are in place that allow for immediate assessment of the impact of any compromise of critical connecting points.	Select	
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.	Select		<p>Examine system configurations to verify that:</p> <ul style="list-style-type: none"> “Write” permissions to any system external to the personalization network and not in the dedicated DMZ are restricted to only pre-approved functions that have been authorized by the VPA; and “Write” functions do not allow the transmission of cardholder data involving direct writes from the system(s) containing the information. 	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
j) Control at all times the physical connection points leading into the personalization network and cloud-based provisioning network.	Select		Observe physical connection points leading into the personalization network and cloud-based provisioning network to verify they are controlled at all times.	Select	
k) Prevent data from being tampered with or monitored by protecting the network cabling associated with personalization-data movement.	Select		Observe a sample of personalization network cabling to verify that access is restricted, the cabling is protected, and safeguards are in place to avoid tampering.	Select	
l) Transfer required issuer data and keys into the personalization network or the cloud-based provisioning network via a defined and documented process.	Select		Examine procedures to verify they define the process by which issuer data and keys are transferred to the personalization and cloud-based provisioning networks. Interview personnel to verify that the data transfer process conforms to documented procedures.	Select	
m) Ensure a process is in place for updates and patches and identification of their criticality, as detailed in Section 5.3, "Configuration and Patch Management."	Select		Examine documented procedures to verify they include a process for updates and patches that includes identification of their criticality as delineated in the Section 5.3, "Configuration and Patch Management."	Select	
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.	Select		Interview personnel to verify that system-monitoring assets are functional and utilized. Examine evidence to verify that abnormal operations on cloud-based provisioning network systems and on cloud-based provisioning network endpoints can be: <ul style="list-style-type: none"> • Detected, • Isolated, and • Corrected on a real-time and 24/7 basis.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
4.3 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.	Select		Examine documented procedures to verify a process is in place to authorize all changes to network devices and protocols prior to implementation. Examine a sample of change-management logs for network devices and protocols to verify the changes are authorized.	Select	
b) Document the current network device configuration settings, rulesets, and justification for each device.	Select		Examine a sample of network device documentation to verify configuration settings, rulesets, and their justifications are documented. Interview personnel to verify they are familiar with the documentation and process by which the documentation is updated.	Select	
c) Ensure all available services are approved by an authorized security manager.	Select		Interview personnel to identify available services. Examine evidence that available services were approved by an authorized security manager.	Select	
d) Implement logical and physical security controls that protect the integrity of network devices used.	Select		Examine documentation of logical and physical security controls that protect the integrity of network devices used to verify existence. Observe a sample of the controls to verify effective implementation.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Implement mechanisms to effectively monitor the activity on network devices.	Select		Interview personnel to verify mechanisms are defined and implemented to effectively monitor the activity on network devices. Examine policies and procedures to verify mechanisms are defined to effectively monitor the activity on network devices.	Select	
f) Implement patches in compliance with Section 5.3, "Configuration and Patch Management."	Select		Examine a sample of device configurations and verify that patches have been implemented in compliance with Section 5.3.	Select	
g) Maintain an audit trail of all changes and the associated approval.	Select		Examine a sample of change-control logs to verify that an audit trail of changes and associated approvals is maintained.	Select	
h) Implement unique IDs for each administrator.	Select		Examine a sample of administrator IDs and verify that unique IDs are used.	Select	
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.	Select		Examine change-control documentation to verify there is a process for backing up network devices prior to any changes to those devices. Examine procedures for backups and managing backup media to verify media are securely stored and managed. Observe the media storage location to verify it provides a secure storage environment.	Select	
j) Implement a mechanism to ensure that only authorized changes are made to network devices.	Select		Examine network device change logs to verify that changes to network devices were authorized before implementation.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
4.4 Firewalls					
The requirements in this section apply to firewalls protecting the data-preparation and personalization networks.					
4.4.1 General					
The vendor must:					
a) Ensure all documents relating to firewall configurations are stored securely.	Select		Observe the firewall configuration documentation storage area to verify: <ul style="list-style-type: none">• Hard copy and non-digital documentation are stored in locked/secured areas accessible only to authorized personnel.• Digital records are stored in a secure directory with access limited to authorized personnel.	Select	
b) Deploy an external firewall outside the HSA to protect the HSA's DMZ.	Select		Examine network diagrams and other relevant materials to verify that an external firewall outside the HSA is implemented to protect the HSA's DMZ in accordance with acceptable configurations. Examine firewall rules to verify that an external firewall is in place outside the HSA to protect the HSA's DMZ.	Select	
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.	Select		Examine firewall rules to verify the separation via a firewall between the data-preparation network and the personalization network unless both are located within the same high security area or network.	Select	
d) Deploy physically separate firewalls between the external network and the DMZ and between the DMZ and the cloud-based provisioning network.	Select		Examine network diagrams and firewall rules to verify that firewalls are installed between the external network and the DMZ and between the DMZ and the cloud-based provisioning network.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Have the capability to detect, isolate, and correct abnormal operations on network systems on a real-time basis, 24/7, on the external (DMZ) facing firewall.	Select		Examine documentation to verify that abnormal operations on network systems can be: <ul style="list-style-type: none"> • Detected, • Isolated, and • Corrected on a real-time, 24/7, basis. Examine a sample of logs to verify that abnormal operations on network systems are: <ul style="list-style-type: none"> • Detected, • Isolated, and • Corrected on a real-time, 24/7, basis.	Select	
f) Implement appropriate operating-system controls on firewalls.	Select		Examine configurations to verify that appropriate operating-system controls are implemented on firewalls.	Select	
g) Review firewall rule sets and validate supporting business justification either: <ul style="list-style-type: none"> • Monthly, or • Quarterly with review after every firewall configuration change. 	Select		Examine evidence that firewall rule sets have been validated either: <ul style="list-style-type: none"> • Monthly, or • After every firewall configuration change and every 3 months. Examine a sample of firewall rule sets to verify that their business justification is documented.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
h) Restrict physical and logical access to firewalls to only those designated personnel who are authorized to perform firewall or router administration activities.	Select		Observe the firewall/router environment to verify that that physical access to firewalls is limited to only those designated personnel who are authorized to perform administration activities. Examine a sample of access rules to verify logical access is restricted to only those designated personnel who are authorized to perform firewall or router administration activities.	Select	
i) Ensure the firewall rule set is such that any server only requiring inbound connections (for example, web servers) is prohibited from making outbound connections, and vice versa.	Select		Examine firewall rules to verify that firewall and router configurations prohibit making outbound connection when only inbound traffic is expected. Examine firewall rules to verify that firewall and router configurations prohibit incoming connections when only outbound traffic is expected.	Select	
j) Ensure that only authorized individuals can perform firewall administration.	Select		Examine policies and procedures to verify that only authorized individuals can perform firewall administration. Interview personnel to verify firewall administration is restricted to authorized individuals. Examine a sample of access rules to verify that only authorized individuals can perform firewall administration.	Select	
k) Run firewalls and routers on dedicated hardware. All non-firewall-related software such as compilers, editors, and communication software must be deleted or disabled.	Select		Examine documentation to verify that non-firewall related software is deleted or disabled from firewalls and routers. Examine a sample of firewalls and routers to verify they are dedicated hardware from which all non-firewall related software has been deleted or disabled.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
l) Implement daily, automated analysis reports to monitor firewall activity.	Select		Examine evidence that automated tools exist to monitor and analyze firewall activity. Observe a sample of firewall analysis reports to verify that automated analysis is in place and that daily reports are produced.	Select	
m) Use unique administrator passwords for firewalls used by the personalization system as well as those passwords used for other network devices in the facility.	Select		Examine authentication policies and procedures to verify passwords for firewall administration are different than passwords used for other network devices. Interview personnel to verify that unique passwords are established for firewall administration.	Select	
n) Implement both mechanisms to protect firewall and router system logs from tampering, and procedures to check the integrity of the logs monthly.	Select		Examine evidence that firewall and router system logs are protected from modification and a mechanism is in place to check their integrity monthly.	Select	
o) Explicitly permit inbound and outbound traffic to the cloud-based provisioning and personalization networks. A rule must be in place to deny all other traffic.	Select		Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cloud-based provisioning and personalization network. Examine a sample of firewall and router configurations to verify that: <ul style="list-style-type: none"> • Approved inbound and outbound traffic for cloud-based provisioning and personalization networks is explicitly permitted; and • All other inbound and outbound traffic is specifically denied—for example by using an explicit “deny all” or an implicit “deny after allow” statement. 	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
4.4.2 Configuration					
The firewalls must:					
a) Be configured to permit network access to required services only.	Select		Examine policies and procedures for permitting network access to only required services. Examine a sample of system configuration settings to verify that the configurations permit network access to only required services.	Select	
b) Be hardened in accordance with industry best practices, if the firewall is implemented on a commercial off-the-shelf (COTS) operating system.	Select		Examine policies and procedures for hardening firewalls in accordance with industry best practices. Examine a sample of firewall configuration files to verify the configurations are consistent with industry-accepted hardening standards.	Select	
c) Prohibit direct public access between any external networks and any system component that stores cardholder data.	Select		Examine policies and procedures for prohibiting direct public access between any external networks and any system component that stores cardholder data to verify existence. Examine a sample of firewall and router configurations to verify there is no direct access between the Internet and system components that store cardholder data.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Prevent the disclosure of private IP addresses and routing information from internal networks to the Internet by implementing IP masquerading or Network Address Translation (NAT) on the firewall between the DMZ and personalization and the cloud-based provisioning networks.	Select		Examine policies and procedures for implementing IP masquerading or Network Address Translation (NAT) on the firewall between the DMZ and personalization and the cloud-based provisioning networks to verify existence. Examine a sample of firewall and router configurations to verify that methods are in place on the firewall between the DMZ and personalization and the cloud-based provisioning networks to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.	Select	
e) If managed remotely, be managed according to Section 4.6, "Remote Access."	Select		If firewalls are managed remotely, examine policy and procedures documentation to verify management activities are managed according to Section 4.6.	Select	
f) Be configured to deny all services not expressly permitted.	Select		Observe a sample of configuration settings to verify that all services not expressly permitted default to "deny."	Select	
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.	Select		Interview personnel to identify necessary services, protocols, and ports. Examine a sample of systems/networks to verify that unnecessary services are disabled. Examine a sample of services, protocols, and ports to verify that their business justification is documented, and that they were approved by the IT Security Manager.	Select	
h) Disable source routing on the firewall.	Select		Examine a sample of firewall configurations to verify that source routing is disabled.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
i) Notify the administrator in real time of any items requiring immediate attention.	Select		Examine policy and procedures to verify that administrator(s) are to be notified in real time of any items requiring immediate attention. Interview administrators to verify that administrator(s) are notified in real time and that immediate attention is given when required.	Select	
j) Maintain documented baseline security configuration standards for system components based on industry-accepted system hardening standards, which include, but are not limited to: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> User and group access security File and directory security Restricted services System update and installation standards Installed security software 	Select		Examine policies and procedures to verify that a baseline configuration has been established for the organization's system components and addresses at a minimum, but not limited to: <ul style="list-style-type: none"> User and group access security File and directory security Restricted services System update and installation standards Installed security software Interview personnel to verify the baseline configuration standard is based on an industry standard.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
k) The vendor must perform baseline security configurations checks in the cloud- based provisioning environment either: <ul style="list-style-type: none"> • Monthly, or • Quarterly with review after each configuration change. 	Select		Examine evidence to verify that the baseline security configuration was validated either: <ul style="list-style-type: none"> • Monthly, or • Quarterly with review after each configuration change. Examine a sample of baseline configuration checks to verify that they occurred either: <ul style="list-style-type: none"> • Monthly, or • Quarterly with review after each configuration change. 	Select	
4.5 Anti-virus Software or Programs					
The vendor must:					
a) Define, document, and follow procedures to demonstrate: <ul style="list-style-type: none"> • 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 	Select		Examine policies and procedures documentation to verify coverage of: <ul style="list-style-type: none"> • Identification of security alerts—e.g., subscribing to security alerts such as Microsoft and the Computer Emergency Response Team (CERT) • Identification of system component updates that affect the supportability and stability of operating systems, software drivers, and firmware components • Inventory of current systems in the environment including information about installed software components and about running services Interview personnel to ensure procedures are known and followed.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Deploy anti-virus software on all systems potentially affected by malicious software—e.g., personal computers and servers.	Select		Examine a sample of system components potentially affected by malicious software to verify that anti-virus software is deployed.	Select	
c) Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	Select		Examine a sample of system components to verify that: <ul style="list-style-type: none"> • Anti-virus software is present and running. • Activity logs are generated. 	Select	
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.	Select		Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date. Examine a sample of systems to verify that either updates (based upon alerts collected as part of 4.5.a) were applied or documentation exists for why they were not.	Select	
4.6 Remote Access					
<i>For purposes of this section, this applies to remote administration by the vendor, and not issuer connections.</i>					
4.6.1 Connection Conditions					
a) Remote access is permitted only for the administration of the network or system components.	Select		Examine policies and procedures to verify that remote access is permitted only for the administration of the network or system components. Examine a sample of users with remote access to verify such access is permitted only for the administration of the network or system components.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Access from outside the facility to the physical access-control system is not permitted except as used in conjunction with an approved SOC.	Select		Examine a sample of system configurations to verify that remote access is not permitted from outside the facility to the physical access-control system except as used in connection an approved SOC.	Select	
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.	Select		Examine a sample of remote access system configurations and access logs to verify access is accepted only from pre-determined and authorized locations using vendor-approved systems.	Select	
d) Access using personally owned hardware is prohibited.	Select		Examine policies and procedures to verify that remote access using a personally owned device is prohibited. Examine a sample of remote access system configurations and access logs to verify that remote access from personally owned devices is not permitted.	Select	
e) Remote access is not permitted where qualified personnel are temporarily off-site and remote access is a convenience.	Select		Examine policies and procedures to verify that remote access is not permitted when qualified personnel are temporarily off-site.	Select	
f) The remote access process must be fully documented and include at least the following components:			Examine policies and procedures to verify the remote access process is fully documented and includes the following components but is not limited to:		
i. System components for which remote access is permitted	Select		• System components for which remote access is permitted	Select	
ii. The location from which remote access is permitted	Select		• The location from which remote access is permitted	Select	
iii. The conditions under which remote access is acceptable	Select		• The conditions under which remote access is acceptable	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
iv. Users with remote access permission	Select		<ul style="list-style-type: none"> Users with remote access permission 	Select	
v. The access privileges applicable to each authorized user	Select		<ul style="list-style-type: none"> The access privileges applicable to each authorized user 	Select	
g) All access privileges must be validated on a quarterly basis by an authorized individual.	Select		Examine documentation from a sample of reviews to verify that remote access privileges are reviewed at least quarterly by an authorized individual.	Select	
h) Remote access is prohibited to any system where clear-text cardholder data is being processed.	Select		Examine a sample of system configurations to verify that remote access is not permitted to any system where clear-text cardholder data is being processed.	Select	
i) Remote access is prohibited to clear-text cardholder data, clear-text cryptographic keys, or clear-text key components/shares.	Select		Examine remote access policies and procedures to verify that remote access is not permitted to clear-text cardholder data, clear-text cryptographic keys, or clear-text key components/shares.	Select	
j) The vendor must:			Examine policies and procedures to verify the following, at a minimum:		
i. Ensure that systems allowing remote connections accept connections only from preauthorized source systems.	Select		<ul style="list-style-type: none"> Systems allowing remote connections accept connections only from preauthorized source systems. 	Select	
ii. Ensure remote administration is predefined and preauthorized by the vendor.	Select		<ul style="list-style-type: none"> Remote administration is predefined and preauthorized by the vendor. 	Select	
iii. Ensure remote changes comply with change-management requirements as outlined in Section 5.2, "Change Management."	Select		<ul style="list-style-type: none"> Remote changes comply with change-management requirements as outlined in Section 5.2, "Change Management." 	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
iv. Ensure that all remote access locations are included in the facility's compliance assessment and meet these requirements.	Select		<ul style="list-style-type: none"> All remote access locations are included in the facility's compliance assessment and meet these requirements. 	Select	
v. Be able to provide evidence of compliance validation for any remote access location.	Select		<ul style="list-style-type: none"> The vendor is able to provide evidence of compliance validation for any remote access location. 	Select	
k) Ensure that non-vendor staff performing remote administration maintain liability insurance to cover potential losses. All personnel performing remote administration must meet the same pre-screening qualification requirements as card production staff working in high security areas.	Select		<p>Interview a sample of non-vendor staff performing remote administration and verify that they maintain liability insurance to cover potential losses.</p> <p>Examine policies and procedures to verify that personnel performing remote administration must meet the same pre-screening qualification requirements as employees working in high security areas.</p>	Select	
l) All remote access must use a VPN that meets the requirements in the following section.	Select		Examine a sample of remote access to verify that remote access occurs using a VPN that meets the requirements of Section 4.6.2, "Virtual Private Network (VPN)."	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
4.6.2 Virtual Private Network (VPN)					
a) For remote access, VPNs must start from the originating device—e.g., PC or off-the-shelf device specifically designed for secure remote access—and terminate at either the target device or the personalization firewall. If the termination point is the firewall, it must use IPSec or at least a TLS connection in accordance with PCI Data Security Requirement 4.1 to the target device.	Select		Examine VPN system documentation and a sample of configuration settings to verify that: <ul style="list-style-type: none">For remote access, VPNs must start from the originating device and terminate at either the target device or the personalization firewall.When terminating at the personalization firewall, an IPSec or TLS connection to the target device is used in accordance with PCI Data Security Requirement 4.1.	Select	
b) For remote access to DMZ components, the VPN must terminate at the target device.	Select		Examine policy and procedure documentation to verify that it defines that VPN tunnels for remote access to DMZ components must terminate at the target device.	Select	
c) SSL and TLS 1.0/1.1 are expressly prohibited in connection with the aforementioned.	Select		Examine a sample of system configurations to verify that for remote access to DMZ components, SSL and TLS 1.0 are disabled.	Select	
d) Traffic on the VPN must be encrypted using Triple DES with at least double-length keys or Advanced Encryption Standard (AES).	Select		Examine a sample of system configurations to verify that only the listed algorithms are permitted.	Select	
e) Modifications to the VPN must be in compliance with the change-management requirements as outlined in Section 5.2, “Change Management.”	Select		Examine a sample of modifications made to VPN configurations and verify that changes are in compliance with the change-management requirements as outlined in Section 5.2, “Change Management.”	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) Mechanisms—e.g., digital signatures, checksums—must exist to detect unauthorized changes to VPN configuration and change-control settings.	Select		Examine a sample of VPN configuration files and change-control settings to verify they are protected from unauthorized modifications using mechanisms such as digital signatures and checksums.	Select	
g) Multi-factor authentication must be used for all VPN connections.	Select		Examine a sample of VPN system documentation and configuration settings to verify multi-factor authentication is used for VPN connections. Observe a sample of VPN access processes to verify multi-factor authentication is used.	Select	
h) Access must be declined after three consecutive unsuccessful access attempts.	Select		Examine a sample of system component configuration setting to verify that authentication parameters are set to require that user accounts be locked out after not more than three consecutive invalid logon attempts.	Select	
i) Access counters must only be reset by an authorized individual after user validation by another authorized individual.	Select		Examine documentation for access counter resets to verify that it is only reset by an authorized individual after user validation by another authorized individual.	Select	
j) The connection must time out within five minutes if the session is inactive.	Select		Examine a sample of system component configuration settings to verify that system/session idle time-out features have been set to five minutes or less.	Select	
k) Remote access must be logged, and the log must be reviewed weekly for suspicious activity. Evidence of log review must be maintained.	Select		Examine documented procedures to verify remote access logs are reviewed at least weekly to identify suspicious activity and that evidence of log review is retained. Examine a sample of system configurations and audit logs to verify that remote access is logged and logs are reviewed.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
I) VPN traffic using Internet Protocol Security (IPsec) must meet the following additional requirements:			Examine a sample of VPN configuration files to verify that the following requirements, at a minimum, are met:		
i. Tunnel mode must be used except where communication is host-to-host.	Select		• Tunnel mode is used except where communication is host-to-host.	Select	
ii. Aggressive mode must not be used for tunnel establishment.	Select		• Aggressive mode is not to be used for tunnel establishment.	Select	
iii. The device authentication method must use certificates obtained from a trusted Certificate Authority.	Select		• The device authentication method uses certificates obtained from a trusted Certificate Authority.	Select	
iv. Encapsulating Security Payload (ESP) must be used to provide data confidentiality and authentication.	Select		• Encapsulating Security Payload (ESP) is used to provide data confidentiality and authentication.	Select	
v. The Perfect Forward Secrecy (PFS) option of Internet Key Exchange (IKE) must be used to protect against session key compromise.	Select		• The Perfect Forward Secrecy (PFS) option of Internet Key Exchange (IKE) is used to protect against session key compromise.	Select	
4.7 Wireless Networks					
4.7.1 General					
The vendor must:					
a) Implement a documented policy regarding wireless communications and clearly communicate this policy to all card production staff.	Select		Examine usage policies to verify that they address wireless communications. Interview a sample of personnel and validate that the policy is clearly communicated to all card production staff.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Not use wireless communications for the transfer of any personalization data and/or cloud-based provisioning data.	Select		Examine wireless communications policies to verify that wireless communications are prohibited for the transfer of any personalization data and/or cloud-based provisioning data.	Select	
c) Identify, analyze, and document all connections. Analysis must include purpose, risk assessment, and action to be taken.	Select		Examine a sample of connections to verify that connections are identified, analyzed, and documented including purpose, risk assessment, and action to be taken.	Select	
d) Use a wireless intrusion-detection system (WIDS) capable of detecting hidden and spoofed.	Select		Examine output from recent wireless scans to verify that, at a minimum: <ul style="list-style-type: none"> The scan is performed for all wireless networks. Hidden and spoofed networks can be detected. 	Select	
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.	Select		Examine output from recent wireless scans to verify that the WIDS is used to conduct random scans within the HSA at least monthly to detect rogue and hidden wireless networks.	Select	
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.	Select		Examine policies and procedures for resolving any issues identified when unauthorized connections or possible intrusions are detected to verify existence, including that investigations must occur immediately and that resolutions occur in a timely manner. Examine output from recent scan reports and verify that all unauthorized connections or possible intrusions are detected, investigated immediately, and resolved in a timely manner.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine policies and procedures to verify that a scanning device is used for rogue and hidden wireless networks—regardless of whether or not the vendor uses a wireless network—and that random scans of the HSA occur at least monthly. Examine a sample of output from recent scans to verify that the scanning device is used to conduct random scans of the HSA at least monthly.	Select	
4.7.2 Management					
<i>If wireless communication channels are used to transport any non-personalization data within or near the personalization environment, the following requirements apply.</i>					
a) All wireless connections must be authorized by management, with their purpose, content, and authorized users defined and periodically validated.	Select		Examine policies and procedures to verify that wireless connections are authorized by management, with their purpose, content, and authorized users defined and periodically validated. Examine a sample of documentation for wireless connections to verify the connections are authorized by management and periodically validated.	Select	
b) Wireless networks must only be used for the transmission of non-cardholder data—e.g., production control, inventory tracking—and be properly secured. <i>The vendor must have controls in place to ensure that wireless networks cannot be used to access cardholder data.</i>	Select		Examine policies and procedures to verify wireless networks are used for the transmission of non-cardholder data—e.g., production control, inventory tracking—and are properly secured.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) The vendor must deploy a firewall to segregate the wireless network and the wired network.	Select		Examine a network schematic to verify that a firewall is deployed to segregate the wireless network and the wired network. Examine firewall settings and router configurations to verify that a firewall is installed between all wireless networks and the wired network.	Select	
d) All wireless gateways must be protected with firewalls.	Select		Examine a sample of firewall settings and router configurations to verify that wireless gateways are protected with firewalls.	Select	
e) All wireless access points must be configured to prevent remote administration over the wireless network.	Select		Examine documentation to verify wireless access points are configured to prevent remote administration over the wireless network. Examine a sample of system configurations to verify they prevent remote administration over the wireless network.	Select	
f) All wireless traffic must be encrypted with Triple DES or AES and an encryption key of at least 128 bits, using WPA, WPA2, or 802.11x (or an equivalent protocol). WEP encryption must be disabled.	Select		Examine vendor documentation and wireless configuration settings to verify the use of Triple DES or AES and an encryption key of at least 128 bits, using WPA, WPA2, or 802.11x (or an equivalent protocol), and the disablement of WEP encryption.	Select	
g) The service set identifier (SSID) must not be broadcast.	Select		Examine system configuration settings to verify that the service set identifier (SSID) is not broadcast. Observe via a network-detecting device to determine whether SSIDs are being broadcast for any wireless communication channels used to transport any non-personalization data within or near the personalization environment—if yes, then a finding.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine policies and procedures to verify they require that all default security settings for wireless connections are changed upon installation including passwords, SSID, admin passwords, and Simple Network Management Protocol (SNMP) community strings. Examine a sample of system configuration settings to verify that default security settings are not used for wireless connections.	Select	
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.	Select		Examine supporting documentation to verify that the vendor validates any wireless access points that contain flash memory at least once each month to ensure that the firmware contains the authorized software version and appropriate updates. Examine a sample of evidentiary matter to verify that validation of wireless access points that contain flash memory occurs at least once each month to ensure that the firmware contains the authorized software version and appropriate updates.	Select	
j) The vendor must disable the SNMP at all wireless access points.	Select		Examine vendor documentation to verify that SNMP is disabled at all wireless access points. Observe a sample via using the system administrator's help to verify the vendor has disabled SNMP at wireless access points.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
k) Static passwords used to join wireless networks must be compliant with the requirements in Section 6.2, "Password Control," but may be shared with other individuals in the organization on a need-to-know basis.	Select		Examine documented standards and verify that static passwords used to join wireless networks are compliant with the requirements in Section 6.2 and are only shared with other individuals in the organization on a need-to-know basis.	Select	
4.7.3 Additional Requirements for Wi-Fi Standard <i>If the wireless network uses Wi-Fi based on IEEE 802.11, the vendor must ensure that the following requirements are met.</i>					
a) Default SSIDs must be changed upon installation and new passwords must be at least 8 characters.	Select		Examine vendor documentation to verify that default SSIDs are not used and new passwords are at least 8 characters. Observe a sample via using the system administrator's help to verify that default SSIDs have been changed and the new passwords are at least 8 characters.	Select	
b) A log of media access-control addresses and associated devices (including but not limited to make, model, owner, and reason for access) must be maintained, and a check of authorized media access-control addresses on the access point (AP) must be conducted at least quarterly.	Select		Examine a sample of logs of media access-control addresses and associated devices to verify they include at least the make, model, owner, and reason for access. Interview personnel to verify that a check of authorized media access-control addresses on the access point (AP) is conducted at least quarterly. Examine a sample of scan reports and verify that checks of authorized media access-control addresses on the access point (AP) occur at least quarterly.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) A media access control address-based access-control list (ACL) must be used for access control of clients.	Select		Interview responsible personnel to verify the use of ACLs for access control of clients. Examine supporting documentation to verify a media access control address-based access-control list (ACL) is used for access control of clients.	Select	
d) Wi-Fi Protected Access (WPA) must be enabled if the wireless system is WPA-capable.	Select		Examine a sample of configurations and scan reports to verify that, where capable, Wi-Fi Protected Access (WPA) is enabled.	Select	
e) Default passwords on the AP must be changed.	Select		Examine supporting documentation to verify that default passwords on the AP are required to be changed upon installation. Observe a sample via the system administrator's help to verify that default passwords on the AP are changed.	Select	
f) The management feature for the AP must be disabled on the wireless interface and must only be managed via the trusted, wired interface.	Select		Examine configurations and verify that the management feature for the access point is disabled on the wireless interface and can only be managed via the trusted, wired interface.	Select	
g) The AP must be assigned unique Internet protocol (IP) addresses instead of relying on Dynamic Host.	Select		Examine configurations and verify that an access point is assigned unique Internet protocol (IP) addresses instead of relying on Dynamic Host.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
4.8 Security Testing and Monitoring					
4.8.1 Vulnerability					
The vendor must:					
a) Perform quarterly external network vulnerability scans using an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC).	Select		Examine policies and procedures to verify that quarterly external network vulnerability scans using an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC) are required. Examine a sample of external vulnerability scans and verify that quarterly external vulnerability scans occurred in the most recent 12-month period and were completed by a PCI SSC Approved Scanning Vendor (ASV).	Select	
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.	Select		Examine policies and procedures to verify that internal and external network vulnerability scans are required at least quarterly and after any significant change in the network. Examine a sample (including the most recent significant change in the network) of internal and external network vulnerability scans to verify scans occur at least quarterly and after any significant change in the network.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Interview responsible personnel to verify that all findings from network vulnerability scans are prioritized and tracked, and that corrective action for high-priority vulnerabilities is started within two working days. Examine a sample of documentation to verify that findings from network vulnerability scans are prioritized and tracked, and that corrective action for high-priority vulnerabilities is started within two working days.	Select	
d) Retain evidence of successful remediation and make this evidence available during site compliance evaluations upon request.	Select		Interview responsible personnel to verify evidence of successful remediation is retained and available upon request.	Select	
4.8.2 Penetration					
The vendor must:					
a) Perform internal and external penetration tests at least once a year and after any significant infrastructure changes.	Select		Examine policies and procedures to verify that internal and external penetration tests are performed at least once a year and after any significant infrastructure changes. Examine the most recent internal and external penetration tests to verify that the following requirements, at a minimum, were met:	Select	
i. The internal penetration test must not be performed remotely.	Select		<ul style="list-style-type: none"> The internal penetration test was not performed remotely. 	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
ii. Penetration tests must be performed on the network layer and include all personalization network components as well as operating systems.	Select		<ul style="list-style-type: none"> Penetration tests were performed on the network layer and included all personalization network components as well as operating systems. 	Select	
iii. Penetration tests must be performed on the application layer and must include at least the following: <ul style="list-style-type: none"> Injection flaws—e.g., SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. Buffer overflow Insecure cryptographic storage Improper error handling Insecure communications All other discovered “high-risk” network vulnerabilities with criteria for ranking vulnerabilities, including: <ul style="list-style-type: none"> Consideration of the Common Vulnerability Scoring System (CVSS) base score, and/or The classification by the vendor, and/or Type of systems affected. 	Select		<ul style="list-style-type: none"> Penetration tests were performed on the application layer and included at least the following: <ul style="list-style-type: none"> Injection flaws—e.g., SQL injection Buffer overflow Insecure cryptographic storage Improper error handling Insecure communications All other discovered high-risk network vulnerabilities 	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Ensure all findings from penetration tests are prioritized and tracked. Corrective action for high-priority vulnerabilities must be started within two working days.	Select		Interview responsible personnel to verify that all findings from penetration tests are prioritized and tracked, and that corrective action for high-priority vulnerabilities is started within two working days. Examine a sample of documentation to verify that findings from penetration tests are prioritized and tracked, and that corrective action for high-priority vulnerabilities is started within two working days.	Select	
c) Retain evidence of successful remediation and make this evidence available during site compliance evaluations upon request.	Select		Interview responsible personnel to verify evidence of successful remediation is retained and available upon request.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
4.8.3 Intrusion Detection Systems					
The vendor must:					
a) Use intrusion-detection systems (IDS) for network traffic analysis. IDS may be implemented as part of an intrusion-prevention system (IPS) if an IPS is used. These must be deployed, managed, and maintained across the vendor's networks not only for intrusion detection and prevention but also to monitor all data-preparation and personalization network traffic and cloud-based provisioning networks. This includes all traffic generated by machines within the personalization network, including IDS data from within the DMZ. For networks where clear-text PINs traverse, the systems must not be configured to allow capture of clear PIN values.	Select		Examine policies and procedures to verify that intrusion-detection systems are in place to monitor all traffic across the vendor networks, generated by machines within the perimeter, all data-preparation and personalization network traffic, and cloud-based provisioning networks. Examine a sample of system configurations and network diagrams to verify that intrusion-detection systems are in place to monitor all traffic across the vendor networks, generated by machines within the perimeter, all data-preparation and personalization network traffic, and cloud-based provisioning networks. Examine a sample of system configurations to verify that the systems are not configured to allow capture of clear PIN values in networks where clear-text PINs traverse.	Select	
b) Ensure the IDS alerts personnel to suspicious activity in real time.	Select		Interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises in real time. Examine a sample of records to verify the IDS alerts personnel to suspicious activity in real time.	Select	

Section 4 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Ensure the IDS monitors all traffic at the personalization network perimeter as well as at critical points inside the personalization network, such as but not limited to firewalls and public-facing interfaces or servers where cardholder data is decrypted.	Select		<p>Examine system configurations and network diagrams to verify that intrusion-detection systems are in place to monitor all traffic:</p> <ul style="list-style-type: none"> At the perimeter of the personalization network At critical points inside the personalization network 	Select	

Section 5: System Security

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
5.1 General Requirements					
The vendor must:					
a) Document security controls that protect cardholder data and the cloud-based provisioning network.	Select		Examine documentation to identify security controls that protect CHD and the cloud-based provisioning network. Interview personnel to determine that the procedures are known and followed.	Select	
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.	Select		Examine documentation to: <ul style="list-style-type: none">Identify systems and their functions that are used in the personalization process or in the cloud-based provisioning process.Verify that systems and functions are only used to perform their intended function—i.e., control personalization or cloud-based provisioning process activities.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Change supplier-provided default parameters prior to or during installation in the production environment.	Select		Examine configuration settings to verify they are different than what has been published as defaults coming with the product.	Select	
d) Encrypt non-console administrative access when it takes place from within the personalization network.	Select		Examine services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access. Interview personnel and review documentation to identify non-console administrative access in the personalization network and verify that non-console administrative access is encrypted.	Select	
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).	Select		Examine configuration standards and processes—e.g., external time synchronization sources—to verify that time-synchronization technology is implemented and kept current.	Select	
f) Restrict and secure access to system files at all times.	Select		Examine access controls to system files to determine that access is restricted. Observe access attempts for both authorized and unauthorized individuals to verify that access is restricted as documented.	Select	
g) Ensure that virtual systems do not span different network domains.	Select		Examine system-architecture documentation and configuration settings to verify that virtual systems do not span different network domains.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
h) Ensure that all components of the personalization network physically reside within the HSA.	Select		Examine system documentation and architecture diagrams to: <ul style="list-style-type: none"> Identify components that make up the personalization network and HSA. Verify that system components are resident within the HSA. Observe the physical network infrastructure to verify it conforms to the documented network diagram.	Select	
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.	Select		Examine system documentation, including firewall rules and architecture diagrams to verify the PIN printer is: <ul style="list-style-type: none"> Separated from other networks by its own firewall; or Standalone—i.e., the printer and HSM are integrate—; or Directly attached to the HSM. 	Select	
j) Ensure that the access-control system complies with the system security requirements in this document.	Select		Examine documentation and interview personnel to: <ul style="list-style-type: none"> Identify controls associated with the access-control system. Verify controls for the access-control system comply with system security requirements defined in this document. 	Select	
k) Ensure that the access-control system is compliant to Section 6 of this document, “User Management and System Access Control.”	Select		Examine access-control systems documentation to verify that controls are implemented in accordance with Section 6 of this document, “User Management and System Access Control.”	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
5.2 Change Management					
The vendor must:					
a) Ensure that change-control procedures address, at a minimum: <ul style="list-style-type: none">Ensuring that requests for changes are submitted by authorized usersIdentification of components that will be changedDocumentation of impact and back-out proceduresAttestation of successful testing, when requiredMaintenance of an audit trail of all change requestsRecord of whether or not the change was successful	Select		Examine change-control policies and procedures to verify the following are defined: <ul style="list-style-type: none">Ensuring that requests for changes are submitted by authorized usersIdentification of components that will be changedDocumentation of impact and back-out proceduresAttestation of successful testing, when requiredMaintenance of an audit trail of all change requestsRecord of whether or not the change was successful	Select	
b) Ensure that network and system changes follow a documented change-management process, and that the process is validated at least every 12 months.	Select		Examine a sample of changes to network and system components to verify changes follow the documented change-management process. Examine documentation and supporting evidence to verify that the change-management process is validated at least every 12 months.	Select	
c) Ensure all changes are approved by the CISO or authorized individual prior to deployment.	Select		Examine a sample of changes to network and system components to verify changes were approved by the CISO or authorized individual before deployment.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Ensure that the change-management process includes procedures for emergency changes.	Select		Interview personnel and review documentation to verify that the change-management process includes procedures for emergency changes. Examine a sample (if applicable) of emergency changes to verify they followed procedures.	Select	
e) Implement version identification and control for all software and documentation.	Select		Examine documentation to verify the organization's change-management policies and procedures include requirements for version control and identification.	Select	
f) Ensure that the version identification is updated when a change is released or published.	Select		Examine documentation to verify that version identification is updated when a change is released or published.	Select	
g) Implement a controlled process for the transfer of a system from test mode to live mode, and from live mode to test mode.	Select		Examine documentation to verify the existence of a controlled process for the transfer of a system from test mode to live mode, and from live mode to test mode.	Select	
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.	Select		Examine a sample of change-management documentation for system transfers from test to live and from live to test to verify that: <ul style="list-style-type: none"> Both development and production staff sign off on the transfer of a system from test to live, and from live to test; and This sign-off must be witnessed under dual control. 	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
5.3 Configuration and Patch Management					
The vendor must:					
a) Implement a documented procedure to determine whether applicable patches and updates have become available.	Select		Examine documented procedures to verify that they include determination of whether applicable patches and updates have become available.	Select	
b) Make certain a process is implemented to identify and evaluate newly discovered security vulnerabilities and security patches from software vendors.	Select		Examine documentation to verify that processes are defined to identify new security vulnerabilities and obtain security patches from appropriate software vendors.	Select	
c) Ensure that secure configuration standards are established for all system components.	Select		Examine documentation to verify that secure configuration standards are established for all system components.	Select	
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.	Select		Examine configuration standards and verify there are requirements to remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Select	
e) Ensure that the configuration of all system components associated with data transmission, storage, and personalization are validated against the authorized configuration monthly.	Select		Examine documentation to verify all system components associated with data transmission, storage, and personalization are validated against the authorized configuration monthly.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) Ensure all systems used in support of both personalization or cloud-based provisioning networks are actively supported in the form of regular updates.	Select		Examine documentation to verify that all systems used in support of both personalization and cloud-based provisioning networks are actively supported in the form of regular updates.	Select	
g) Evaluate and install the latest security-relevant patches for all system components within 30 days of their release (if they pass validation tests).	Select		Examine a sample of system components and related software to: <ul style="list-style-type: none"> • Compare the list of security patches installed on each system component to the most recent vendor security-patch list; and • Verify the applicable vendor-supplied security patches are installed within 30 days of their release. 	Select	
h) Verify the integrity and quality of the patches before application, including source authenticity.	Select		Examine procedures to verify that a process is defined, the source of the patches is authenticated, and that the quality of the patch is validated before installation. Interview personnel to verify that patch installation process conforms to written procedures.	Select	
i) Make a backup of the system being changed before applying any patches. The backup must be securely stored.	Select		Examine a sample of system components and related software and compare the list of security patches installed against backup file entries to verify backups are performed. Observe security control mechanisms for backups and verify they are in place and active. Interview personnel and review patch update procedures to verify backups are required before applying patches. Identify controls for secure storage.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		<p>Examine policies and procedures related to security-patch installation to verify processes are defined for installation of critical patches to Internet-facing system components within 7 business days of release.</p> <p>Examine a sample of Internet-facing system components and compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify that:</p> <ul style="list-style-type: none"> • Applicable, critical vendor-supplied security patches are installed within 7 days of release. <p>OR</p> <ul style="list-style-type: none"> • Supporting documentation is in place recording that the CISO, IT Security Manager, and IT director understand and accept the risk and ensure implementation occurs within 30 business days. 	Select	
k) Ensure that emergency hardware and software implementations comply with the procedures and validation requirements established for emergency implementations.	Select		<p>Examine the documented procedures for emergency hardware and software implementation.</p> <p>Examine a sample of emergency and hardware and software changes to verify they follow documented procedures.</p>	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
I) Implement a documented procedure to determine whether applicable patches and updates have become available.	Select		Examine a sample of emergency hardware and software implementations to verify that all configuration and patch management procedures are followed. Interview personnel and review documentation to verify that emergency changes followed stated configuration and patch management requirements.	Select	
5.4 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, product logs, and application logs containing security events.	Select		Examine all networks and network devices in the vendor environment—including systems and applications connected to the cloud-based provision network—to ensure that audit logs are enabled and function correctly. Interview personnel to ensure that audit trails are enabled and active for identified items, including operating system logs, security software logs, product logs, and application logs containing security events.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Ensure that audit logs include at least the following components: <ul style="list-style-type: none"> • User identification • Type of event • Valid date and time stamp • Success or failure indication • Origination of the event • Identity or name of the affected data, system component, or resources • Access to audit logs • Changes in access privileges 	Select		Examine the audit logs to ensure they contain the required components.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
<p>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:</p> <ul style="list-style-type: none"> • Immediate (real time) response to threats designated as alerts for high risk associated events • Daily review of IDS and IPS systems • Weekly review for wireless access points and authentication servers • Monthly review for routers • Monthly review of user account audit logs for databases, applications, and operating systems 	Select		<p>Examine policies and procedures to verify that procedures are defined for reviewing and reporting of unusual activity and include requirements for log frequency as stated in the requirement.</p> <p>Examine a sample of each type of log and frequency and obtain evidence that log review was performed. Unless specified by the procedures, the order of assessment is at the discretion of the auditor.</p> <p>Interview personnel to verify the stated policies and procedures are known and followed.</p>	Select	
<p>d) Verify at least once a month that all systems are meeting log requirements.</p>	Select		<p>Examine evidence that demonstrates monthly verification that systems are meeting the logging requirements.</p> <p>Interview personnel to ensure they verify at least monthly that systems are meeting the logging requirements.</p>	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Ensure that logs for all critical and cloud-based provisioning systems are backed up daily, secured, and retained for at least one year. Logs must be accessible for at least three months online and one year offline.	Select		Examine logs for critical and cloud-based provisioning systems to: <ul style="list-style-type: none"> Verify that logs are securely backed up daily. Verify that logs are accessible online for at least three months. Verify that logs are retained offline for one year. For both online and backed-up audit logs, review relevant security controls to ensure access is appropriate.	Select	
f) Protect and maintain the integrity of the audit logs from any form of modification.	Select		Examine relevant security controls for both online and backed-up audit logs to ensure the ability to modify or delete audit logs is prohibited.	Select	
g) Implement a security-incident and event-logging framework for its organization.	Select		Examine documentation to ensure existence of an incident-response process. Interview personnel to verify they are aware of their security-incident and event-logging framework. Examine log entries to verify framework is active and in use.	Select	
5.5 Backup and Recovery for Mobile Provisioning Networks					
a) The backup and recovery procedures for mobile provisioning must be documented.	Select		Examine documentation to verify existence of procedures supporting the backup and recovery of the mobile provisioning network.	Select	
b) The procedures must include the backup and recovery of hardware and software that support the provisioning activity.	Select		Examine documented procedures to verify they include requirements for the backup and recovery of hardware and software that support the provisioning activity.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) The procedures must differentiate between and address short-term and long-term service outages.	Select		Examine documented procedures to verify they include requirements for both short-term and long-term service outages.	Select	
d) The vendor must protect backup copies from intentional or unintentional modifications or destruction.	Select		Examine applicable access-control lists to ensure the ability to modify or delete audit backups is prohibited.	Select	
e) Backups, whether stored within or outside of the HSA, must be encrypted and protected equivalent to the primary data as delineated in Section 3.1, "Classifications."	Select		Interview personnel and review documentation to identify backups and their data classification. Examine documentation about the system used to protect backups to ensure that it is protected equivalent to the primary data—e.g., including the vendor, type of system/process, and the encryption algorithms used to encrypt backups. Examine a sample of backups and verify strong cryptography, with associated key-management processes and procedures where used.	Select	
f) Controls must be established to prohibit creating unauthorized backups.	Select		Examine existing security controls to verify they prohibit the creation of unauthorized backups.	Select	
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.	Select		Interview personnel and review documentation to identify alternate processing sites. Examine documentation to verify that the alternate site has been approved to perform provisioning services before the provisioning occurs.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
5.6 Software Design and Development					
5.6.1 General					
The vendor must:					
a) Document the design, development, and maintenance processes.	Select		Examine documentation of design, development, and maintenance processes to verify existence.	Select	
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.	Select		Examine policies and procedures to verify that: <ul style="list-style-type: none">• The software life cycle process aligns with industry standards; and• Web application development is based on recognized secure coding guidelines.	Select	
c) Document all software components for each system and describe the functionality provided.	Select		Examine documentation to verify it covers software components for each system and describes how they function.	Select	
d) Protect any software backup copies from accidental destruction.	Select		Examine a sample of backups to verify they are adequately protected from accidental destruction.	Select	
5.6.2 Design					
a) The vendor must document the flow of personalization data within the environment from the receipt/generation to end of lifecycle.	Select		Examine data-flow diagrams for personalization data within the environment from the receipt/generation to end of lifecycle. Interview personnel to verify documentation includes information to support the receipt/generation of data to the end of the lifecycle.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
5.6.3 Development					
The vendor must:					
a) Ensure access to source code for applications used on the personalization network is restricted to authorized personnel only.	Select		Interview personnel to identify locations of application source code. Examine system configuration and access control lists to identify users and processes that have access to source code components. Examine approval records to ensure access to source code was authorized.	Select	
b) Ensure that in-house developed personalization software logs any restart (and details associated with that restart event).	Select		Interview personnel to identify in-house developed personalization logs. Examine log configuration settings to verify restart actions are included. Examine a sample of personalization logs to verify restart actions (and details associated with that restart event) are captured.	Select	
c) Ensure that in-house developed personalization software enforces authorization at restart.	Select		Examine restart procedures to ensure in-house developed personalization software enforces authorization at restart.	Select	
d) Ensure separation of duties exists between the staff assigned to the development environment and those assigned to the production environment.	Select		Examine policies and procedures to verify a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. Examine access-control settings to verify that access controls are in place to enforce separation personnel assigned to the development/test environments and the production environment(s).	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		<p>Examine system configuration and access-control lists to identify users and processes that have access to source code components.</p> <p>Examine documented policies and procedures for granting access to source code and verify authorizations and approvals are required.</p> <p>Examine a sample of access request records to verify the access followed the documented process and was authorized.</p>	Select	
5.7 Use of Web Services for Issuer Interfaces					
The vendor must ensure that:					
a) Mutual authentication is required. It must be implemented using either client and server X.509 certificates issued and signed by a trusted Certificate Authority (CA) or a VPN constructed in accordance with Section 4.6.2, "Virtual Private Network."	Select		<p>Examine documentation for web services for issuer interfaces to identify mutual authentication is used.</p> <p>Examine system configurations and settings to ensure X.509 certificates, signed by a trusted Certificate Authority (CA) or VPN, are used.</p> <p>If VPN is used, examine the VPN configuration and settings to ensure they adhere to requirements in Section 4.6.2.</p>	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
<p>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.</p> <ul style="list-style-type: none"> • 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. 	Select		<p>Examine system configuration settings to verify:</p> <ul style="list-style-type: none"> • Strong cryptography is used for the application. • Implementations disallow cipher renegotiation within an established TLS session. • Integrity protection is provided through the use of the SHA-2 or higher algorithm. 	Select	
<p>c) All web service clients and servers that are exposed to untrusted networks are protected by a suitably configured application firewall supporting message validation.</p>	Select		<p>Examine network diagrams and settings to identify interfaces where web services are exposed to untrusted networks—e.g., Internet.</p> <p>Examine network system configurations and review applicable firewall rule sets to verify traffic is restricted and message validation is required.</p>	Select	
<p>d) Implement controls to ensure message integrity.</p>	Select		<p>Examine network documentation to identify controls to support message integrity.</p> <p>Examine network system configurations and review applicable firewall rule sets to verify message integrity is ensured.</p>	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
5.8 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.	Select		Interview personnel to verify a software release process exists and is in use. Examine documentation to verify a quality assurance process is required as part of the software release process and testing of code is performed before software is released. Examine a sample of recent software updates and identify evidence to verify testing of the code was performed.	Select	
b) For internally developed software, ensure that security testing includes verification that temporary code, hard-coded keys, and suspicious code are removed.	Select		Examine policies/procedures to identify testing processes for internally developed software. Examine documentation to verify it addresses removing temporary code, hard-coded keys, and suspicious code. Examine a sample of recent internally developed software updates and verify steps to remove temporary code, hard-coded keys, and suspicious code were performed.	Select	
c) Ensure all software implementation complies with Section 5.2, “Change Management.”	Select		Examine a sample of recent software updates to verify they comply with Section 5.2, “Change Management.”	Select	
d) Test software prior to implementation to ensure correct operation.	Select		Examine a sample of recent software updates and verify evidence exists that testing software prior to implementation was performed.	Select	

Section 5 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Prevent debugging within production environment.	Select		Interview personnel to identify the controls in place to prevent debugging in the production environment. Examine policies/procedures to verify they address prevention of debugging within production environment.	Select	
f) Have a predefined PC device configuration for PC devices used within the HSA.	Select		Examine configuration standards for PC devices used within the HSA. Examine a sample of PC devices used in the HSA and obtain evidence that the devices have been configured according to specified configuration standards.	Select	
g) Implement an approval process for all software beyond the standard PC device configuration for PC devices used within the HSA.	Select		Examine policies/procedures to identify the approval process for software used within the HSA. Examine a sample of recent software updates and verify approvals were required.	Select	
h) Ensure no unauthorized software can be installed.	Select		Interview personnel to identify controls established to prevent unauthorized software from being installed. Examine the implementation of applicable controls to verify they are in place and in use.	Select	
i) Ensure all software is transferred from development to production in accordance with the change-control process.	Select		Examine policies/procedures to identify change-control processes for software, including the methods used to transfer software from development to production. Examine a sample of recent software updates and verify steps to transfer software from development to production were performed.	Select	

Section 6: User Management and System Access Control

Section 6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
6.1 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.	Select		Interview personnel to identify both those authorized to perform, and the processes followed for granting access to vendor's network, applications, and information. Examine documented procedures to ensure they address granting access to vendor's networks, applications, and information. Examine a sample of recent access requests to verify they were processed by authorized personnel and in accordance with documented procedures.	Select	
b) Restrict approval and level of access to staff with a documented business need before access is granted.	Select		Examine policies/procedures to ensure they address that: <ul style="list-style-type: none">Approval and level of access must be restricted to those with a documented business need before access is granted; andDocumented approvals of access in place must be retained while the account is active.	Select	
c) Retain documented approvals while the account is active, at a minimum.	Select		Examine a sample of access requests to verify: <ul style="list-style-type: none">Users obtained associated approvals, andApproval documentation has been retained for all active accounts.	Select	

Section 6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Restrict systems access by unique user ID to only those individuals who have a business need.	Select		Examine a sample of user accounts to verify each individual associated with a unique user ID has a documented, valid business need for the system access.	Select	
e) Incorporate multi-factor authentication for all non-console access into HSA systems for personnel with administrative access.	Select		Interview personnel to verify that multi-factor authentication is used for all non-console access into HSA systems for personnel with administrative access.	Select	
f) Incorporate multi-factor authentication for all remote network access (both user and administrator and including third-party access for support or maintenance) originating from outside the entity's network.	Select		Examine a sample of remote network access system documentation and configuration settings to verify multi-factor authentication is used for remote network access connections. Observe a sample of remote network access processes to verify multi-factor authentication is used.	Select	
g) Only grant individuals the minimum level of access sufficient to perform their duties.	Select		Interview security administration personnel to verify access is granted based on least-privilege principles sufficient to perform their duties. Examine policies/procedures to verify they require that access be granted based on least-privilege principles sufficient to perform their duties. Examine a sample of recent access requests to verify user access is limited to least privilege and based on documented business need.	Select	

Section 6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
h) Make certain that systems authentication requires at least the use of a unique ID and password.	Select		Examine policies/procedures for system access to verify they require at least the use of a unique ID and password. Examine system authentication settings and verify that user IDs in the system are unique and in order to gain access, a password is required.	Select	
i) Restrict administrative access to the minimum number of individuals required for management of the system.	Select		Interview management to understand the minimum number of administrative user resources required to support the personalization environment. Examine user ID lists and security privileges to identify users with administrative access and verify the number of users with administrative aligns with management's expectations.	Select	
j) Ensure that group, shared, and generic accounts and passwords are disabled wherever the system supports unique values.	Select		Examine policies/procedures to verify they require that group, shared, and generic accounts and passwords are disabled wherever the system supports unique values. Examine a sample of system components and user ID lists to verify group, shared, and generic accounts and passwords are disabled.	Select	

Section 6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
k) Ensure that where generic administrative accounts cannot be disabled, these accounts are used only when unique administrator sign-on credentials are not possible and only in an emergency.	Select		Interview system administration personnel to identify existence of generic accounts and how their usage is controlled. Examine policies/procedures for the management of generic administrative accounts that cannot be disabled. Verify these accounts are used only when unique administrator sign-on credentials are not possible and only in an emergency. Examine system security event log to identify when applicable generic administrative accounts were used and verify there is supporting documentation that authorizes their use in an emergency.	Select	
l) Ensure that when generic administrative accounts are used, the password is managed under dual control where no individual has access to the full password. Each component of the password must comply with the password control requirements in Section 6.2 below except for password length when an exception condition exists.	Select		Interview system administration personnel to verify password-management practices require that generic administrative passwords are managed under dual control and in accordance with Section 6.2 Examine policies/procedures for the management of generic administrative account passwords and verify procedures require that such passwords be managed under dual control and in accordance with Section 6.2.	Select	
m) Validate all system access at least quarterly.	Select		Interview personnel to verify system access is re-validated at least quarterly. Examine validation evidence to verify the activity is performed.	Select	

Section 6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
n) Revalidate card production staff access to any systems upon a change of duties.	Select		Interview personnel to verify card production staff access is revalidated when the employee has a change in duties. Examine a sample of HR transfer records and verify that revalidation was performed.	Select	
o) Ensure that access controls enforce segregation of duties.	Select		Interview personnel to identify that policies/procedures support segregation of duties. See glossary definition, "Segregation of Duties," in the Security Requirements.	Select	
p) For cloud-based provisioning, restrict issuer access and privileges to only the issuer's own cardholder data.	Select		Interview personnel and identify controls that restrict issuer access and privileges to only the issuer's own cardholder data. Examine access-control settings to ensure access conforms to stated policies.	Select	
q) Strictly limit privileged or administrative access and ensure such access is approved by both the user's manager and the IT Security Manager.	Select		Interview personnel to identify controls that limit privileged or administrative access. Examine access-control settings to ensure access confirms to stated policies. Examine a sample of administrative-access requests and verify access was approved by the user's manager and IT Security Manager.	Select	
r) Establish management oversight of privileged access to ensure compliance with segregation of duties.	Select		Interview personnel to identify controls that provide oversight of privileged access and compliance with segregation of duties policies. Examine policies/procedures to verify they require oversight of privileged access that ensures compliance with segregation of duties. Examine evidence—e.g., audit logs—to verify management oversight is performed.	Select	

Section 6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
s) Ensure that all privileged administrative access is logged and reviewed weekly.	Select		Examine policies/procedures to verify that they require weekly review of privileged administrative access. Examine evidence—e.g., access logs—to verify reviews are performed according to policies and procedures.	Select	
6.2 Password Control					
6.2.1 General					
The vendor must:					
a) Implement a policy and detailed procedures relating to the generation, use, renewal, and distribution of passwords.	Select		Examine policy and detailed procedures to identify processes for generation, use, renewal, and distribution of passwords.	Select	
b) Implement procedures for handling lost, forgotten, and compromised passwords.	Select		Examine policy and detailed procedures to identify processes for handling lost, forgotten, and compromised passwords. Interview system administrators to validate adherence to procedures.	Select	
c) Distribute password procedures and policies to all users who have access to cardholder data, or any system used as part of the personalization process.	Select		Examine procedures for disseminating password procedures and policies to users with access to cardholder data or any system used as part of the personalization process. Interview a sample of user population to verify password procedures and policies were distributed.	Select	

Section 6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Ensure that only users with administrative privileges can administer other users' passwords.	Select		Examine procedures for managing user IDs and verify that only users with administrative privileges can administer user passwords. Observe a sample of user password resets and verify only users with administrative privileges can perform a reset.	Select	
e) Not store passwords in clear text.	Select		Examine system documentation and configuration settings to verify that passwords are not stored in clear text. Examine a sample of system components and their password files to verify that passwords are unreadable during storage.	Select	
f) Change all default passwords.	Select		Examine a sample of system components and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords. Verify that ALL default passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)	Select	
6.2.2 Characteristics and Usage					
The vendor must ensure that:					
a) Systems are configured so that newly issued and reset passwords are set to a unique value for each user.	Select		Interview personnel to verify newly issued and reset passwords are set to a unique value for each user. Examine a sample of system configuration settings to verify newly issued and reset passwords are set to a unique value for each user.	Select	

Section 6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Newly issued passwords are changed on first use.	Select		Examine system configuration settings to verify newly issued passwords are changed on first use.	Select	
c) "First use" passwords expire if not used within 24 hours of distribution.	Select		Examine system configuration settings to verify that first-time passwords are set to expire if not used within 24 hours.	Select	
d) Systems enforce password lengths of at least 12 characters, with an exception for operating systems that do not support 12 characters. Passwords can never be less than a minimum length of 8 characters or an equivalent strength.	Select		Examine the system configuration settings for a sample of system components to verify that password parameters are set to require a minimum length of at least 12 characters or meet the exception condition.	Select	
e) Passwords consist of using a combination of at least three of the following categories: <ul style="list-style-type: none"> • Upper-case letters • Lower-case letters • Numbers • Special characters 	Select		Examine the system configuration settings for a sample of system components to verify that user passwords are set to require at least three of the following categories: <ul style="list-style-type: none"> • Upper-case letters • Lower-case letters • Numbers • Special characters 	Select	
f) Passwords are not the same as the user ID.	Select		Examine the system configuration settings for a sample of system components to verify passwords cannot be the same as the user ID.	Select	
g) Passwords are not displayed during entry.	Select		Observe authentication procedures for entering a password and verify the password is not displayed as it is entered.	Select	

Section 6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
h) Passwords are encrypted during transmission and rendered unreadable when stored.	Select		Examine password configurations to verify passwords are encrypted during transmission and rendered unreadable when stored. Examine a sample of passwords in transit and in storage to verify password values are not in clear text.	Select	
i) Passwords have a maximum life not to exceed 90 days and a minimum life of at least one day.	Select		Examine the system configuration settings for a sample of system components to verify that user password parameters are set to have a maximum life of not more than 90 days and a minimum life of at least one day.	Select	
j) When updating passwords, the system prevents users from using a password that is the same as one of their previous four passwords.	Select		Examine the system configuration settings for a sample of system components to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.	Select	
k) The user's identity is verified prior to resetting a user password.	Select		Interview system administration personnel to verify the user's identity is verified prior to resetting a user password. Examine password reset procedures to verify the user's identity is verified prior to resetting a user password. Observe a password reset request to verify user identity is verified.	Select	
l) Authentication credentials to the tokenization process are secured to prevent unauthorized disclosure and use.	Select		Interview personnel and review policies/procedures to identify controls that protect authentication credential to the tokenization process.	Select	

Section 6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
6.3 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.	Select		Examine the system configuration settings for a sample of system components to verify that system/session inactivity time out has been set to 15 minutes or less. Observe a user session to verify the user is logged out after 15 minutes, if the system does not permit session locking.	Select	
b) Enforce a manual log-out process where manufacture and personalization equipment does not have the ability to automatically log off a user.	Select		Interview personnel to verify a manual log-out process is defined and in use when mechanisms do not exist to automatically log off a user.	Select	
6.4 Account Locking					
a) Accounts that have been inactive for a specified period (with a maximum of 90 days) must be removed from the system.	Select		Examine user accounts to verify that any inactive accounts over 90 days old are either removed or disabled.	Select	
b) Systems must enforce the locking of a user account after a maximum of six unsuccessful authentication attempts.	Select		Examine the system configuration settings for a sample of system components to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts.	Select	

Section 6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		<p>Examine documented procedures to verify that accounts can only be unlocked by either the security administrator or other authorized individual, or via an automated password reset mechanism.</p> <p>Interview administrators to verify that an account is unlocked only after the identity of the user is verified.</p> <p>Examine policies/procedures for automated password reset mechanisms to verify they require conformance to the stipulated criteria.</p> <p>Observe the mechanism including the challenge/response criteria, for accounts that can be unlocked via an automated reset mechanism, to verify the questions are designed as stipulated in the requirement.</p>	Select	
d) A user's account must be locked immediately upon that user leaving the vendor's employment until it is removed.	Select		<p>Examine policies/procedures to verify that user access is locked when the user leaves the vendor's employment.</p> <p>Examine a record sample of users leaving vendor employment to verify that their account(s) were locked immediately.</p>	Select	
e) A user's account must be locked immediately if that user's password is known or suspected of being compromised.	Select		Examine policies/procedures to verify that any user account is immediately locked if the password is known or suspected of being compromised.	Select	

Section 6 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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: <ul style="list-style-type: none"> • Remote access • Database • Application • OS 	Select		Examine the system configuration settings and audit logs for a sample of system components to verify that lock-out activity is logged. Examine documented procedures to verify access logs are reviewed at least weekly to identify suspicious activity.	Select	

Section 7: Key Management: Secret Data

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
7.1 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.	Select		Examine the written description of the vendor's cryptographic architecture to verify that it includes details of all keys used by each HSM and a description of usage for each key.	Select	
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.	Select		Examine policies/procedures for key management to verify that they require the implementation of dual control and split knowledge for cryptographic key management.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Interview personnel to identify that controls exist beyond procedural controls to prevent any one individual from gaining access to key components or shares sufficient to form the actual key. Examine a sample of evidence to verify controls are in place and functioning to prevent any one individual from gaining access to key components or shares sufficient to form the actual key.	Select	
d) Where clear key components or shares pass through a PC or other equipment, the equipment must never be connected to any network and must be powered down when not in use. These computers must be dedicated and be hardened and managed under dual control at all times.	Select		Examine documented procedures for all key-handling methods to verify that where clear key components or shares pass through a PC or other equipment, the equipment is: <ul style="list-style-type: none"> • Powered off when not in use; • Not connected to any network; • Dedicated and hardened; and • Managed under dual control at all times. 	Select	
e) Keys used for protection of keying material or other sensitive data must meet the minimums delineated in Annex A.	Select		Examine documentation—e.g., cryptography architecture—to identify keys used for the protection of keying material and other sensitive data and to verify the keys adhere to the minimums delineated in Annex A.	Select	
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.	Select		Interview personnel to identify key-encrypting keys used to transmit or convey other cryptographic keys. Examine documentation to verify identified keys are at least as strong as the keys being transmitted or conveyed.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
g) Cryptographic keys must not be hard-coded into software.	Select		Interview personnel to verify that the embedding of cryptographic keys into software—for example, in shell scripts, command files, communication scripts, software code etc.—is strictly prohibited. Examine the software configuration—for example, shell scripts, command files, communication scripts, software code etc.—for a sample of system components to verify that cryptographic keys are not embedded.	Select	
h) Audit trails must be maintained for all key-management activities.	Select		Examine policies and procedures to verify that all key-management activities and all activities involving clear-text key components must be logged. Examine a sample of key-management audit trails to verify existence.	Select	
i) Key-management activities must be performed by vendor or issuer staff.	Select		Examine documented key-management policies and procedures verify that all functions are performed by vendor or issuer staff. Interview responsible personnel to verify that all functions are performed by vendor or issuer staff.	Select	
j) Key-management activities must only be performed by fully trained and authorized personnel.	Select		Examine documented procedures and processes to verify that only authorized personnel have the ability to perform key-management activities. Interview responsible personnel to ensure they have undergone relevant training for the key-management functions they perform.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine documentation to identify digital certificates used in conjunction with cloud-based provisioning products or services. Interview personnel to verify the certificates have been issued either from a trusted Certificate Authority (CA) or directly under an issuer or application provider PKI.	Select	
l) All key-management activities must be documented, and all activities involving clear key components must be logged. The log must include: <ul style="list-style-type: none"> • Unique identification of the individual that performed each function • Date and time • Function • Purpose 	Select		Interview personnel to verify that key-management activities are documented and activities involving clear-text key components are logged, and the logs include: <ul style="list-style-type: none"> • Unique identification of the individual that performed each function • Date and time • Function performed • Purpose Examine a sample of audit logs and other documentation to verify that key-management activities are documented and activities involving clear-text key components are logged, and that the logs include: <ul style="list-style-type: none"> • Unique identification of the individual that performed each function • Date and time • Function performed • Purpose 	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
7.2 Symmetric Keys					
Ensure that:					
a) Symmetric keys only exist in the following forms: <ul style="list-style-type: none">As plaintext inside the protected memory of a secure cryptographic deviceAs a cryptogramAs 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.	Select		Examine documented procedures and system configurations to verify symmetric keys exist only in the following forms: <ul style="list-style-type: none">As plaintext inside the protected memory of a secure cryptographic deviceAs a cryptogramAs 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.	Select	
b) Key components for each specific custodian must be stored in a separate, secure container that is accessible only by the custodian and/or designated backup(s).	Select		Examine a sample of key components and verify for each specific custodian that the keys are stored in a separate, secure container that is only accessible by the custodian and/or designated backup(s). This should include verification of access to physical keys, override keys, and/or PIN codes to access the containers.	Select	
c) No single person shall be able to access or use all components or a quorum of shares of a single secret cryptographic key.	Select		Examine a sample of key components and verify no single person has access to or can use all components or have access to a quorum of shares of a single secret cryptographic key.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
7.3 Asymmetric Keys					
Ensure that:					
a) Private keys exist only in the following forms: <ul style="list-style-type: none">As plaintext inside the protected memory of a secure cryptographic deviceAs a cryptogramAs two or more components or as part of an “m of n” sharing scheme where the value of “m” is at least 2; managed using the principles of dual control and split knowledge	Select		Examine documented procedures to verify private keys exist only in the following forms: <ul style="list-style-type: none">As plaintext inside the protected memory of a secure cryptographic deviceAs a cryptogramAs part of an “m of n” sharing scheme where the value of “m” is at least 2	Select	
b) Key components for each specific custodian must be stored in a separate, secure container that is accessible only by the custodian and/or designated backup(s).	Select		Examine a sample of key components and verify for each specific custodian that key components are stored in a separate, secure container that is accessible only by the custodian and/or designated backup(s).	Select	
c) No single person shall be able to access or use all components or a quorum of shares of a single private cryptographic key.	Select		Examine documented procedures to verify that a single person cannot access or use all components or a quorum of shares of a single private cryptographic key. Interview responsible personnel to verify that the implemented method(s) ensure that no single person can access or use all components or a quorum of shares of a single private cryptographic key.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
<p>d) Public keys must have their authenticity and integrity ensured. In order to ensure authenticity and integrity, a public key must be encrypted, or if in plaintext form, must exist only in one of the following forms:</p> <ul style="list-style-type: none"> • Within a certificate, • Within a PKCS#10, • Within a SCD, or • With a MAC (message authentication code) created using the algorithm defined in ISO 16609. 	Select		<p>Examine documented procedures for public keys to verify that public keys must exist only in one of the following forms:</p> <ul style="list-style-type: none"> • Within a certificate, • Within a PKCS#10, • Within an SCD, or • With an associated MAC (message authentication code) created using the algorithm defined in ISO 16609. <p>Interview responsible personnel to verify that the implemented method(s) ensure the authenticity and integrity of public keys.</p>	Select	
<p>e) Asymmetric keys also adhere to:</p> <ul style="list-style-type: none"> • The payment system requirements for obtaining the issuer certificate • The payment system specification for asymmetric keys 	Select		<p>Examine documentation to identify requirements for obtaining an issuer certificate and the associated payment system(s) specifications.</p> <p>Examine for a sample of asymmetric keys evidence to verify requirements were met.</p>	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
7.4 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.					
7.4.1 General Requirements					
a) The vendor must define procedures for the transfer of key-management roles between individuals.	Select		Examine documented procedures to verify that procedures for transferring key-management roles between individuals are defined. Interview responsible personnel in applicable key-management roles to verify they are aware of and are following the documented procedures.	Select	
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.	Select		Examine documented procedures to verify that access to physical equipment associated with key-management activity is managed such that no single person is able to access or perform key-management functions. Observe the process of accessing physical equipment to verify that dual control is required to access or perform key-management functions.	Select	
7.4.2 Key Manager					
a) There must be a nominated Key Manager with overall responsibility for all activities relating to key management.	Select		Examine documentation to verify the Key Manager has overall responsibility for all activities relating to key management.	Select	
b) CISO must approve the Key Manager for the position within the vendor.	Select		Examine approval authorization documentation to verify CISO (or delegate) approved the Key Manager.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) The Key Manager must:					
i. Have a nominated deputy.	Select		Interview the Key Manager to verify that the Key Manager has a nominated deputy. Examine documentation to identify the nominated deputy for the Key Manager.	Select	
ii. Own and be responsible for ensuring that all key-management activity is fully documented.	Select		Interview the Key Manager to verify that key-management activity is fully documented. Examine documented policies and procedures for appropriateness.	Select	
iii. Be responsible for ensuring that all key-management activity is carried out in accordance with the documented procedures.	Select		Interview the Key Manager to verify that all key-management activity is carried out in accordance with documented procedures.	Select	
iv. In collaboration with the personnel department, vet all key custodians to ensure their suitability for the role.	Select		Examine policies/procedures to identify vetting process for key custodians to ensure they are suitable for their role. Examine documented evidence for a sample of key custodians that supports the vetting process.	Select	
v. Be an employee of the vendor. This also applies to the deputy key manager.	Select		Examine employee rosters for the organization and verify that key custodians and the deputy key manager are employees of the vendor.	Select	
d) The Key Manager must be informed immediately of any security breach or loss of integrity relating to key activities.	Select		Examine policies/procedures to identify process for reporting security breaches or other incidents associated with key activities to ensure the Key Manager is included in the process.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) The Key Manager must be responsible for ensuring that:					
i. All key custodians have been trained with regard to their responsibilities, including incremental changes, and this forms part of their annual security training.	Select		Examine policies/ procedures to verify the requirement for annual security training for key custodians and that it includes key-custodian responsibilities. Examine evidence for a sample of key custodians that verifies annual training is performed.	Select	
ii. Each custodian signs a statement, or is legally bonded, acknowledging that they understand their responsibilities.	Select		Examine a sample of key custodians' signed statements acknowledging that they understand their responsibilities.	Select	
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.	Select		Interview key custodians to verify that they report to a different manager if the custodians together form a threshold to create a key. Interview key custodians to verify that key custodians do not report to the Key Manager if the Key Manager is also a key custodian—because that would form a threshold to create a key. Examine personnel organization charts to verify applicable key custodians report to different managers.	Select	
f) The Key Manager must not have the right to override operations of the key custodians or perform activities for other key custodians.	Select		Interview responsible personnel to verify that Key Managers do not have the right to override operations of the key custodians or perform activities for other key custodians.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
7.4.3 Key Custodians					
a) The roles and responsibilities of key custodians must be fully documented at a level sufficient to allow performance of required activities on a step-by-step basis.	Select		Examine documentation to verify that roles and responsibilities of key custodians are fully documented at a level sufficient to allow performance of required activities on a step-by-step basis. Interview key custodian personnel to verify the documented roles and responsibilities allow performance of required activities on a step-by-step basis.	Select	
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.	Select		Interview personnel to verify that identification of key custodians is based on a need-to-know basis and not identified in general documentation.	Select	
c) The suitability of personnel must be reviewed on an annual basis.	Select		Examine documentation to verify that primary and backup key custodians are reviewed annually for suitability to the role.	Select	
d) The key custodians must be employees of the vendor and never temporary staff or consultants.	Select		Examine documentation to verify that key custodians and their backups are employees of the vendor. Interview a sample of key custodians to verify they are employees of the vendor.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Interview responsible personnel to verify that key custodians are provided with a list of responsibilities for safeguarding key components, shares, or other keying materials entrusted to them. Examine a sample of signed statements for key custodians to verify they acknowledge understanding of their responsibilities for safeguarding key components, shares, or other keying materials entrusted to them.	Select	
f) Only fully trained key custodians and their backups may participate in key-management activities.	Select		Examine policies/ procedures to verify that they require key custodians and their backups are fully trained in key-management activities. Interview key custodians (and backups) to ensure training was required prior to performing key-management activities.	Select	
g) Physical barriers must exist to ensure that no key custodian has access to sufficient components or shares to form the clear key.	Select		Interview personnel to identify the physical barriers that exist to ensure no key custodian has access to sufficient components or shares to form the clear key. Observe physical barriers to ensure they are in place and active.	Select	
7.4.4 Key-Management Device PINs					
<i>In relation to PINs and pass-phrases used with key-management devices:</i>					
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).	Select		Interview personnel to identify secure storage requirements for PIN or pass-phrases. Examine locations where the PIN or pass-phrase is stored and ensure it is stored securely.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Only those individuals needing access to a device must have access to the PIN or pass-phrase for that device.	Select		Interview personnel to ensure that access to the PIN or pass-phrase is limited to only those person(s) needing access to the device.	Select	
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.	Select		Examine policy regarding using PINs and pass-phrases to access key-management devices to verify that the policy includes the length and character-mix of such PINs and pass-phrases, and the frequency of change. Examine a sample of system settings to verify composition rules are enforced and the frequency of PIN/pass phrase change aligns with policy.	Select	
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.	Select		Interview personnel to identify controls to prevent key-management activity under single control. Examine key-management activity audit logs to verify dual control was required for applicable activity.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
7.5 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.	Select		Examine key-management documentation including, where necessary, documentation of the secure cryptographic devices to verify that keys and key components are generated using a random or pseudo-random process described in ISO 9564-1 and ISO 11568-5 that is capable of satisfying the statistical tests of NIST SP 800-22 or equivalent.	Select	
b) Key generation must take place in a hardware security module (HSM) that has achieved PCI approval or FIPS 140-2 or 140-3 Level 3 or higher certification for physical security. <i>During operation, the HSM must utilize a security algorithm that complies with payment system requirements as defined in Annex A.</i>	Select		Interview personnel to verify that: <ul style="list-style-type: none">• Key generation takes place in a secure cryptographic device—e.g., HSM.• The HSM has achieved PCI approval or FIPS 140-2 Level 3 or higher certification for physical security. Examine key-management/device documentation to verify that: <ul style="list-style-type: none">• Key generation takes place in a secure cryptographic device—e.g., HSM.• The HSM has achieved PCI approval or FIPS 140-2 Level 3 or higher certification for physical security.• During key-generation, the HSM utilizes a secure algorithm that complies with Annex A of this document.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Cables must be inspected under dual control to ensure disclosure of a plaintext key or key component or share is not possible.	Select		Examine key-management documentation to verify that procedures are in place to inspect cables under dual control prior to key-management activity, to ensure disclosure of a clear-text key or key component is not possible. Observe personnel performing inspection of cables to verify that procedures are followed.	Select	
d) Use the principles of split knowledge and dual control during the generation of any cryptographic keys in component or share form.	Select		Interview personnel to verify that split knowledge and dual control are required during the generation of any cryptographic keys in component or share form. Examine a sample of key-ceremony records and events to verify that split knowledge and dual control are required during the generation of any cryptographic keys in component or share form.	Select	
e) Key components, if printed, must be created in such a way that the key component cannot be tapped or observed during the process by other than the authorized key custodian. Additionally, the key components cannot be observed on final documents without evidence of tampering.	Select		Interview personnel to verify that any printed key components: <ul style="list-style-type: none"> • Are created in such a way that they cannot be observed in the creation process by anyone other than the authorized key custodian; and • Cannot be observed on final documents without evidence of tampering. Examine procedures to verify that printed key components are created in such a way that the key component cannot be tapped or observed during the process by other than the authorized key custodian and cannot be observed on final documents without evidence of tampering.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) Immediately destroy any residue from the printing or generation process that might disclose a component so that an unauthorized person cannot obtain it.	Select		Examine key-management documentation to verify that any residue from the printing or generation process is immediately destroyed. Interview personnel to verify that procedures are followed.	Select	
g) Ensure that a generated key is not at any time observable or otherwise accessible in plaintext to any person during the generation process.	Select		Interview personnel to verify that any generation of keys is not observable or otherwise accessible in clear text to any other person during the generation process. Observe a key-generation process (live or demonstration if necessary) to verify procedures are followed.	Select	
h) Key components or shares must be placed in pre-serialized, tamper-evident envelopes when not in use by the authorized key custodian.	Select		Interview personnel to verify that key components or shares are placed in pre-serialized, tamper-evident envelopes when not in use by the authorized key custodian. Examine locations of key components or shares not in use by the authorized key custodian to verify they are contained in pre-serialized, tamper-evident envelopes.	Select	
7.5.1 Asymmetric Keys Used for Payment Transactions					
a) Adhere to the public-key algorithm and ensure that the length of issuer RSA key pairs used for payment-transaction processing is in accordance with payment-system requirements.	Select		Examine payment system requirements for public-key algorithms regarding the length of issuer key pairs and the vendor's key-management documentation for consistency.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Ensure that the generation of asymmetric key pairs ensures the secrecy of the private key and the integrity of the public key.	Select		Examine key-management documentation and interview personnel to verify: <ul style="list-style-type: none"> The generation of asymmetric key pairs ensures the secrecy of the private key and the integrity of the public key; and Their creation and management are in compliance with the payment system requirements for obtaining the issuer certificate. 	Select	
c) Create and manage asymmetric keys in compliance with the payment system requirements for obtaining the issuer certificate.	Select		Examine payment system requirements for the creation and management of asymmetric keys and the vendor's key-management documentation for consistency.	Select	
7.6 Key Distribution					
a) Keys must be distributed only in their allowable forms.	Select		Examine key-management documentation to verify that keys are distributed only in their allowable forms in accordance with Sections 7.2, "Symmetric Keys, and 7.3, "Asymmetric Keys."	Select	
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.	Select		Examine key-management documentation to verify that keys and key components or shares are encrypted prior to electronic transmission.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine documentation for conveying key components to verify that the use of different communication channels, such as different courier services and not the same courier on different days, is required. Examine key-management activity audit logs to verify key components were sent according to required procedures.	Select	
ii. A two-part form that identifies the sender and the materials sent must accompany the keying data.	Select		Examine procedures for key generation to ensure a two-part form is used and the form identifies the materials sent. Examine the two-part form to verify that it includes details of the sender and the material sent.	Select	
iii. The form must be signed by the sender and require that the recipient return one part of the form to the originator.	Select		Examine a sample of recently generated key components and verify the forms were adequately signed and returned according to procedures.	Select	
iv. Key components or shares must be placed in pre-serialized, tamper-evident envelopes for shipment.	Select		Examine policies/procedures to verify that key components or shares are placed in pre-serialized TEE bags prior to shipment. Examine a sample of key-management activity logs and verify that pre-serialized numbers are logged as part of the process.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine key-management policies/procedures to verify that inspection of the shipping package received is required and that any signs of tampering require initiation of key-compromise procedures. Interview personnel to verify that procedures are followed.	Select	
ii. Verify the contents of the package with the attached two-part form.	Select		Examine procedures for key-component receipt to verify a two-part form is used and the form identifies the materials sent. Interview personnel to verify that procedures are followed.	Select	
iii. Return one part of the form to the sender of the component or share, acknowledging receipt.	Select		Examine procedures for key-component receipt to verify that one part of the form is returned to the sender of the component or share, acknowledging receipt. Interview personnel to verify that procedures are followed.	Select	
iv. Securely store the component or share according to the vendor's key-storage policy.	Select		Examine procedures for key-component receipt to verify that the component or share is securely stored according to the vendor's key-storage policy. Interview personnel to verify that procedures are followed.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine key-management documentation to verify that prior to certificate acceptance a prearranged method to validate certificate status is in place and includes the valid period of usage and revocation status, if available. Interview personnel to verify that procedures are followed.	Select	

7.7 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 or 140-3 Level 3 or higher certification for physical security.	Select		Examine key-management documentation to verify that any hardware used in the key-loading function is dedicated, controlled, and maintained in a secure environment under dual control. Observe any hardware used in the key-loading function to verify it is dedicated, controlled, and maintained in a secure environment and under dual control. Examine documentation to verify that all newly deployed key-loading devices are SCDs and are either PCI-approved or FIPS 140-2 or 140-3 Level 3 or higher certification for physical security.	Select	
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).	Select		Examine key-management documentation to verify that the target cryptographic devices, cabling, and paper components are inspected for any signs of tampering prior to key loading. Observe personnel performing physical inspections of the target cryptographic devices, cabling, and paper components to verify processes are followed to detect signs of tampering prior to key loading.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Tokens, PROMs, or other key component/share mechanisms used for loading keys (or key components/shares) must only be in the physical possession of the designated custodian (or their backup), and only for the minimum practical time.	Select		Examine key-management documentation to verify that all key/key component/key share-holding mechanisms used for loading keys, key components, or shares are: <ul style="list-style-type: none"> In the physical possession of the designated custodian or their backup, and Only for the minimum practical time. 	Select	
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.	Select		Examine vendor/device documentation to verify that a device used to transfer keys between the cryptographic device that generated the key(s) and the cryptographic devices that will use those key(s), is itself a secure cryptographic device.	Select	
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.	Select		Interview personnel to verify that residual information is not retained after key loading. Observe a key-loading ceremony and verify information is not retained after transferring the keying material.	Select	
e) All key-loading activities must be under the control of the Key Manager.	Select		Examine key-management documentation and interview personnel to verify that all key-loading activities are performed under the control of the Key Manager. Observe key-loading activities to verify that all such activities are under control of the Key Manager.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine key-management documentation to verify that all key/key component/key share-holding device used for key loading are managed under dual control. Observe personnel performing key loading to verify that all key/key component/key share-holding mechanisms are handled under dual control.	Select	
g) Make certain that the key-loading process does not disclose any portion of a key component/share to an unauthorized individual.	Select		Examine key-management documentation to verify that the key-loading process does not disclose any portion of a key component/share to an unauthorized individual. Interview personnel to verify that procedures are followed.	Select	
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.	Select		Examine key-management documentation to verify that any key component/share that is human-readable is only visible: <ul style="list-style-type: none"> • At one point in time to the key custodian, and • For the duration of time required to load the key. Interview personnel to verify that procedures are followed.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		<p>Examine key-management documentation to verify that for all keys or key components/shares loaded:</p> <ul style="list-style-type: none"> • A validation mechanism is in place to ensure authenticity of the keys and key components and provide assurance that the keys and key components have not been tampered with, substituted or compromised; • If check values are used, they are not the full length of the key or key components/shares; • The validation process is performed under dual control; and • The outcome of the validation process is reported to the Key Manager. <p>Observe personnel performing validation processes to verify that they are conducted under dual control and the outcomes are reported to the Key Manager.</p>	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
<p>j) Once a key or its components/shares have been loaded and validated as operational, either:</p> <ul style="list-style-type: none"> Securely destroy or delete it from the key-loading materials as defined in Section 7.11, "Key Destruction"; or Securely store it according to these requirements if preserving the keys or components/shares for future loading. 	Select		<p>Examine key-management documentation to verify that once a key and/or its components/shares have been loaded and validated as operational, the key and/or its components/shares are either:</p> <ul style="list-style-type: none"> Securely destroyed or deleted from the key-loading materials, or If the keys or its components/shares are to be used for future loading, they are securely stored in accordance with requirements in this document. <p>Observe personnel performing process to verify that either secure destruction or deletion, or secure storage of the key and/or its components/shares is performed.</p>	Select	
<p>k) During the key-loading process, key custodians as well as the key manager must verify that the key usage set for the key being loaded matches the keys intended use. This information must be recorded in an audit trail of the key ceremony.</p>	Select		<p>Examine key-management documentation to verify procedures are in place to validate key usage.</p> <p>Examine key ceremony audit logs to ensure they are complete and correct.</p>	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
7.8 Key Storage <i>The following requirements relate to the secure storage of secret keys, private keys, and their plaintext key components or shares.</i>					
a) Key components/shares must be stored in pre-serialized, tamper-evident envelopes in separate, secure locations (such as safes).	Select		Examine key-management documentation and interview personnel to verify: <ul style="list-style-type: none">• Key components/shares are stored in pre-serialized, tamper-evident envelopes;• The envelopes are stored in secure locations (such as safes); and• Removal of the envelopes from their secure location is detectable. Observe the envelopes used to verify that they are pre-serialized and tamper-evident. Observe storage locations to verify the envelopes are stored in separate, secure locations.	Select	
b) These envelopes must not be removable without detection.	Select		Examine key-management documentation and interview personnel to verify removal of the envelopes from their secure location is detectable. Observe storage locations to verify the envelopes cannot be removed without detection.	Select	
c) An inventory of the contents of key storage safes must be maintained and audited quarterly.	Select		Examine key-management documentation and interview personnel to verify that: <ul style="list-style-type: none">• An inventory of the contents of key storage safes is maintained; and• The inventory is audited at least quarterly. Examine inventory and audit documentation to verify inventory is complete and audits are performed at least quarterly.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine key-management documentation for secret or private key component/shares that are stored on a physical media to verify that the key custodian (or designated backup) is the only person allowed possession of both the media and its corresponding access code.	Select	
e) Ensure that access logs, at a minimum, include the following: <ul style="list-style-type: none"> • Date and time (in/out) • Names and signatures of the key custodians involved • Purpose of access • Serial number of envelope (in/out) 	Select		Examine key-management documentation to verify that access logs are maintained. Examine access logs to key component/share storage and verify that they contain: <ul style="list-style-type: none"> • Date and time (in/out) • Names and signatures of the key custodians involved • Purpose of access • Serial number of envelope (in/out) 	Select	
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.	Select		Examine key-management documentation to verify that logs for access and destruction of master keys are retained until at least after all keys protected by those master keys are retired and no longer in circulation.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
7.9 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.	Select		Examine documentation to identify controls that ensure private keys are used only to create digital signatures or perform decryption and that private keys shall not be used to encrypt other keys. Examine evidence that verifies controls are in place and active.	Select	
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.	Select		Examine documentation to identify controls that ensure private keys are used only to create digital signatures or perform decryption; that private keys shall not be used to encrypt other keys; and RSA encryption (public) keys must be prohibited from being used to generate signatures. Examine evidence that verifies controls are in place and active.	Select	
iii. Public keys shall be used only to verify digital signature OR perform encryption operations.	Select		Examine documentation to identify controls that ensure public keys can only be used to verify digital signatures OR perform encryption operations. Examine evidence that verifies controls are in place and active.	Select	
iv. Key-encrypting keys must never be used as working keys (session keys) and vice versa.	Select		Examine policies/procedures to identify controls that KEKs are not used as working keys and vice versa. Examine evidence that verifies controls are in place and functioning.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
b) Key-encipherment keys used to encrypt other keys for conveyance—e.g., KEK, ZCMK—must be unique per established key zone and, optionally, unique per issuer within that zone. These keys must only be shared between the two communicating entities and must not be shared with any third organization.	Select		Examine documentation to verify it requires that transport keys are: <ul style="list-style-type: none"> • Unique per established key zone • Only shared between the two communicating entities Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	
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.	Select		Examine key-management documentation to verify that cryptographic keys are only used for the one, specific purpose for which they were defined. Observe HSM settings and configurations to verify they enforce a separation of keys.	Select	
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.	Select		Examine documented key-management policies and procedures to verify that they require that: <ul style="list-style-type: none"> • All secret and private keys have a predefined expiry date by which they must be retired from use and cannot be used for a period longer than the designated life span of that key. • Issuer-provided keys with a defined expiry date are not used after the issuer-specified expiry date. Observe issuer keys currently in use to verify they are within the issuer-specified expiry date.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) There must be no process by which, once deployed, the life of a key can be extended beyond its original designated life span.	Select		Examine key-management procedures to ensure a key cannot be extended beyond its original designated life span after deployment.	Select	
f) The vendor must:					
i. Prohibit any keys from being shared or substituted between production and test systems.	Select		Examine key-management documentation to verify that keys used for pilots are not used for full product rollout unless the keys were managed to the same level of security compliance as required for production. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	
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.	Select		Examine key-management documentation to verify that keys used for prototyping are not used in production. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine documented procedures to verify procedures require that the life of key-encrypting keys (KEKs) is shorter than the time required to conduct an exhaustive search of the key space. Examine documented procedures to verify procedures require that only the algorithms and key lengths stipulated in Normative Annex A of this document be used. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	
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.	Select		Examine documented procedures to verify that private and secret keys exist in the minimum number of locations consistent with effective system operation. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	
v. Ensure that private and secret keys exist in the minimum number of locations consistent with effective system operation.	Select		Examine documented procedures for generating all types of keys and verify the procedures ensure that only unique keys, or sets of keys, are used, and any key variants exist only within the device with the original key. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
vi. Not use key variants except within the device with the original key.	Select		Examine documented procedures to verify that private keys are only used to decipher or to create a digital signature; and public keys are only used to encipher or to verify a signature.	Select	
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.	Select		<p>Examine documentation of key-inventory control and monitoring procedures to verify all keys are identified and accounted for in the inventory.</p> <p>Examine key inventory records to verify the following details are included:</p> <ul style="list-style-type: none"> • Key label/name • Effective date • Expiration date (if applicable) • Key purpose/type • Key length <p>Interview personnel to verify that key-inventory procedures are known and followed.</p>	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine key-management documentation to verify that all derivation keys are unique per issuer. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	
g) All derivation keys must be unique per issuer.	Select		Examine key-management documentation to verify that all IC keys are unique per IC. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	
h) IC keys must be unique per IC.	Select		Examine key-management documentation to verify that transport keys used for mobile provisioning are unique per device. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
i) Transport keys used for mobile provisioning must be unique per device.	Select		Examine key-management documentation to verify that keys used for pilots are not used for full product rollout unless the keys were managed to the same level of security compliance as required for production. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	
7.10 Key Back-up/Recovery <i>It is not a requirement to have backup copies of key components, shares, or keys. However, if backup copies are used, the requirements below must be met.</i>					
a) Ensure that key back-up and recovery are part of the business recovery/resumption plans of the organization.	Select		Examine documented procedures to verify that key back-up and recovery are part of the business recovery/resumption plans of the organization.	Select	
b) Require a minimum of two authorized individuals to enable the recovery of keys.	Select		Examine documented recovery procedures to verify that recovery of keys requires dual control. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	
c) All relevant policies and procedures that apply to production keys must also apply to backup keys.	Select		Examine documented procedures and backup records to determine whether any backup copies of keys or their components exist. Observe back-up processes to verify backup copies of secret and/or private keys are maintained in accordance with the same requirements as are followed for the production keys.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Vendor must prohibit the loading of backup keys into a failed device until the reason for that failure has been ascertained and the problem has been corrected.	Select		Examine documented to verify the procedures ensure that the loading of backup keys into failed devices is not permitted until after the reason for that failure has been ascertained and the problem has been corrected. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	
e) The back-up of keys must conform to Information Security Policy.	Select		Examine documented procedures to verify that the back-up of keys conforms to the organization's Information Security Policy. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	
f) All access to backup storage locations must be witnessed and logged under dual control.	Select		Examine documented procedures to verify that all access to all backup storage locations is witnessed and logged under dual control. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
7.11 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.	Select		Examine documented procedures to verify processes are in place for destroying keys and their components/shares after successful loading and validation. Examine a sample of key-history logs and key-destruction logs to verify that all key components/shares have been destroyed immediately upon completion of loading. Examine storage locations for key components/shares that have been loaded to verify they are no longer present.	Select	
b) When a cryptographic device—e.g., HSM—is decommissioned, any data stored and any resident cryptographic keys must be deleted or otherwise destroyed.	Select		Interview personnel to verify that all keying material is rendered irrecoverable (for example, zeroized), or that devices are physically destroyed under dual control to prevent the disclosure of any sensitive data or keys. Observe processes for removing cryptographic devices from service to verify that tests and inspections of devices are performed to confirm that keys have been rendered irrecoverable or the devices are physically destroyed.	Select	
c) Securely destroy all copies of keys that are no longer required for card production or provisioning.	Select		Examine documented procedures to verify processes are in place for destroying all copies (including backups) of keys that are no longer required.	Select	
d) All key destruction must be logged, and the log retained for verification.	Select		Examine a sample of key-destruction logs to verify that all copies of keys have been destroyed once the keys are no longer required.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
e) Destroy keys and key components/shares so that it is impossible to recover them by physical or electronic means.	Select		Examine documented procedures for destroying keys and key components/shares and confirm they are sufficient to ensure that no part of the key or component can be recovered. Observe key-destruction processes to verify that no part of the key or component can be recovered.	Select	
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.	Select		Examine documented procedures for removing HSMs from service to verify that if any key within the HSM cannot be destroyed, the device itself is destroyed in a manner that ensures it is irrecoverable. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	
g) Destroy all hard-copy key components/shares maintained on paper by cross-shredding, pulping, or burning. Strip shredding is not sufficient.	Select		Examine documented procedures to verify all hard-copy key components/shares maintained on paper are destroyed by cross-shredding, pulping, or burning—and not by strip shredding. Interview key custodians and key-management supervisory personnel to verify the implementation of the aforementioned.	Select	
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.	Select		Examine documented procedures to verify that keys stored on electronic media are: <ul style="list-style-type: none"> Overwritten with random data a minimum of three times, and/or Destroyed by smashing so they cannot be reassembled. Interview personnel to verify the implementation of the aforementioned.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
i) Destroy all key components under dual presence with appropriate key-destruction affidavits signed by the applicable key custodian.	Select		<p>Examine documented procedures for destroying keys to verify that dual control is implemented and key-destruction affidavits are signed by the applicable key custodian for all key-component destruction processes.</p> <p>Observe a demonstration of processes for removing keys from service to verify that dual control is implemented.</p> <p>Examine a sample of key-destruction logs and verify that the key custodian signs an affidavit as a witness to the key destruction process.</p>	Select	
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.)	Select		<p>Observe the key-destruction process and verify that it is witnessed by a person who is not a key custodian for any component of that key; or</p> <p>Examine a sample of key-destruction logs and verify that a witness who is not a key custodian for any component of the key signs an affidavit as a witness to the key-destruction process.</p>	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
7.12 Key-Management Audit Trail					
a) Key-management logs must contain, at a minimum, for each recorded activity: <ul style="list-style-type: none">• The date and time of the activity took place• The action taken—e.g., whether key generation, key distribution, key destruction• Name and signature of the person performing the action (may be more than one name and signature if split responsibility is involved)• Countersignature of the Key Manager or CISO• Pre-serialized key envelope number, if applicable	Select		Examine key-management logs to verify the following is recorded for each activity: <ul style="list-style-type: none">• The date and time of the activity took place• The action taken—e.g., key generation, key distribution, key destruction• Name and signature of the person performing the action (may be more than one name and signature if split responsibility is involved)• Countersignature of the Key Manager or CISO (or equivalent)• Pre-serialized key envelope number, if applicable	Select	
b) Key-management logs must be retained for at least the life span of the key(s) to which they relate.	Select		Examine documented procedures to verify procedures require key-management logs must be retained for the life span of the key(s) to which they relate. Examine a sample of key-management logs for different types of keys and verify logs are retained for the life span of the key(s) to which they relate.	Select	
c) The vendor must prohibit access to key-management logs by any personnel outside of the Key Manager or authorized individuals.	Select		Examine documented procedures to ensure access to key-management logs is only permitted for the Key Manager or authorized individuals. Observe access to a sample of key-management logs to verify it is only permitted to authorized individuals.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
d) Any facility to reset the sequence number generator or other mechanisms such as time and date stamps in the HSM must be restricted.	Select		Examine documented procedures to ensure procedures restrict access to any capability to reset the sequence number generator or other mechanisms in the HSM. Examine access-control lists or other processes to verify that only authorized personnel have access to the sequence number generator.	Select	
e) The CISO or an authorized individual must investigate all audit log validation failures.	Select		Examine documented procedures to verify the CISO (or equivalent) investigates all audit log validation failures. Interview personnel to verify the implementation of the aforementioned.	Select	
f) During the personalization process, an electronic log must be maintained to identify what keys were used.	Select		Examine documentation to verify an electronic log is maintained to identify keys used during the personalization process. Examine a sample of logs to verify that they track what keys are used during the personalization process.	Select	
g) The vendor must ensure that the deletion of any audit trail is prevented.	Select		Examine documented procedures to verify controls are defined for protecting audit trails from unauthorized deletion. Examine a sample of system configurations to verify controls are implemented to prevent unauthorized deletion of audit trails.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
7.13 Key Compromise					
<i>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.</i>					
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.	Select		Examine documented procedures for key compromise to verify they include who is to be notified; and at a minimum include the CISO (or equivalent), Key Manager, IT Security Manager, and the VPA. Interview personnel to verify that procedures are known and followed.	Select	
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.	Select		Examine documented procedures for key compromise to verify they include the actions to be taken to protect and/or recover system software and/or hardware, symmetric and asymmetric keys, previously generated signatures, and encrypted data. Interview personnel to verify that procedures are known and followed.	Select	
iii. An investigation into the cause of the compromise, including a documented analysis of how and why the event occurred and the damages suffered.	Select		Examine documented procedures for key compromise to verify they include requiring an investigation into the cause of the compromise, including a documented analysis of how and why the event occurred and the damages suffered. Interview personnel to verify that procedures are known and followed.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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).	Select		Examine documented procedures for key compromise to verify they include that the vendor will remove from operational use all compromised keys within a predefined time frame and provide a means of migrating to new key(s). Interview personnel to verify that procedures are known and followed.	Select	
v. Where keys are issuer-owned, the issuer must be notified immediately for further instruction.	Select		Examine documented procedures for key compromise to verify they include that where keys are issuer-owned, the issuer must be notified immediately for further instruction. Interview personnel to verify that procedures are known and followed.	Select	
b) Ensure that the replacement key is not a variant of the compromised key.	Select		Examine documented procedures to ensure replacement keys are not created from a variant of the compromise key. Interview personnel to verify the implementation of the aforementioned.	Select	
c) Where a key compromise is suspected but not yet proven, the Key Manager must have the ability to activate emergency key-replacement procedures.	Select		Examine documented procedures to verify that in the event of a suspected key compromise, the Key Manager has authority to activate emergency key replacement procedures. Interview Key Manager to verify he/she is aware of their responsibility and understand the procedures to activate emergency key-replacement procedures.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine documented procedures to verify they require that in the event of a suspected key compromise, all instances of the key must be immediately revoked pending the outcome of the investigation. Interview personnel to verify that procedures are understood and communicated to affected personnel.	Select	
e) All keys that are encrypted with a key that has been revoked must also be revoked.	Select		Examine documented procedures to verify that all keys encrypted with a key that has been revoked are also revoked. Interview personnel to verify that procedures are understood and communicated to affected personnel.	Select	
f) In the event that a KEK has been compromised, all keys encrypted with the KEK must be replaced.	Select		Examine documented procedures to verify that if a KEK is compromised, the KEK and all keys encrypted with that KEK are replaced. Interview personnel to verify that procedures are understood and communicated to affected personnel.	Select	
g) In the event that a MDK has been compromised, all keys derived from that master key must be replaced.	Select		Examine documented procedures to verify that if a MDK is compromised, the MDK and all keys derived from that MDK are replaced. Interview personnel to verify that procedures are understood and communicated to affected personnel.	Select	
h) The payment system VPA must be notified within 24 hours of a known or suspected compromise.	Select		Examine documented procedures to verify steps include notification of the VPA within 24 hours of a known or suspected compromise.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine documented procedures to verify data items that have been signed with a key that has been revoked are withdrawn as soon as possible and replaced. Interview personnel to verify that procedures are understood and communicated to affected personnel.	Select	
7.14 Key-Management Security Hardware					
a) All key-management activity must be performed using an HSM.	Select		Examine policies/procedures to verify all key-management activity uses an HSM.	Select	
b) When in its normal operational state:					
i. All of the HSM's tamper-resistant mechanisms must be activated.	Select		Examine documented procedures to verify that when the HSM is in its normal operational state, all of the HSM's tamper-resistant mechanisms must be activated. Observe HSMs in normal operational state to verify they are configured according to the documented procedures, and that all of the HSM's tamper-resistant mechanisms are activated.	Select	
ii. All physical keys must be removed.	Select		Examine documented procedures to verify that when the HSM is in its normal operational state, all physical keys must be removed. Observe HSMs in normal operational state to verify they are configured according to the documented procedures, and that all physical keys are removed.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
iii. All unnecessary externally attached devices must be removed (such as an operator terminal).	Select		Examine documented procedures to verify that when the HSM is in its normal operational state, all unnecessary externally attached devices must be removed (such as an operator terminal). Observe HSMs in normal operational state to verify they are configured according to the documented procedures, and that all unnecessary externally attached devices are removed (such as an operator terminal).	Select	
c) HSMs used for key management or otherwise used for the protection of sensitive data must be approved by PCI or certified to FIPS 140-2 or 140-3 Level 3 or higher certification for physical security.	Select		Examine documentation to ensure that all HSMs used for key management or otherwise used for the protection of sensitive data are: <ul style="list-style-type: none"> • Approved by PCI or certified to FIPS 140-2 or 140-3 level 3 or higher. • Listed on the PCI SSC website with a valid PCI SSC listing number, as an Approved PCI PTS Device under the approval class "HSM." • Listed on the NIST Cryptographic Module Validation Program (CMVP) list with a valid listing number and approved to FIPS 140-2 or 140-3 Level 3 (overall), or higher. Refer to http://csrc.nist.gov. 	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine documented procedures to verify that HSMs are not brought into service unless there is assurance that the HSM has not been substituted or subjected to unauthorized modifications or tampering. Interview personnel to verify that HSMs are physically protected up to the point of key insertion or inspection, to provide assurance that the HSM has not been substituted or subjected to unauthorized modifications or tampering.	Select	
e) The process for the installation and commissioning of the HSM must be documented and logged.	Select		Examine documented procedures and logs for HSM installations to verify processes for installation and commissioning of HSMs are documented and logged.	Select	
f) When an HSM is removed from service permanently or for repair, all operational keys must be deleted from the device prior to its removal.	Select		Examine documented procedures for removing HSMs from service to verify that all operational keys are deleted from the device (for example, zeroized) prior to its removal from service. Observe demonstration of processes for removing HSMs from service to verify all operational keys are deleted from the device.	Select	
g) The removal process for the repair or decommissioning of the HSM must be documented and logged.	Select		Examine documented procedures and interview personnel to verify that processes for removal of an HSM for repair or decommissioning must be documented and logged. Observe processes and examine logs for HSM removal to verify processes for removal of an HSM for repair or decommissioning are documented and logged.	Select	

Section 7 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
h) The HSM must be under physical dual control at all times.	Select		<p>Examine documented procedures to verify that HSMs must be under physical dual control at all times when accessed or when in any privileged mode.</p> <p>Interview personnel to verify that procedures are understood and communicated to affected personnel.</p> <p>Examine HSM storage locations and records to ensure they have been managed under dual control after receipt.</p>	Select	

Section 8: Key Management: Confidential Data

Section 8 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
8.1 General Principles					
a) Key-encipherment keys must meet the minimum key sizes as delineated in Normative Annex A.	Select		Examine the documented key hierarchy and verify keys meet the minimum key sizes as delineated in Normative Annex A.	Select	
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.	Select		<p>Examine documented key-management policies and procedures to verify a policy exists that requires key-encrypting keys (KEKs) used to transmit or convey other cryptographic keys be at least as strong as the key being transmitted or conveyed.</p> <p>Examine the documented key hierarchy to verify keys used to transmit or convey other cryptographic keys are at least as strong as the key being transmitted.</p> <p>Observe key-management operations and device configurations to verify that all key-encrypting keys (KEKs) used to transmit or convey other cryptographic keys are at least as strong as the key being transmitted or conveyed.</p>	Select	

Section 8 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
c) Cryptographic keys must not be hard-coded into software.	Select		Examine documented key-management policies and procedures to verify a policy exists that prohibits hard-coded cryptographic in software. Interview personnel to verify that the embedding of cryptographic keys into software (for example, in shell scripts, command files, communication scripts, software code etc.) is strictly prohibited. Examine software configuration files (for example, shell scripts, command files, communication scripts, software code etc.) to verify that cryptographic keys are not embedded.	Select	
d) Audit trails must be maintained for all key-management activities.	Select		Interview personnel to verify audit trails are maintained for all key-management activities. Examine a sample of key-management audit logs to verify their existence and that they address all key-management activities—e.g., generation, conveyance, destruction, etc.	Select	
e) Key-management activities must be performed by vendor or issuer staff.	Select		Interview personnel to verify key-management activities are only performed by authorized personnel. Examine a sample of key-management audit logs to verify key-management activities are only performed by vendor or issuer staff.	Select	

Section 8 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
f) Key-management activities must only be performed by fully trained and authorized personnel.	Select		Examine the vendor's training requirements for individuals involved with key-management activities to verify training program and materials exist. Examine evidence that training has been provided for identified personnel.	Select	
g) The vendor must generate keys and key components using a random or pseudo-random process using one of the following: <ul style="list-style-type: none"> • An approved key-generation function of a PCI-approved HSM • An approved key-generation function of a FIPS 140-2 or 140-3 Level 3 (or higher) for physical security HSM • An approved random number generator that has been certified by an independent qualified laboratory according to <i>NIST SP 800-22</i> 	Select		Examine key-management procedures to verify that it requires that all devices used to generate cryptographic keys meet one of the following: <ul style="list-style-type: none"> • An approved key-generation function of a PCI-approved HSM • An approved key-generation function of a FIPS 140-2 or 140-3 Level 3 (or higher) for physical security HSM An approved random number generator that has been certified by an independent qualified laboratory according to <i>NIST SP 800-22</i> Examine certification letters or technical documentation to verify that all devices used to generate cryptographic keys or key components meet one of the following: <ul style="list-style-type: none"> • An approved key-generation function of a PCI-approved HSM or POI • An approved key-generation function of a FIPS 140-2 or FIPS 140-3 Level 3 (or higher) HSM • An SCD that has an approved random number generator that has been certified by an independent qualified laboratory according to <i>NIST SP 800-22</i> 	Select	

Section 8 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
h) Before the vendor accepts a key, it must ensure that it knows its origin.	Select		Interview personnel to verify that as part of key-acceptance procedures, the vendor knows the key's origin. Observe a demonstration of the key-acceptance process to verify the vendor knows the key's origin.	Select	
i) Keys must be stored in a manner that preserves their integrity.	Select		Observe the storage locations for a sample of keys and verify the storage is adequate to preserve their integrity.	Select	
j) Keys must be used for only one purpose and not shared between cryptographic zones.	Select		Examine documented key-management policies and procedures to verify keys must be used for only one purpose and are not shared between cryptographic zones. Examine a sample of key check values to verify they are unique except by chance.	Select	
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.	Select		Examine key-management policies and procedures to verify secret and private keys require a pre-defined expiry date. Examine a sample of keys to identify key expiry dates and verify that active secret and private keys and issuer keys have not expired.	Select	
l) There must be no process by which, once deployed, the life of a key can be extended beyond its original designated life span.	Select		Examine key-management policies and procedures to verify that they prohibit the life of a key from being extended beyond its original designated life span. Interview personnel to verify that keys are not extended beyond their original designated life span.	Select	

Section 8 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
m) The vendor must prohibit any keys from being shared or substituted between production and test systems.	Select		Interview personnel to identify controls that prohibit keys from being shared between test and production systems. Examine a sample of test and production configuration files to verify the same key check values are not present except by chance in both environments.	Select	
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.	Select		Examine the documented key hierarchy and verify keys meet the minimum key sizes as delineated in Normative Annex A.	Select	
o) The vendor must ensure that keys exist in the minimum number of locations consistent with effective system operation.	Select		Interview personnel to verify it is known that keys may only exist in the minimum number of locations consistent with effective system operation and the vendor is able to identify the locations. Examine a sample of keys to identify storage locations and verify storage is limited to effective system operation.	Select	
p) The vendor must ensure that keys are accessible only to the minimum number of people required for effective operation of the system.	Select		Interview personnel to verify keys are only accessible to the minimum number of people required for effective system operations.	Select	
q) The vendor must have a documented process for handling known or suspected key compromise that includes the revocation of the key.	Select		Examine documented key-management policies and procedures to verify a process is defined for handling known or suspected key compromise that includes the revocation of the key. Interview personnel to verify the policies and procedures are known.	Select	

Section 8 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
r) In the event of the compromise of a key, all instances of the key must be revoked.	Select		Examine documented key-management policies and procedures to verify that in the event of key compromise, steps are defined to ensure all instances of the key are revoked.	Select	
s) All keys that are encrypted with a key that has been revoked must also be revoked.	Select		Examine documented key-management policies and procedures to verify that in the event of key compromise, steps are defined to ensure all keys that are encrypted with a key that has been revoked are also revoked.	Select	
t) In the event that a KEK has been compromised, all keys encrypted with that KEK must be replaced.	Select		Examine documented key-management policies and procedures to verify that in the event of key compromise, steps are defined to ensure all keys that are encrypted with a KEK are replaced.	Select	

Section 9: PIN Distribution via Electronic Methods

Section 9 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
9.1 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.	Select		Examine system documentation and network diagrams to identify process flows and communication channels for the PIN distribution system (PDS) to verify the PDS cannot communicate with any other system where associated cardholder data is stored or processed. Examine interface rules or applicable controls to verify that other systems where cardholder data is stored or processed cannot communicate with the PIN distribution system.	Select	
b) The PIN distribution system must run on a dedicated computer and be isolated from any other network by a dedicated firewall.	Select		Examine system documentation and network diagrams to verify that the PDS runs on a dedicated computer and is isolated from any other network by a dedicated firewall. Examine firewall configurations to verify the PIN distribution system runs on a dedicated computer and is isolated from other networks by a dedicated firewall.	Select	
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.	Select		Interview personnel to identify controls that prohibit functions (other than PIN distribution) from being established during a PIN distribution process. Examine a sample of logs to verify that when a session is established during a distribution—e.g., a telephone call, e-mail, or SMS message—the session is terminated once the PIN has been sent.	Select	

Section 9 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine system documentation and configuration to verify that during transmission to and storage in the PDS, all PIN and authentication values are encrypted using cryptographic algorithms and key sizes in accordance with Annex A.	Select	
e) Communication of the PIN to the cardholder must only take place after verification of the identification value and associated authentication value.	Select		Interview personnel to verify communication of the PIN occurs only after verification of the identification and authentication values. Observe demonstration of a cardholder PIN reset and verify that appropriate verification occurs prior to communicating the PIN.	Select	
f) The identification and authentication values must not disclose the account number.	Select		Examine the identification and authentication values for a sample of PIN distribution requests to verify that account number is not present.	Select	
g) The authentication value must be different than the identification value and must not be a value easily associated with the cardholder.	Select		Examine a sample of PIN distribution requests to verify the authentication value is different than the identification value and is not a value easily associated with the cardholder.	Select	
h) The authentication value must be communicated to the cardholder in such a way that access by anyone other than the cardholder is detected.	Select		Examine evidence for communicating the authentication values to the cardholder to verify they prevent undetected access by anyone other than the cardholder.	Select	

Section 9 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
i) The authentication value must be restricted to the PIN distribution system and not accessible by any other system.	Select		Interview personnel to identify controls that restrict the authentication value to the PIN distribution system. Examine identified controls to verify they restrict the authentication value to the PDS and it is not accessible by any other system.	Select	
j) The PIN must only be distributed in response to the receipt of valid identification and authentication values.	Select		Interview personnel to verify the PIN is only distributed after validation of identification and authentication values. Observe a demonstration of the process to ensure identification and authentication values are validated before the PIN is distributed.	Select	
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.	Select		Examine the documented PIN distribution system process flow to verify the request provides the information necessary to identify the cardholder based upon the identification value and includes the cardholder authentication value. Observe a demonstration of a cardholder request to verify identification and authentication values are present.	Select	
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.	Select		Examine evidence to verify controls are established to prevent the distribution system from associating an identification value or authentication value with a specific cardholder's name, address, or account number. Examine a sample of requests to verify the identification and authentication values do not correlate to a cardholder's name, address, or account number.	Select	

Section 9 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine evidence to verify that a threshold for invalid attempts exists and upon exceeding this limit the PDS alerts the vendor to take further action as defined by the issuer. Examine a sample of invalid attempts—e.g., a system log—where the threshold was exceeded to verify procedures were performed to take action as defined by the issuer.	Select	
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.	Select		Examine system documentation and PIN distribution flows to verify the PIN is only decrypted immediately before being passed to the final distribution channel.	Select	
o) The PIN distribution system must not contain any other cardholder data—e.g., PAN, cardholder name).	Select		Interview system/database administrator to identify the PDS system locations in which cardholder data may exist. Examine a sample of the PIN distribution system data tables or other evidentiary material to verify other cardholder data does not exist.	Select	
p) The association of the PIN to a specific account must not be possible in the distribution system.	Select		Examine documentation to identify the controls established to prevent the association of a PIN to a specific account in the PIN distribution system. Examine a sample of the PIN distribution system tables to verify cardholder data does not exist.	Select	
q) The identification value, PIN, and authentication value must not be logged and must be deleted immediately after successful delivery is confirmed.	Select		Examine a sample of logs to verify the identification value, PIN, and authentication value are not captured and the data elements are deleted immediately after successful delivery is confirmed.	Select	

Section 9 Requirement	Card Vendor Self-Evaluation		Test Procedure	Assessor Compliance Evaluation	
	Comply	Comments		Result	Comment/Non-Compliance Assessment
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.	Select		Examine documentation to identify processes for when the PIN is not delivered to the cardholder to verify that it is deleted from the system after a fixed period of time, as designated by the issuer.	Select	

Annex A – Cryptographic Key Life Cycles – Examples

Key Name *	Algorithm	Key Length (HEX)	Purpose of Use	Generation	Distribution	Storage	HSMs	Loading	Destruction	Update
ZMK	2TDES	112	Encrypts keys during transmission between two entities. ZMK key types include: ZMK Bank encrypts keys (PEK, MDK, dCVV) between the issuer and <i>vendor</i> . ZMK <i>vendor</i> encrypts keys (KMC) used to lock the chip between pre-personalizer and personalizer.	The third party entity Bank or <i>vendor</i>	Bank brings ZMK components on site. <i>Vendor</i> ZMK sent in three paper based components.	Inside HSM	Affina PSG	3 Key Custodians 1 KM Head of CPC For ZMK Bank 3 bank personnel also present	Cross-shredded	Not planned
PEK	2TDES	112	Encrypts PIN Block between Issuer and <i>vendor</i> .	Issuer	Encrypted under ZMK Bank.	Inside HSM	Affina PSG	1 Key Custodian 1 KM Head of CPC	Not planned	Not planned
MDK	2TDES	112	Issuer Master Application Keys, derivatives of which are for Authentication, Secure Messaging Integrity and Secure Messaging Confidentiality.	Issuer	Encrypted under ZMK Bank.	Inside HSM	Affina PSG	1 Key Custodian 1 KM Head of CPC	Not planned	Not planned
dCVV	2TDES	112	Master Key, derivatives of which are used in contactless application to create a dynamic CVV.	Issuer	Encrypted under ZMK Bank.	Inside HSM	Affina PSG	1 Key Custodian 1 KM Head of CPC	Not planned	Not planned
KMC	2TDES	112	Locks chips between card manufacturer and <i>vendor</i> .	Chip vendor	Encrypted under ZMK Bank.	Inside HSM	Affina PSG	1 Key Custodian 1 KM Head of CPC	Not planned	Not planned

Key Name *	Algorithm	Key Length (HEX)	Purpose of Use	Generation	Distribution	Storage	HSMs	Loading	Destruction	Update
ISK/IPK	RSA	1152/ 1408	RSA Keys ISK is used to create ICC Certificate. IPK is placed on the card in Certificate format.	Vendor	IPK sent to Visa in self-signed format.	Inside HSM	Affina PSG	1 Key Custodian 1 KM Head of CPC	As per procedures.	Depends on Scheme Key Expiry dates.
ICCK	RSA	1152	DDA keys. ICSK is personalized in chip. ICPK is placed on the card in Certificate format. If separate PIN encipherment key required—also generated.	Vendor	Not distributed, coded on chip card.	Not stored	Affina PSG	Automated	N/A	N/A
LMK	3DES	32	Local Master Key Used to encrypt keys in database.	Generated on SafeNet PSG HSM.	Not distributed.	In memory of HSM and as 3 paper-based components.	SafeNet PSG	Loaded by 3 Key Custodians.	Deletion from the memory of the HSM Physical destruction in cross cut shredder	Not Confirmed
ZMK	3DES	32	Zone Master Key Shared between a third party and <i>vendor</i> .	Generated on SafeNet PSG HSM or by third party.	3 paper-based components sent via different couriers.	In memory of HSM and as paper based components.	SafeNet PSG	Loaded by 3 Key Custodians.	Deletion from the memory of the HSM Physical destruction in cross cut shredder	Annually
KEK/ KTK	3DES	32	Key-Encryption Key / Key-Transport Key Shared between internal cryptographic zones.	Generated on SafeNet PSG HSM by key custodian.	3 paper-based components used internally by the custodians.	In memory of HSM and as paper based components.	SafeNet PSG / Thales	Loaded by 3 Key Custodians.	Deletion from the memory of the HSM Physical destruction in cross cut shredder	Not Confirmed

Key Name *	Algorithm	Key Length (HEX)	Purpose of Use	Generation	Distribution	Storage	HSMs	Loading	Destruction	Update
MPK	3DES	32	Master Personalization Key Used by the card supplier to lock the chips.	Generated by the chip producer and distributed as a cryptogram.	Distributed only as a cryptogram protected under a zone master key.	As cryptogram in protected memory of HSM.	SafeNet PSG	Translated from under ZMK	Deletion from the memory of the HSM Physical destruction in cross cut shredder	Per batch of chips
MDK	3DES	32	Master Derivation Key Used by the data preparation system to generate the UDKs.	Generated by the issuer.	Ciphered with a ZMK.	As cryptogram in protected memory of HSM.	SafeNet PSG	Translated from under ZMK	Deletion from the memory of the HSM Physical destruction in cross cut shredder	On request of issuer