Payment Card Industry (PCI)
Card Production Security Requirements

Technical FAQs for use with Version 1.0

December 2013

Table of Contents

Logical Security Requirements

These technical FAQs provide answers to questions regarding the application of the *Payment Card Industry (PCI) Logical Security Requirements.* These FAQs provide additional and timely clarifications to the application of the Security Requirements. The FAQs are an integral part of those requirements and shall be fully considered during the evaluation process.

Updates: New questions or those modified for clarity are shown in **red**.

General Questions

No FAQ in this section – Reserved for future use.

Section 1 – Scope

No FAQ in this section – Reserved for future use.

Section 2 – Roles and Responsibilities

No FAQ in this section – Reserved for future use.

Section 3 – Security Policy and Responsibilities

No FAQ in this section – Reserved for future use.

Section 4 – Data Security

4.1.2 Confidential Data

4.1.2.a Confidential data is data restricted to authorized individuals. This includes cardholder data and the keys used to encrypt cardholder data. These are confidential data and must be managed in accordance with Section 9 of this document, "Key Management: Confidential Data."

Q 1 **December 2013 – Confidential data is defined to include PAN, expiry date, service code, and cardholder name. Does this apply to all these data elements individually or in any combination?**

A *The PAN must always be considered confidential, and the other three data elements are considered confidential if stored or otherwise available in conjunction with the PAN.*

Section 5 – Network Security

5.6.1 Remote Access / Connection Conditions

5.6.1.j The vendor must ensure that all remote access locations are included in the facility's compliance assessment and meet these requirements.

Q 2 July 2013 – Remote access is permitted only for administration of the network or system components and is not permitted to any system where clear-text cardholder data is being processed. If system administration is handled remotely by the card vendor or outsourced to a third party, are they still subject to the criteria defined within the Remote Access Section?

A *Yes, administration of the network and system components is a critical activity that requires a secure environment that complies with the defined security requirements and is audited for compliance.*

5.6.2 Virtual Private Network (VPN)

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

Q 3 December 2013 – Section 5.6.2 stipulates criteria that VPNs must meet. Under what circumstances does this criteria apply, and is there differentiation between mobile VPNs and site-to-site VPNs?

A The VPN requirements are part of the Remote Access requirements in Section 5.6. Therefore, they apply to the remote administration of networks and system components that comprise the HSA and do not apply to VPNs that are used for other purposes. For example, the VPN requirements apply to administration of the personalization network and do not apply to VPNs used for conveyance of issuer data to the card vendor.

Section 6 – System Security

6.1 General Requirements

6.1.f The vendor must ensure that virtual systems do not span different network domains.

Q 4 December 2013 – For purposes of this requirement, how are network domains defined for what is allowed or not allowed?

A *In a virtualized environment, activities involving data preparation and personalization can use the same equipment. However, you cannot use the same equipment for systems in the DMZ and data-preparation or personalization area. This is because data preparation and personalization must occur within the HSA, whereas other activities must occur outside the HSA.*

6.3 Configuration and Patch Management

6.3.j The vendor must implement critical patches within two business days. When this is not possible the CISO, 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 seven business days.

Q 5 December 2013 – Is there any dispensation from this requirement?

A *This requirement is under revision. Meanwhile, the need to patch within seven business days applies to all Internet-facing system components. Otherwise the maximum is thirty days, and still requires the proper sign-offs.*

Section 7 – User Management and System Access Controls

7.2.2 Password – Characteristics and Usage

7.2.2.c The vendor must ensure "first use" passwords expire if not used within 24 hours of distribution.

Q 6 December 2013 – Some systems are not capable of expiring passwords within 24 hours as required by 7.2.2.c. What alternatives are available?

A *If a system cannot expire initial passwords that are not used within 24 hours of distribution, then the passwords must not be issued more than 24 hours before expected use. If 24 hours elapses without use, they must be manually expired within that 24-hour period.*

7.4 Account Locking

7.4.c Locked accounts must only be unlocked by the security administrator.

Q 7 December 2013 – Are other mechanisms available to meet this requirement?

A *This requirement is under revision. Meanwhile, user accounts can also 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 in the Human Resources Department.*

Section 8 – Key Management: Secret Data

8.6 Key Distribution

8.6.d Key components or shares must only be received by the authorized custodian, who must inspect and ensure that no one has tampered with the shipping package.

Q 8 December 2013 – Are there any alternatives to meet this requirement for when the authorized custodian is unavailable?

A *Yes, if the primary custodian is unavailable, a pre-designated and authorized backup custodian can receive the package. Alternatively, drop boxes can be used for the courier to leave the package in a locked container that is only accessible by the primary and backup custodians.*

8.9 Key Usage

8.9.b Transport keys used to encrypt other keys for conveyance (e.g., KEK, ZCMK) must be unique per established key zone and, optionally, unique per issuer within that zone. These keys must only be shared between the two communicating entities and must not be shared with any third organization.

Q 9 July 2013 – Can the same transport keys be used between the card vendor and separate locations of another organization?

A *No, each location would constitute a separate key zone and therefore different transport keys must be used. The same is true for a card vendor with multiple locations communicating to one or more locations of another organizational entity.*

8.9.g IC keys must be unique per IC.

Q 10 December 2013 – Does 8.9.g apply to all IC keys?

A *No, it does not apply to manufacturer or founder keys. It does apply to other keys such as those used for pre-personalization.*

Section 9 – Key Management: Confidential Data

No FAQ in this section – Reserved for future use.

Section 10 – PIN Distribution via Electronic Methods

No FAQ in this section – Reserved for future use.

Physical Security Requirements

These technical FAQs provide answers to questions regarding the *Payment Card Industry (PCI) Card Production Physical Security Requirements.* These FAQs provide additional and timely clarifications to the application of the Security Requirements. The FAQs are an integral part of those requirements and shall be fully considered during the evaluation process.

Updates: New or questions modified for clarity are in **red.**

General Questions

No FAQ in this section – Reserved for future use.

Section 2 – Personnel

2.1.3.1 Employment Application Forms

2.1.3.1.b The vendor must maintain a personnel file for each employee that includes but is not limited to the following information:

- *Gathered as part of the hiring process:*
  - *Background check results*
  - *Verification of aliases (when applicable)*
  - *List of previous employers and referral follow-up results*
  - *Education history*
  - *Social security number or appropriate national identification number*
  - *Signed document confirming that the employee has read and understands the vendor's security policies and procedures*
  - *Fingerprints and results of search against national and regional criminal records*
- *Gathered as part of the hiring process and periodically thereafter:*
  - *Current photograph, updated at least every three years*
  - *Record of any arrests or convictions, updated annually*
  - *Annual credit checks*

Q 1 **December 2013 – Drug testing is not required in the *PCI Card Production Security Requirements.* Is this an oversight?**

A *No, PCI does not require drug testing due to the wide variances in country laws governing where or when drug testing is allowed. However, that does not preclude card vendors from requiring drug testing wherever and whenever they deem necessary.*

Q 2 **July 2013 – Requirement 2.1.3.1 requires annual credit checks. In some countries, only a small fraction of the employees have ever had a credit transaction, so the local credit bureau does not have any record of them. What should happen in these cases?**

A *The intent of the requirement is to determine whether the person is under any financial duress that should be considered for their employment. Even if the credit check is expected to not show anything, it still must be attempted. If the person does not have a credit history, the vendor should apply alternative procedures as the vendor deems appropriate in order to fulfill the intent of this requirement.*

2.4.1 External Service Providers – General Guidelines

2.4.1.a The vendor must ensure that the requirements of Section 2.1, "Employees," of this document have been met by the employer of all suppliers, repair and maintenance staff, and any other external service provider.

Q 3 **December 2013 – Requirement 2.4.1 states that all third-party service providers (for example, suppliers, repair and maintenance staff, and any other external service providers) must meet the same requirements as employees of the card vendor who have access to card products, components, and the high security area (HSA). This includes pre-employment testing, screening, training, termination checks, etc. Does the card vendor have to directly conduct these reviews?**

A *No. The intent of this objective is to ensure that service provider employees with access to the HSA conform to the same employment screening criteria as staff employed by the vendor. As noted in Requirement 2.4.1, the employer of these third-party service providers should conduct the necessary reviews. The card vendor meets this requirement by either directly performing the review or by contractually obligating the third-party external service provider to conduct these reviews.*

Section 3 – Premises

3.3.2.2 Security Control Room / Location and Security Protection

3.3.2.2.q The vendor must cover all security control room windows with a one-way mirror film or other material preventing viewing from outside.

Q 4 **December 2013: Are any methods of covering security control room windows allowed, other than those described in 3.3.2.2.q?**

A *Yes. Other mechanisms may be used as long as they achieve the same result of preventing observation to inside the security control room to view the security equipment—e.g., CCTV images.*

3.3.3.1 High Security Areas (HSAs) / Definition

3.3.1.d If these HSAs are within the same building, they must be contiguous.

Q 5 **December 2013 – Areas in production facilities where card products, components, or data are stored or processed are called high security areas. Section 3.3.3 states that these HSAs must be contiguous if they are within the same building. In some building designs these areas are non-contiguous and retrofitting is prohibitively expensive. Are there any other options?**

A *Yes. HSAs in the same building that are not contiguous may exist provided they are treated physically and logically as separate facilities—i.e., use of secure physical transport and encryption of sensitive data.*

3.3.4.1 HSA / Access Control

3.3.4.1.e The HSA and all separate rooms within the HSA must be protected by internal motion detectors.

Q 6 **December 2013 – Does this requirement apply to chemical storage areas, cleaner cupboards, and other maintenance/supplies storage?**

A *A space within the HSA may be defined as a cupboard or similar which does not require motion detection if it is not possible for an individual to walk into the space and no longer be visible.*

3.3.5 HSA Rooms

3.3.5.a Separate rooms within the HSA must meet all of the above requirements with the exception of person-by-person access.

Q 7 **July 2013 – Requirement 3.3.4 specifies controls that must be applied to all rooms within the High Security Area (HSA), and Requirement 3.3.5 specifies the following as rooms that may exist within the HSA as:**

- **Pre-Press Room**
- **Work in Progress (WIP) Storage Room**
- **Sheet Destruction and Card Destruction Room(s)**
- **PIN Mailer Production Room**
- **Server Room & Key Management Room**

Do the controls specified apply to other rooms within the HSA?

A *Yes, they apply to all rooms in the HSA. Non-compliant rooms must be either closed off or reconfigured to no longer be separate rooms.*

Q 8 **December 2013: Local regulations or other safety considerations may require the presence of fire doors in the HSA. Are there any special considerations?**

A *Yes. If the HSA contains fire doors and these doors are normally closed or can be manually closed, these doors are subject to the same access controls as any other door that provides access to a room.*

If the HSA contains fire doors and these doors are locked open and only closed automatically when a fire alarm is activated, the access controls that normally apply for accessing a room do not apply.

Q 9 **December 2013 – Separate rooms within the HSA must meet all of the requirements in Section 3.3.4, with the exception of person-by-person access. If a room cannot or will not be made to meet these requirements, what options exist?**

A *The card vendor has three options:*

- *Close off the room from accessibility to anyone with HSA access.*
- *Reconfigure smaller rooms into a larger room meeting the requirements.*
- *Convert non-compliant rooms into spaces within a HSA that are no longer fully enclosed—e.g., by removing doors.*

Note that where person-by-person access is not required, anti-passbook is still required.

Q 10 December 2013 – For purposes of 3.3.4, do elevators, stairwells, closets and glass-enclosed rooms (e.g., conference rooms or other room type) constitute a room?

A *If an elevator has a door, access to it must be controlled. Stairwells are not a room if they do not have doors. Closets would not be considered a room if a person could not physically enter. However, a storage room with a door is considered a room. Glass-enclosed rooms are also considered rooms for purposes of this requirement.*

3.3.5.b Toilet rooms are prohibited except where required by local law. Where used, the entry/exit way must be camera-monitored.

Q 11 December (update) 2013 –What is the rationale for Requirement 3.3.5.b?

A *The intent is to prevent any single individual being unobserved while within any room within the HSA. This is not a new requirement and was in place under the prior individual payment brand requirements so there should be limited impact on card vendors previously held to payment brand criteria. Toilet rooms that are not fully enclosed and are accessible without opening the door (i.e., sufficient space exists above and/or below the enclosure to access the area) are not subject to this requirement.*

3.4.5.4 Retention of Video Recordings

3.4.5.4.b The backup recording must be stored in a separate, secure location within the facility and must ensure segregation of duties between the users and administrators of the system.

Q 12 December 2013 – Are backups required to be stored in the same facility as the primary copies to meet Requirement 3.4.5.4.b?

A *This requirement is under revision. Meanwhile, backups may be stored in other facilities via techniques such as disk mirroring, provided the storage is secure in accordance with these requirements.*

Q 13 December 2013 – Does the use of RAID technology meet the criteria for separate backup recordings?

A *No. RAID technology is a storage technique that divides and replicates data among multiple physical drive in order to provide reliability, availability, performance and capacity. It is not a mechanism for backing up data.*

Section 4 – Production Procedures and Audit Trails

4.5.1.2 Core Sheets / Partially or Fully Printed Sheets

4.5.1.2.b Audit or accountability forms for core sheets must provide the following information for every order processed:

- *Good sheets*
- *Rejected sheets*
- *Set-up sheets*
- *Quality control sheets*
- *Unused core sheets*

Q 14 December 2013 – Does this requirement apply to core sheets used at the facility?

A *It applies only to sheets printed with the payment system brand or issuer design and not to blank sheets.*

4.7.1 Audit Controls – Manufacturing / General

4.7.1.c An effective audit trail is comprised of a series of audit logs that must contain but are not limited to the following information:

- *Description of the component or card product(s) being transferred*
- *Name and signature of the individual releasing the component or card product(s)*
- *Name and signature of the individual receiving the component or card product(s)*
- *Number of components or card products transferred*
- *Number of components used*
- *Number returned to vault or WIP storage*
- *Number rejected or damaged*
- *Number to be destroyed*
- *Date and time of transfer*
- *Name and signature of supervisor*
- *Signatures of persons inventorying components*

Q 15 December 2013 – Audit controls for manufacturing include tracking the number returned to the vault or WIP storage. Does this require that finished products that are already packed in containers or cartons prior to shipment be recounted before storage in the vault or WIP storage?

A *Finished products that have been previously counted in a controlled manner and sealed in tamper-evident packaging do not require recounting; however, they must still be part of the audit trail log.*

4.7.3 Personalization Audit Controls

4.7.3.d For accounts /envelopes, must include:

- *Number of accounts*
- *Number of card carriers printed*
- *Number of carriers wasted*
- *Number of envelopes*
- *Number of envelopes wasted*
- *Operator name and signature*
- *Supervisor or auditor name and signature*

Q 16 December 2013 – Section 4.7.3.d requires various counts for envelopes. Does this apply for all envelopes?

A *It applies only to envelopes with the payment system brand or issuer design and not to blank envelopes.*

4.7.3.e For PIN mailers, include:

- *Number of mailers to be printed*
- *Number of mailers actually printed*
- *Wasted mailers that have been printed*
- *Number of mailers transferred to the mailing area/room*
- *Operator name and signature*
- *Supervisor's or auditors name and signature*

Q 17 December 2013 – What happens if a supervisor or auditor is not available to sign off on the various required counts?

A *For purposes of this requirement, the terms "operator," "supervisor," and "auditor" do not mean a formal job title, but rather define a function. Specifically supervisor/auditor refers to the function of the individual who verifies the count, while operator refers to the individual who conducts the count.*

4.8.2 Tipping Foil

4.8.2.a The vendor must shred completely used tipping foil reels containing cardholder information as follows:

- *In-house,*
- *Under dual control, and*
- *Within 24 hours of their being removed from the embossing machine*

Q 18 December 2013 – Many facilities use portable/mobile shredding equipment managed by third-party service providers. How is this accommodated to meet 4.8.2.a?

A *The HSA includes the loading bay. The used foil can be destroyed there using portable/mobile equipment provided any access points (e.g., doors) from outside the HSA are closed and properly secured.*

Q 19 December 2013 – Considering Requirement 4.8.2.a, there may be circumstances where there is minimal material created that requires destruction. Can the destruction occur less frequently?

A *The requirement is under revision. Meanwhile, the destruction can occur as frequently as the vendor deems necessary, but in all cases, no less frequently than weekly. The vendor must maintain proper controls over these materials at all times prior to destruction, and the destruction must occur within the HSA.*

4.8.3 Indent Printing Module

4.8.3.a The vendor must use indent-printing modules only for payment system cards.

Q 20 December 2013 – How is this requirement applied?

A *Payment system proprietary Indent-printing modules cannot be used for other purposes than payment cards.*