Payment Card Industry (PCI)
Card Production Security Requirements

Technical FAQs for use with Version 1.0

October 2014

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

Q 1 **October 2014 - If a Chip Card manufacturer sets up a remote personalization service within an Issuer, is the Issuer facility required to be PCI Card Production compliant?**

A *If a third party (vendor) sets up and operates a personalization service inside an issuer's premises then the issuer facility is required to be approved. If the service is operated by the issuer so that only the issuer has access to card stocks, cardholder data and keys then it is not required to be approved. For further information regarding details of who is responsible for ensuring the compliance of the facility, contact the payment brand(s) of interest.*

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 2 **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.*

4.2 Encryption

All secret and confidential data must be:

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

b) Encrypted at all times during transmission and storage.

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

d) The vendor must only decrypt or translate cardholder data on the data-preparation or personalization network and not while it is on an Internet or public facing network.

Q 3 **October 2014 - Does transmission include the file movement between the systems on the data-preparation or personalization or does it apply only to data that is transmitted between organizational entities over a public network?**

A *If the data is going from one system or server to another then it is being transmitted and must be encrypted. It does not matter if the networks are not internet or public facing. The intention is that data is in clear only in memory for the minimum time required for processing.*

4.7 Contactless Personalization

4.7 The security requirements for dual-interface cards that are personalized using the contact interface are the same as for any other chip card. The requirements in this section apply to personalization of chip cards via the contactless NFC interface.

The vendor must:

a) Ensure personalization signals cannot be detected beyond the HSA.

b) Conduct a scan of area surrounding the HSA whenever the personalization environment is changed to confirm personalization data sent by wireless communication does not reach beyond the HSA.

c) Ensure that when personalization signals are encrypted, they comply with the encryption standards defined in Normative Annex A.

d) Perform a manual or automated inspection of the secure personalization area at least twice each month in order to detect any rogue radio-frequency (RF) devices.

e) Ensure that personalized cards (including rejects) are stored and handled as batches of two or more cards or enclosed within protective packaging that restricts reading card emissions until the cards are packaged for final distribution or destruction.

Q 4 **July 2014 - Do all the requirements of 4.7 apply when the personalization data is encrypted prior to sending it to the card**

A *This requirement is under revision. If 4.7 c is met then a, b, d need not apply.*

Section 5 – Network Security

5.2 General Requirements

The vendor must:

a) Maintain a current network topology diagram that includes all system components on the network.

b) Ensure the network topology diagram is reviewed, updated as appropriate, and verified at least once each year and whenever the network configuration is changed.

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

d) 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.

e) Put controls in place to restrict, prevent, and detect unauthorized access to this network. Access from within the high security area to anything other than the personalization network must be "read-only."

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

g) 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. These write functions must not transmit cardholder data.

h) Control at all times the physical connection points leading into the personalization network.

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

j) Transfer required issuer data and keys into the personalization network via a defined and documented process.

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

Q 5 **October 2014 - Access from within the high security area to anything other than the personalization network must be read-only. If the data preparation network is also in the high security area, can the personalization network write to the data preparation network?**

A *Yes, if they are separate networks then generally the data preparation network will deposit files for production on the personalization network or the personalization network will read them from the data preparation network. It's not a problem as long as they are both in the same HSA. If they are in separate HSAs, the communication path must conform to the DMZ security.*

Q 6 **October 2014 - Controls must be 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 and these write functions must not transmit cardholder data. If the data preparation and personalization networks are separate, can the data preparation network have write permissions to a corporate network?**

A *No, the data preparation network must meet the same requirements as the personalization network, data preparation is simply the first step in personalization*

Q 7 **October 2014 - Inventory and order systems may reside in the HSA on the data preparation and personalization networks. Corporate users may require access to the inventory and order detail updates performed on those systems. However, logical access from outside the HSA to these networks is not allowed, and access from within the HSA to anything other than the personalization network must be read-only How can the corporate users obtain access to this information?**

A *The information needs to be transferred out of the HSA using an approved process via the DMZ, just like cardholder return files, etc. Direct write from the system containing the information is not permitted.*

5.6 Remote Access

5.6.1 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 8 **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 9 **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.*

5.7 Wireless Networks

5.7.1 General

The vendor must:

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

b) Not use wireless communications for the transfer of any personalization data.

c) Identify, analyze, and document all connections. Analysis must include purpose, risk assessment, and action to be taken.

d) Use a scanning device that detects hidden networks, as well as wireless intrusion detection systems (WIDS)—fixed and/or mobile—that will detect hidden and spoofed networks.

e) Use a WIDS to conduct random monthly wireless scans within the HSA to detect rogue and hidden wireless networks.

Q 10 October 2014 - Requirement 5.7.1.d requires that a scanning device is used to detect hidden networks, and the use of a wireless intrusion detection network to detect hidden and spoofed networks. If a vendor does not have a wireless network, do they still need to comply?

A *This requirement is under revision. Yes, the vendor must still use a scanning device that is capable of detecting rogue and hidden wireless networks. Random scans of the HSA must be conducted at least monthly.*

5.8 Security Testing and Monitoring

5.8.1 Vulnerability

The vendor must:

a) Perform quarterly external vulnerability scans using an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC).

b) Perform internal and external vulnerability scans after any significant change. Scans after changes may be performed by internal staff.

c) Ensure all findings from vulnerability scans are prioritized and tracked. Corrective action for high-priority vulnerabilities must be started within two working days.

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

Q 11 October 2014 - Is an internal vulnerability scan only required when there has been a change and no longer each quarter?

A *This requirement is under revision. Because of evolving threat vectors, both external and internal network vulnerability scans must occur at least quarterly, as well as 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.*

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 12 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 1 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 2 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 3 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 as in the Human Resources Department.*

Section 8 – Key Management: Secret Data

8.4.2 Key Manager

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

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

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

Key custodians who form the necessary threshold to create a key must not report directly to the same manager.

Q 4 July 2014 - If the key manager is also a key custodian, can other key custodians report to the key manager?

A *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.*

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

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.

8.8 Key Storage

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

i. Date and time (in/out)

ii. Names of key custodians involved

iii. Purpose of access

iv. Serial number of envelope

Q 6 October 2014 - What specifically is the requirement regarding the signature of a custodian being placed on the access logs? Does it require the full name (first and last) or can the signature be first initial and last name or only be the initials of the custodians?

A *Signatures must be sufficient to identify each custodian. Full names or initials or any combination are acceptable as long as it can be positively affirmed who provided the signature.*

8.9 Key Usage

8.9.a Each key must be used for only one purpose and not shared between payment systems, issuers or cryptographic zones, for example:

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 7 July 2014 –Can vendor and issuer keys exist at another site, such as for subcontracted card production activities, or for disaster recovery purposes?

A *Copies of keys at another site (e.g. Issuer keys or personalization keys) may exist if there is a contract with that site e.g., if they are subcontracting the personalization activity to that site. This subcontracting needs the written permission of the issuer(s) impacted.*

For disaster recovery purposes, the same conditions apply. There must be a contract in place with the disaster recovery site and written permission of the issuer(s) impacted. These conditions apply whether the other site is operated by the vendor or by a third party.

Outside of the aforementioned conditions, the only storage that can be outside the HSA or offsite is of encrypted keys.

However, copies of the HSM's master file key cannot exist off site in any scenario. Storage of keys is a personalization activity so it must take place in the HSA, i.e. at the approved site. Custodians must be employees of the company i.e. not employees of another vendor.

Q 8 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 9 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.*

8.14 Key-Management Security Hardware

8.14.c HSMs used for key management or otherwise used for the protection of sensitive data must be approved by PCI or certified to FIPS 140-2 Level 3, or higher.

Q 10 July 2014 – Does the HSM FIPS/PCI certification include customization of native HSM firmware if the FIPS/PCI mode is not impacted.

A *If firmware is modified it impacts the approval. However, HSMs may allow customers or integrators to install additional applications where the vendor can show that by permitting this:*

- *It cannot adversely affect the security features of the product that are relevant to the PCI HSM certification.*
- *It cannot modify any of the cryptographic functionality of the HSM or introduce new primitive cryptographic functionality.*

- *The application is strongly authenticated to the HSM by digital signature.*
- *The application does not have access to sensitive keys.*

Applications, in this context, are functional entities that execute within the boundary of the HSM and may or may not provide services external to the HSM. Applications are typically processes or tasks that execute under the control of an Operating System (OS) or software executive routine.

Applications are considered to be separated by access rights. OS/firmware is considered all code, which is responsible to enforce, manage, or change such access rights.

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.*

2.5.1 Vendor Agents – General Guidelines

2.5.1.a Prior to conducting any business with an agent or third party regarding card-related activities, the vendor must register the agent with the VPA and obtain the following information:

- *Agent's name, address, and telephone numbers*
- *Agent's role or responsibility*

Q 4 July 2014 – In the context of this requirement, what are card-related activities and what activities are allowed for agents or third parties?

A *Card related activities such as sales and marketing activities are allowed. Agents and third parties must never produce, own or handle cards.*

Section 3 – Premises

3.1 External Structure

3.1.1 External Construction

a) The vendor must prevent unauthorized access to buildings, building areas, or structures containing technical machinery or equipment such as the heating system generator, auxiliary power supply, and air conditioning.

Q 5 October 2014 - If a facility has a fence around the whole property, is a separate fence still required around the technical machinery?

A *Yes, separate access controls are still required. There will be many people who will have access beyond the fence (everyone entering the facility) but who will not be authorized to access the machinery nor do they need to have access to the technical machinery. In general, technical machinery is not protected by a fence but by proper locked coverings or doors.*

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 6 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 7 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 8 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.*

New

Q 9 July 2014 - Is the Access Control Server located in the Security Control Room or in the Server Room?

A *The activities in the HSA are restricted to card production activities and therefore the access control server cannot be located in the HSA where the Server Room is required to be because networked systems are not allowed in the HSA.*

R: Ensure that if the access control server is not located in the security control room it must be located in a room of equivalent security. The access control server cannot be located in the HSA

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 10 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 11 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 12 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 13 December 2013 – For purposes of 3.3.4, do elevators, stairwells, closets and glass-enclosed rooms (e.g., conference rooms or other room types) 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.*

Q 14 October 2014 - If curtains or similar are used to segment the HSA in subareas, do those subareas constitute rooms for purposes of these requirements.

A *If visibility into the segmented area is not impaired from the general HSA area (for example: use of clear curtains), then the sub area does not constitute a room and therefore, any requirements pertaining to rooms do not apply for these subareas. When visibility is obstructed (for example: use of opaque curtains) in the "door" area, the opaque curtain acts as door thus creating a room and all requirements pertaining to rooms apply.*

Q 15 October 2014 - If the walls and/or door (s) of the room are glass such that the view is not restricted, does that constitute a room?

A *Yes it is a room. While glass allows visibility it still restricts access*

Q 16 October 2014 - Are any of these options acceptable to implement in lieu of implementing the controls for separate rooms under this section such as:

- **Glass doors without locks and a fully lit room**
- **Clear plastic flaps hanging from the door**
- **Swinging or sliding glass doors that do not have any type of closure mechanism**

A *Glass doors without locks and swinging or sliding doors are not acceptable. Clear plastic flaps hanging from the door or no door at all are the only viable options*

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 17 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.*

3.3.5.3 Sheet Destruction and Card Destruction Room(s)

Sheet and card destruction operations must take place in a separate room within the HSA.

Q 18 October 2014 - In the Card Production Physical Security Requirements it states that card destruction must occur in a separate room within the HSA. Would the Vault be considered a separate room or does in need to be in a secured room within the Vault?

A *A dedicated room must be used for destruction. This room must be in the HSA and may optionally be a secured room within the vault. This room must meet all room requirements. For example, the destruction room must have its own access controls.*

Q 19 **October 2014 - Sheet and card destruction must take place in a separate room within the HSA that is dedicated for destruction. Does this apply to other materials such as used tipping foil, holographic materials and signature panels?**

A *Yes*

3.3.5.4 PIN Mailer Production Room

3.3.5.4 b) Employees involved in personal identification number (PIN) printing and mailing processes must not monitor or be involved in the personalization, encoding, and embossing of the related cards.

Q 20 **July 2014 - If PIN printing and mailing, and personalization, encoding and embossing take place in an open area, how can this requirement be met?**

A *PIN printing must occur in a separate room except as delineated in PIN Printing and Packaging of Non-personalized Prepaid Cards. Documented procedures must exist that restrict personnel involved in PIN printing and mailing from being involved in the personalization, encoding and embossing of the related cards.*

3.3.5.5 Server Room & Key Management Room

a) Server processing and key management must be performed in a separate room within the personalization HSA.

b) An internal CCTV camera must be installed to cover the access to this room and provide an overview of the room whenever there is activity within it. The camera must not have zoom or scanning functionality and must not be positioned in such a manner as to allow observation of keystroke entry or the monitoring of the screen.

Q 21 **October 2014 - Server processing and key management must be performed in a separate room within the personalization HSA. What is considered 'server processing'?**

A *This applies to servers used for data preparation and personalization. It does not apply to DMZ based components.*

3.3.6 Vault

3.3.6.b) Vaults must be constructed of reinforced concrete (minimum 15 cm or 6 inches) or materials that provide equivalent strength and durability.

- *An outside wall of the building must not be used as a wall of the vault.*
- *No windows are permitted.*
- *There must be no access to the vault except through the vault door and gate configuration.*
- *The vault must be protected with sufficient number of shock detectors to provide full coverage of the walls, ceiling, and floor.*
- *The vault must be fitted with a main steel-reinforced door with a double mechanical or logical dual-locking mechanism that requires physical and simultaneous dual-control access. The access mechanism requires that access occurs under dual control and does not allow entry by a single individual—i.e., it is not feasible for a single individual to use credentials belonging to someone else to simulate dual access.*

Q 22 **October 2014 - Vaults are required to be constructed out of reinforced concrete with a minimum thickness of 6 inches, or materials that provide equivalent strength and durability. Does the use of Class 1 Certification Standards for the construction meet the equivalence factor, even though only 5 inch slabs may be used?**

A *This requirement is under revision. Yes, the use of Underwriters Laboratories Class 1 Certification Standards for the construction is acceptable*

3.3.6.d If the vault door is required to remain open during production hours, an inner grille must be used. The vault door or inner grille must remain closed and locked at all times, except when staff require access to the vault for example to store or remove items. The inner grille must be fitted with a dual-control locking mechanism or access reader.

Q 23 **July 2014 - Where a vault door is required to remain open during production hours, an inner grille must be used. The inner grille must remain closed and locked at all times, except when staff require access to the vault. In this case the inner grille must be fitted with a dual-control locking mechanism or an access reader. However, access by use of physical keys means the access control system does not know who is in the vault and it is not possible to enforce anti-pass back or to enforce automatic activation of the motion detector as required for all other rooms in the HSA. Are mechanisms to enforce anti-passback and automatic activation of motion detection required in this scenario?**

A *This requirement is under revision. The inner grille must meet the same access control criteria as other rooms within the HSA.*

3.4.2.2. System Administration

Q 24 **July 2014 - Can a company have a badge access system that services multiple buildings on a single premises and/or multiple buildings throughout the world as long as the system is on its own segregated/dedicated network and all system changes are made on-site within a PCI compliant/secure room?**

A *For multiple buildings within the same facility, a single central location can administer all buildings. However, a central facility cannot administer multiple separate facilities. The badge access system must be located within a given facility and only control access to buildings within that facility.*

3.4.5.2 Monitor, Camera, and Digital Recorder Requirements

a) Each monitor, camera, and digital recorder must function properly and produce clear images on the monitors without being out-of-focus, blurred, washed out, or excessively darkened. The equipment must record at a minimum of four frames per second.

b) CCTV cameras must record all activity, including recording events during dark periods through the use of infrared CCTV cameras or automatic activation of floodlights in case of any detected activity. This recording may be via motion activated. The recording must continue for at least a minute after the last pixel of activity subsides. .

c) CCTV monitors and recorders must be located in an area that is restricted from unauthorized personnel.

d) CCTV cameras must be connected at all times to:

- *Monitors located in the control room*
- *An alarm system that will generate an alarm if the CCTV is disrupted*
- *An active image-recording device*

Q 25 October 2014 - For purposes of this requirement, can motion activation recording be used, such that if there is not any activity and associated motion, there is not any need to record? If motion activation is allowed, how long past cessation of motion must be recorded?

This requirement is under revision. The new text will state: CCTV cameras must record all activity, including recording events during dark periods through the use of infrared CCTV cameras or automatic activation of floodlights in case of any detected activity. This recording may be motion activated. The recording must continue for at least fifteen seconds after the last pixel of activity subsides.

3.4.5.4 Retention of Video Recordings

3.4.5.4.a CCTV images must be kept for at least 90 days and must be backed up daily.

Q 26 July 2014 – Backups must be kept for at least 90 days and must occur daily. Does each daily back up need to occur for at least 90 days and does the 90 days only pertain to backups.

A *Standard back-up policies using full/incremental - daily/weekly/monthly – can be used. Both primary and back-up copies must be kept for a minimum of the most recent 90 days.*

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 27 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 28 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 29 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 Audit Controls – Manufacturing

4.7.1 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 30 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.*

4.7.1.1 Log Modifications

a) If modifications are to be made to the audit log, a single line must be made through the original figure.

b) The updated figure and the initials of the employee making the changes must be placed adjacent to the incorrect figure.

4.7.1.2 Log Review

All logs must be prepared and maintained by an individual who is not involved in the direct operation of the equipment.

4.7.3 Personalization Audit Controls

Q 31 October 2014 - Section 4.7 is marked as valid only for Manufacturing, but 4.7.3 specifically refers to Personalization Audit Controls. Does 4.7.1.1 & 4.7.1.2 (logs) refer to only manufacturing logs and not to Personalization logs? Or are we to understand that only 4.7.1 (and not its sections 4.7.1.1 and 4.7.1.2) applies exclusively to Manufacturing while the rest apply to both Manufacturing and Personalization?

A *This requirement is mislabeled. It should say production rather than manufacturing as it applies to both e.g. 4.7.1.1 does contain references to personalization*

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 32 July (update) 2014 – 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. This is so they cannot be inappropriately used in correspondence with cardholders.*

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 33 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 34 October (update) 2014 – 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. This can also be applied to other secure materials that require destruction, such as scrap cards, return mail cards, and vault destroy requests.*

Q 35 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 36 July (update) 2014 – How is this requirement applied?

A *Payment system proprietary typefaces within Indent-printing modules cannot be used for other purposes than payment cards. Proprietary indent printing characters are destroyed at the end of usage.*

4.10 Destruction and Audit Procedures

4.10.b The following materials must be destroyed on a batch basis by shredding or grinding such that the resulting material cannot be reconstructed:

- *Spoiled or waste card products*
- *Holographic materials*
- *Signature panels*
- *Sample and test cards*
- *Any other sensitive card component material or courier material related to any phase of the card production and personalization process.*
- *Destruction of chips, modules, or chip cards must ensure that the chip itself is destroyed.*

Q 37 July 2014 - 4.10 requires that materials must be destroyed on a batch basis. Does this mean materials must be destroyed at the conclusion of each job?

A *No, multiple jobs can be grouped together to form a batch.*

Section 5 – Packaging and Delivery Requirements

Q 38 October 2014 - The acceptable methods of shipping personalized cards are:

(1) Secure shipment in unlimited quantities

(2) Courier Shipment in unlimited quantities

For shipping personalized cards to a pre-sort facility prior to mailing, are there any other acceptable options?

A *Yes. For transfer to the mail facility, personalized cards may be transported using a company vehicle with the following security controls:*

- *A GPS tracking device is used and monitored during transport from within the security control room.*
- *The contents are secured with tamper evident straps and checked upon delivery.*
- *The vehicle is loaded using dual control and locked during transport*
- *Vehicle drivers do not have a key or access to contents*
- *Two persons are in the vehicle equipped with a device to communicate with the security control room.*