



Payment Card Industry (PCI) PIN Security Requirements

**Summary of Requirements
Changes from v3.0 to v3.1**

March 2021

Introduction

In the table below, “Transaction Processing Operations” 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	Overview	ISO PIN Block Format 4 support dates are suspended until further notice.
	Technical Reference	Modified ANSI and NIST references.
	Normative Annex A	Added ANSI TR-34 information.
	Normative Annex B	Added additional language to clarify remote key loading.
	Normative Annex C	Updated wording throughout.
	Appendix A	Updated applicability of requirements.
	Glossary	Updated and added glossary terms.
1	Transaction Processing Operations Normative Annex B	Added reference to FIPS 140-3 Clarified for PCI approved HSMs that the approval may be contingent on being deployed in controlled environments or more robust (e.g., secure) environments as defined in ISO 13491-2 and in the device’s PCI HSM Security Policy.
1	Normative Annex B	Clarified equipment usage.
2	N/A	N/A
3	N/A	N/A
4	N/A	N/A
5	Transaction Processing Operations Normative Annex B	Added reference to FIPS 140-3.
6	Transaction Processing Operations Normative Annex B	Added criteria from technical FAQs for secure room used for printing key components not originally included in RFC.
7	N/A	N/A

Requirement	Section(s)	Modification
8	N/A	N/A
9	N/A	N/A
10	Transaction Processing Operations Normative Annex B	Clarified language on use of RSA keys sizes of 1024 and 2048 and SHA-1/SHA-2 when used for key distribution in accordance with Annex A.
11	N/A	N/A
12	N/A	N/A
13	Normative Annex B	Clarified wording for BDK loading.
14	N/A	N/A
15	Transaction Processing Operations Normative Annex B	Clarified key-check value wording.
16	N/A	N/A
17	N/A	N/A
18	Transaction Processing Operations Normative Annex B	Updated effective dates for phases 2 and 3 of key block implementation.
19	N/A	N/A
20	N/A	N/A
21	Normative Annex A	Added references to Annex C and FIPS 140-2/140-3.
22	Normative Annex A	SCRP devices must have a minimum RSA 2048 bits or equivalent.
23	N/A	N/A
24	N/A	N/A
25	N/A	N/A
26	Transaction Processing Operations Normative Annex B	Added test step.
27	N/A	N/A
28	N/A	N/A
29	Transaction Processing Operations Normative Annex B	Clarified applies to SCDS used for key injection or code signing, including display prompts.

Requirement	Section(s)	Modification
30	N/A	N/A
31	N/A	N/A
32	Transaction Processing Operations	Aligned authentication code criteria with Annex B.
32	Normative Annex B	Aligned encrypted key loading dates with previously issued PCI bulletin which deferred the implementation dates three years and the applicability changed from POI v3 and higher devices to POI v5 and higher devices.
33	N/A	N/A