Payment Card Industry (PCI)

PIN Security Requirements

PCI SSC Modifications – Summary of Significant Changes from v2.0 to v3.0

August 2018

PCI SSC Modifications to PCI PIN Security Requirements

In the table below, “Transaction Processing Operations” refers to the Control Objectives and the “PIN Security Requirements – Technical Reference” section of the *PCI PIN Security Requirements and Testing Procedures* manual. Within that 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	Overview	Main body of requirements now delineated as “Transaction Processing Operations” to clarify scope as pertaining to the acquiring and related processing of PIN-based transactions. Clarified that entities may be subject to requirements in multiple sections, depending on the activities performed. Clarified where vendor-controlled secret and private keys are subject to review under Annexes A and/or B. Clarified consideration of MAC and account data encryption keys. Added criteria to facilitate reviews that all entities subject to these requirements must maintain a summary listing of the cryptographic keys used, including identification of the algorithm (e.g., AES, TDEA, RSA) used and key size (e.g., 128, 2048) for each key type for activities in which they engage, whether for: • Transaction Processing Operations • Symmetric Key Distribution Using Asymmetric Techniques • Key-Injection Facilities Additionally, entities engaged in the processing of PIN-based transactions must construct a network schematic detailing transaction flows with the associated key usage.

Requirement	Section(s)	Modification
General (continued)	Overview (continued)	Added sunset dates for the use of fixed key TDES: • Effective 1 January 2023: Fixed key for TDES PIN encryption in POI devices is disallowed. • Effective 1 January 2023: Fixed key for TDES PIN encryption in host to host connections is disallowed. Added effective dates for support of ISO PIN block format 4. Specifically: • Effective 1 January 2023: All hosts must support ISO PIN block format ISO 4 decryption. • Effective 1 January 2025: All hosts must support ISO PIN block format 4 encryption.
	Technical Reference	Updated Technical References to add *ANSI X9.24-3* and *ANSI TR34*.
	Transaction Processing Operations Normative Annex A Normative Annex B	Added test procedures for all requirements. Clarified usage of term “secure room.”
	Normative Annex A	Clarified that the Annex applies for the distribution of acquirer keys to transaction-originating devices (POIs) for use in connection with PIN encryption, whether the actual distribution of acquirer keys occurs from the transaction processing host or is distributed directly by the vendor. Cited *ANSI TR-34* as a methodology that is compliant with these requirements. Clarified that Annex A does not apply if the key loading is not performed remotely and authentication is provided by another method.
	Normative Annex B	Clarified that Annex is applicable for the loading of acquirer keys.
	Appendix A	Added matrix to delineate the applicability of requirements by business activity.
	Glossary	Updated and added glossary terms.
1	Transaction Processing Operations	Specified criteria from POI Security Requirements that the addition of applications that replace or disable the PCI-evaluated firmware functionality invalidates the device approval for each such implementation unless those applications are validated for compliance to *PTS POI Security Requirements* and listed as such in the approval listings.

Requirement	Section(s)	Modification
1	Transaction Processing Operations Normative Annex B	Modified device information required to be captured.
1	Normative Annex B	Clarified that key-injection platforms and systems shall include hardware devices for managing (e.g., generating and storing) the keys that conform to the requirements for SCDs. Modified PEDs that have not been validated to the PCI KLD approval class must be managed equivalent to personal computers as noted in Requirement 13-9.
2	N/A	N/A
3	N/A	N/A
4	N/A	N/A
5	Transaction Processing Operations Normative Annex B	Clarified that key generation must occur within an SCD.
6	Transaction Processing Operations Normative Annex B	Modified requirement to allow re-authentication whenever key generation is invoked in addition to powering off for devices used for generation of clear-text key components that are output in the clear. Clarified that equipment used for the generation of clear-text key components must be inspected for signs of tampering prior to the initialization of key-generation activities. Clarified that multi-use/purpose computing systems shall not be used for key generation where any clear-text secret or private key or component thereof appears in unprotected memory outside the tamper-protected boundary of an SCD. Clarified that dedicated computers using an SCD meeting Requirement 5.1 may be used for key generation. Clarified that printers used for printing key components must not be networked.

Requirement	Section(s)	Modification
6 (continued)	Transaction Processing Operations Normative Annex B (continued)	Added option for printed key components to be sealed in pre-numbered, tamper-evident, authenticable packaging immediately after printing or transcription, in lieu of within PIN mailers. Added requirement that printers used for printing key components must be managed under dual control, including use of a secure room. Clarified that requirement for policies and procedures to exist to prohibit keys or their components from being transmitted across insecure channels applies to clear-text secret and private keys and their components.
7	Transaction Processing Operations Normative Annex B	Specified that logs for the generation of higher-level keys must at a minimum include date and time, object name/identifier, purpose, name and signature of individual(s) involved, and if applicable, tamper-evident package number(s) and serial number(s) of device(s) involved.
8	Transaction Processing Operations Normative Annex B	Clarified that it is the responsibility of both the sending and receiving parties to ensure these keys are managed securely during transport. Clarified that self-signed root certificates protect the integrity of the data within the certificate but do not guarantee the authenticity of the data.
9	Transaction Processing Operations Normative Annex B	Clarified this requirement also applies to keys moved between locations of the same organization. Clarified that key-compromise process involves both a documented analysis and confirmation. Added requirement for when components or shares of multiple keys are being sent simultaneously between the same sending and receiving custodians.
10	Normative Annex B	Clarified that key-conveyance requirements apply to between locations or systems within the same key-injection facility.
11	N/A	N/A

Requirement	Section(s)	Modification
12	Transaction Processing Operations Normative Annex B	Clarified that dual control includes use of separate key-loading devices for each component/share. Clarified that for devices that do not support two or more passwords/authentication codes, each half of the split password/authentication code must still be at least five characters. Clarified that passwords/authentication codes to the same object may be assigned to a custodian group team e.g., custodian team for component A.
13	Transaction Processing Operations Normative Annex B	Added requirement that keyboards attached to an HSM shall never be used for the loading of clear-text secret or private keys or their components.
13	Normative Annex B	Added sunset dates for allowed usage of PCs to load clear-text secret and/or private keys and/or their components where they exist in unprotected memory outside the secure boundary of an SCD. Specifically: • Effective 1 January 2021, entities engaged in key loading on behalf of others shall not be allowed to use PC-based key-loading methodologies where clear-text secret and/or private keying material appears in the clear in unprotected memory outside the secure boundary of an SCD. • Effective 1 January 2023, entities only performing key loading for devices for which they are the processor shall no longer have this option.
14	Transaction Processing Operations Normative Annex B	Clarified that all cable attachments over which clear-text keying material traverses must be examined at the beginning of an entity's key-activity operations (system power on/authorization).
15	Transaction Processing Operations Normative Annex B	Added key check value method that is optional for TDEA keys and mandatory for AES keys.
15	Normative Annex A	Clarified that authentication mechanisms may include ensuring the SCD serial number is listed in a table of "permitted" devices.
16	N/A	N/A
17	N/A	N/A

Requirement	Section(s)	Modification
18	Transaction Processing Operations Normative Annex B	Clarified that key-compromise process involves both a documented analysis and confirmation. Modified and extended implementation date for managing encrypted symmetric keys as key blocks. New dates are divided into three phases.
19	Transaction Processing Operations Normative Annex B	Added requirement that private keys used for remote key distribution shall not be used in connection with any other purpose.
19	Normative Annex A	Clarified that a CA cannot sign certificates to both subordinate CAs and end-entity (POI) devices. Added requirement for usage of certificates in conjunction with remote key-distribution functions. Specifically: • Certificates associated with encryption for remote key-distribution functions must not be used for any other purpose. • Certificates associated with authentication of the KDH must not be used for any other purpose. • Certificates associated with authentication of the POI must not be used for any other purpose. • Certificates associated with authentication of POI firmware and POI applications must not be used for any other purpose.
20	Transaction Processing Operations Normative Annex B	Clarified that the same BDK with the same KSN installed in multiple injection systems or installed multiple times within the same injection system will not meet uniqueness requirements.
21	Transaction Processing Operations Normative Annex B	Clarified that key-injection facilities may have clear-text keying material outside of an SCD when used within a secure room in accordance with Requirement 32.
22	Transaction Processing Operations Normative Annex A Normative Annex B	Modified requirement to state “key determined to be compromised” instead of “known or suspected compromise key.”
23	N/A	N/A
24	N/A	N/A

Requirement	Section(s)	Modification
25	Transaction Processing Operations Normative Annex B	Specified additional criteria for key custodians.
25	Normative Annex A	Clarified that individual user IDs may be assigned to a role or group. Clarified where requirements apply to CAs operated online.
26	Transaction Processing Operations Normative Annex B	Added requirement that key-component logs must include the name and signature of a non-custodian (for that component/share) witness.
27	N/A	N/A
28	Transaction Processing Operations Normative Annex B	Clarified security-training requirements for key custodians.
29	Transaction Processing Operations Normative Annex B	Specified that logs for access to POIs and other SCDs must at a minimum include date and time, object name/identifier, purpose, name and signature of individual(s) involved, and if applicable, tamper-evident package number(s) and serial number(s) of device(s) involved. Clarified that chain of custody includes procedures, as stated in Requirement 29-1, to ensure that access to all POI devices and other SCDs is documented, defined, logged, and controlled such that unauthorized individuals cannot access, modify, or substitute any device without detection. Added an option for implementing physical protection of devices from the manufacturer’s facility up to the point of key-insertion and deployment. Added requirement for existence of documentation of HSM configuration settings.
30	N/A	N/A
31	Transaction Processing Operations Normative Annex B	Clarified that requirement for irrecoverable deletion of keys and keying material stored within SCDs removed from service applies to private and secret keys.
32	Annex A	Modified to reflect that non-CA personnel must sign an access logbook when entering the Level 3 environment.

Requirement	Section(s)	Modification
32	Normative Annex B	Added sunset dates for allowed injection of clear-text secret or private keying material. Specifically: • Effective 1 January 2021, the injection of clear-text secret or private keying material shall not be allowed for entities engaged in key injection on behalf of others. Only encrypted key injection shall be allowed for POI v3 and higher devices. • Effective 1 January 2023, the same restriction applies to entities engaged in key injection of devices for which they are the processors. This does not apply to key components entered into the keypad of a secure cryptographic device, such as a device approved against the *PCI PTS POI Security Requirements.* It does apply to all other methods of loading of clear-text keying material for POI v3 and higher devices. Added requirements for the retention of CCTV images.
33	N/A	N/A