Payment Card Industry (PCI)

PIN Security Requirements

PCI SSC Modifications – Summary of Significant Changes

December 2014

PCI SSC Modifications to PCI PIN Security Requirements

In the table below, "Main Body" refers to the Control Objectives and the "PIN Security Requirements – Technical Reference" sections of the *PCI PIN Security Requirements* manual.

Within that same document:

- Normative Annex A applies to specific requirements pertaining to acquiring entities involved in the implementation of symmetric-key distribution using asymmetric keys (remote key distribution) or those entities involved in the operation of Certification and Registration Authorities for such purposes.
- Normative Annex B applies to specific requirements pertaining to entities that operate key-injection facilities.

Requirement	Section(s)	Modification
General	**Introduction**	Added criteria that acquiring entities must maintain a summary listing of the cryptographic keys used in connection with the acquiring and processing of PIN data. Added "Limitations" section specifying: 1. Formal acknowledgement of the supremacy of national and local laws if in conflict with any requirement; and 2. Reference to contact payment brands for any compliance program details.
	Technical Reference	Updated Technical References
	Main Body **Normative Annex A** **Normative Annex B**	Changed terminology from Data Encryption Standard (DES) to Data Encryption Algorithm (DEA). Added test procedures for all requirements.
	Normative Annex A	Split Annex A into two sub-Annexes as follows: 1. A1 – Remote Key-Distribution Using Asymmetric Techniques Operations: Characteristics of the actual key-distribution methodology implemented. These requirements apply to all entities implementing remote key distribution using asymmetric techniques. 2. A2 – Certification and Registration Authority Operations: Operations of Certification and Registration Authority platforms used in connection with remote key-distribution implementations. These requirements apply only to the entities operating Certification and/or Registration Authorities.

Requirement	Section(s)	Modification
General (continued)	**Normative Annex C**	Modified Annex to introduce concept of "bits of security" as stipulated in *NIST SP 800-57*. Increased minimum key size for Elliptic Curve and DSA keys to 224 and 2048/224 respectively. Updated information for DH implementations and added information for ECDH implementations.
	Glossary	Updated and added glossary terms.
1	**Main Body** **Normative Annex B**	Added requirement that the entity acquiring PIN-based transactions is responsible for maintaining both summary and detailed inventory information for POI devices.
2	**Main Body**	Specified that AES is not allowed for use in encrypting PINs until subsequent to publication of ISO 9564 with the prescribed AES PIN format.
3	**Main Body**	Updated for addition of AES PIN blocks – ISO Format 4. Noted translation restrictions are not applicable to surrogate PANs used in tokenization implementations.
4	**N/A**	N/A
5	**N/A**	N/A
6	**Main Body** **Normative Annex B**	Clarified that full-length key components and key shares created using recognized key-splitting algorithms do not constitute "parts" of clear-text keys.
		Specified that devices used for the generation of clear-text key components must be powered off when not in use; however logically partitioned devices used concurrently for other processes—e.g., providing services simultaneously to host systems—such as for transaction processing, must have key-generation capabilities disabled when not in use and other activities are continuing. Added additional clarification to the prohibition of multi-use/purpose computing systems for key generation where any clear-text secret or private key or component thereof appears in unprotected memory. Printers used for key generation can only be used for that purpose.
7	**Main Body** **Normative Annex B**	Specified that logs must exist for KEKs exchanged with other organizations MFKs and BDKs.

Requirement	Section(s)	Modification
8	**Main Body** **Normative Annex B**	Noted that the requirement that keys must be transferred either encrypted or—if clear text—as two or more components using different communication channels or within an SCD does not apply to keys installed in POI devices meeting Requirement 1 when shipped from the key-injection facility. Specified that where an SCD (HSM or KLD) is conveyed with pre-loaded secret and/or private keys, the SCD must require dual-control mechanisms to become operational. Those mechanisms must not be conveyed using the same communication channel as the SCD. SCDs must be inspected for signs of tampering.
9	**N/A**	N/A
10	**Main Body** **Normative Annex B**	Specified explicit criteria for equality of key strength for keys enciphering other keys.
11	**N/A**	N/A
12	**N/A**	N/A
13	**N/A**	N/A
14	**N/A**	N/A
15	**N/A**	N/A
16	**N/A**	N/A
17	**N/A**	N/A
18	**Main Body** **Normative Annex B**	Specified that, effective 1 January 2018, encrypted symmetric keys must be managed in structures called key blocks, in accordance with ANSI X9.24-1
19	**Main Body**	Extended allowance to allow production platforms to be used temporarily for test purposes if a business rationale exists, subject to certain conditions. Specified that for logically partitioned HSMs and computing platforms, if one or more logical partitions of a physical device are used for production and one or more other logical partitions are used for testing, including QA or similar, the entire configuration must be managed and controlled as production.

Requirement	Section(s)	Modification
20	**Main Body** **Normative Annex B**	Clarified the requirement that a transaction-originating terminal have completely different key sets to interface with more than one entity, to specify that entity is an acquiring organization and not an "acquirer." Added additional POI portfolio segmentation strategies for entities processing or injecting DUKPT or other key-derivation methodologies into POI devices.
21	**N/A**	N/A
22	**Normative Annex A**	Subordinate CAs must have a minimum length of 2048 for RSA or equivalent. Effective January 2017, KDHs must have a minimum length of 2048 for RSA or equivalent.
23	**N/A**	N/A
24	**Main Body** **Normative Annex B**	Clarified criteria for destruction of keys or their components. Clarified that the for key components for keys other than the HSM MFK that have been successfully loaded and confirmed as operational do not have to be destroyed if the HSM does not store the encrypted values on a DB but only stores the subordinate keys internal to the HSM, and that BDKs used in KLDs may also be stored as components where necessary to reload the KLD.
25	**Main Body** **Normative Annex B**	Specified that key custodians must be employees or contracted personnel. Specified criteria to follow where organizations are of such insufficient size that they cannot support the reporting-structure requirement.
26	**Main Body** **Normative Annex B**	Specified that key-destruction logs must be archived for a minimum of two years subsequent to key destruction.
27	**Main Body** **Normative Annex B**	Specified that the requirement that creation of keys must require a minimum of two authorized individuals to enable the process applies to top-level keys—e.g., the MFK.
28	**Annex A**	Added criteria for vetting certificate requests for KDHs.
29	**N/A**	N/A
30	**Main Body**	Created separate requirement for physical and logical protection for POI devices to differentiate from HSMs and KLDs.
31	**N/A**	N/A

Requirement	Section(s)	Modification
32	**Main Body** **Normative Annex B**	Clarified that for devices that do not support two or more passwords, splitting the single password used by the device into two halves, each half controlled by a separate authorized custodian, is acceptable.
	Annex A	Clarified that synchronization errors between CCTV, intrusion detection and access control cannot exceed one minute.
	Annex B	Added criteria for where a secure room may not be required for key injection of encrypted keying material.
33	**N/A**	N/A