Payment Card Industry (PCI)
PIN Security Requirements

PCI SSC Modifications – Summary of Changes

December 2011

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	Main Body Normative Annex A Normative Annex B	▪ Changed terminology from Tamper Resistant Security Module (TRSM) to Secure Cryptographic Device (SCD). ▪ Harmonized language such that words *must* and *shall* indicate a mandatory requirement. The word *should* indicates a best practice.
	Normative Annex A	▪ Added additional language to clarify applicability of requirements. ▪ Clarified that these requirements pertain to two distinct areas and differentiated by notation those requirements that pertain to the operation of a CA/RA: 1) 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. 2) Characteristics of the actual key-distribution methodology implemented. These requirements apply to all entities implementing remote key distribution using asymmetric techniques.
	Normative Annex B	▪ Clarified that Annex B applies to all entities that operate key injection facilities, including only on behalf of themselves. ▪ Removed Normative Annex A text to streamline. Normative Annex A still applies if applicable

Requirement	Section(s)	Modification
	Normative Annex C	Created new Annex specifying minimum and equivalent key sizes and strengths for approved algorithms
1	Main Body Normative Annex B	Specified that: ▪ All newly deployed ATMs and POS PIN-acceptance devices are compliant with the applicable PCI Point of Interaction Security Requirements and that newly deployed hardware security modules should be compliant to the PCI HSM Security Requirements. ▪ Purchase orders for Point of Interaction PIN-acceptance devices must specify compliance to the applicable PCI Point of Interaction Security Requirements.
2	N/A	N/A
3	N/A	N/A
4	N/A	N/A
5	N/A	N/A
6	Main Body Normative Annex B	Clarified that applicability is to unencrypted secret and private keys and their components.
	Normative Annex B	Clarified that where clear-text secret and/or private keys and/or their components do not reside within the secure boundary of an SCD for key loading, additional controls must be implemented as stated in Requirement 13.
7	N/A	N/A
8	Main Body Normative Annex B	▪ Added verbiage to address m-of-n key-sharing schemes. ▪ Clarified that e-mail shall not be used for the conveyance of secret or private keys or their components, even if encrypted unless the key (or component) has already been encrypted in accordance with these requirements, i.e., in an SCD.
9	Main Body Normative Annex B	Clarified applicability is to unencrypted secret and private key components.
10	Main Body Normative Annex B	Clarified that keys existing outside of an SCD must be protected by keys of equal or greater strength as delineated in Annex C.

Requirement	Section(s)	Modification
11	N/A	N/A
12	Main Body Normative Annex B	▪ Clarified applicability is to unencrypted secret and private keys and their components. ▪ Specified that TR-31 or an equivalent methodology should be used for key loading whenever a symmetric key is loaded encrypted by another symmetric key. ▪ Specified that mutual device authentication is required for host-to-host connections in addition to host-to-PIN acceptance device connections where public key techniques are used for key establishment.
13	Main Body Normative Annex B	Clarified that: ▪ Applicability is to unencrypted secret and private keys and their components. ▪ Non-SCDs shall not be used in the loading of clear-text secret or private keys or their components, outside of a secure key-loading facility, as delineated in Annex B. For example, ATM keyboards shall never be used for the loading of clear-text secret or private keys or their components.
	Normative Annex B	Clarified that: ▪ Where clear-text secret and/or private keys and/or their components do not reside within the secure boundary of an SCD for key loading, additional controls must be implemented as stated in Requirement 13. ▪ SCD equipment must be inspected to detect evidence of monitoring and to ensure that the key loading occurs under dual control.
14	Main Body Normative Annex B	Specified that passwords must be managed such that no single individual has the capability to enable key loading.
15	Main Body Normative Annex B	Clarified that recorded or displayed key-component check values and key check values shall not exceed six hexadecimal characters in length.
	Normative Annex A	Clarified that validation of authentication credentials must occur immediately prior to any key establishment for both initial and any subsequent key exchanges.
16	N/A	N/A

Requirement	Section(s)	Modification
17	Main Body	Clarified that applicability is to be between two different organizations.
18	Main Body Normative Annex B	Specified that TDEA keys should be managed as key bundles at all times.
19	Main Body Normative Annex B	Clarified that master file keys and their variants used by host processing systems for encipherment of keys for local storage cannot be used for other purposes.
	Normative Annex A Normative Annex B	Specified conditions under which a production platform (HSMs and servers/stand-alone computers) may be temporarily used for test purposes.
20	Main Body Normative Annex B	Specified that entities processing or injecting DUKPT or other key-derivation methodologies on behalf of multiple acquiring financial institutions must use different Base Derivation Keys for each financial institution. The processing entity may share one or more Base Derivation Keys for merchants that are sponsored by the same Acquirer.
21	Main Body Normative Annex B	Clarified that: ▪ Applicability is to secret and private keys. ▪ Keys existing outside of an SCD must be protected by keys of equal or greater strength as delineated in Annex C.
	Normative Annex B	Clarified that where clear-text secret and/or private keys and/or their components do not reside within the secure boundary of an SCD for key loading, additional controls must be implemented as stated in Requirement 13.
22	Main Body Normative Annex B	Specified recommended key-usage periods for double-length TDEA keys.
23	Main Body Normative Annex B	Clarified that scope of the requirement includes the processing host master file key and its variants.
24	Main Body Normative Annex B	Clarified that key destruction includes the components of secret and private keys as well as the keys themselves.

Requirement	Section(s)	Modification
25	Main Body Normative Annex B	▪ Clarified that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component. ▪ Specified that key custodians sufficient to form the necessary threshold to create a key must not directly report to the same individual.
	Normative Annex A	Increased minimum pass phrase from six to eight characters for Certification and Registration Authority relevant equipment.
	Normative Annex A	Added biometrics as an associated usage authentication mechanism for security tokens
26	N/A	N/A
27	N/A	N/A
28	N/A	N/A
29	Main Body Normative Annex B	Specified that precautions must be taken to minimize the threat of compromise of PIN-processing equipment once deployed.
	Normative Annex B	Specified that secure areas must be established for the inventory of PEDs that have not had keys injected.
30	N/A	N/A
31	Main Body Normative Annex B	▪ Clarified applicability to hardware security modules and key-injection/loading devices. ▪ Added restrictions for logical access to PIN-processing equipment (HSMs).
	Normative Annex B	Specified physical security requirements for the key-injection area.
32	Main Body Normative Annex B	Specified that HSM security policies/configurations must be validated to secure settings at least annually.
	Main Body	▪ Specified that HSMs used for acquiring functions should not also be used for issuing functions, and that acquiring and issuing functionality should be logically segmented within a given network. ▪ Specified that HSMs used for acquiring functions shall not be configured to output clear-text PINs.