



Payment Card Industry (PCI) Card Production Security Requirements

Technical FAQs for use with Version 1

July 2013

Table of Contents

Logical Security Requirements <i>Frequently Asked Questions</i>	3
General Questions.....	3
Section 5 – Network Security	3
Section 8 – Key Management: Secret Data	3
Physical Security Requirements <i>Frequently Asked Questions</i>	4
General Questions.....	4
Section 2 - Personnel	4
Section 3 - Premises.....	4

Logical Security Requirements Frequently Asked Questions

These technical FAQs provide answers to questions regarding the application of the *PCI (Payment Card Industry) 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 or questions modified for clarity are in **red**.

General Questions

Section 5 – Network Security

Q 1 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

Section 8 – Key Management: Secret Data

Q 2 July 2013 - The Key Usage section stipulates that “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.” 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.

Physical Security Requirements

Frequently Asked Questions

These technical FAQs provide answers to questions regarding the *PCI (Payment Card Industry) 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

Section 2 - Personnel

- Q 1 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.*

Section 3 - Premises

- Q 2 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 either be closed off, or reconfigured to no longer be separate rooms*
- Q 3 July 2013 - Requirement 3.3.5 prohibits toilets in the HSA except where required by local law. What is the rationale for this requirement?**
- A** *The intent is to prevent any single individual being unobserved while within any room within the HSA.*