Payment Card Industry (PCI)

Point-to-Point Encryption Security Requirements and Testing Procedures

Summary of Significant Changes from v2.0 to v3.0

December 2019

PCI P2PE Summary of Significant Changes

This document provides an overall summary of significant changes from P2PE v2.0 revision 1.1 to P2PE v3.0 of the Security Requirements and Testing Procedures (i.e., the P2PE Standard).

Table 1: Change Types

Change Type	Definition
Clarification	Clarifies intent of requirement or testing procedure. Ensures that concise wording in the standard portrays the desired intent of requirements.
Additional guidance	Explanation, definition, and/or instruction to increase understanding or provide further information or guidance on a particular topic.
Evolving / New	Changes to ensure that the standard is up to date with emerging threats and changes in the market. May consist of a new or modified requirement, test procedure, or context.
Removal	Deleted a requirement or context due to redundancy or to better reflect the intent of the standard.
Restructure	Changes to eliminate redundant requirements or better align content with other requirements/standards.

Table 2: Summary of Changes

P2PE v2.0	P2PE v3.0	CHANGE	TYPE
GENERAL			
Title		The P2PE Standard has been renamed: **FROM** "Point-to-Point Encryption Solution Security Requirements and Testing Procedures" **TO** "Point-to-Point Encryption Security Requirements and Testing Procedures"	Clarification
Various Sections	N/A	All references to domain applicability relative to assessment responsibilities (e.g., which Domains each Component Provider Type must assess to) have been removed. This encompasses the following changes: ▪ "Alignment of P2PE Requirements with Entities Offering P2PE Services" section has been removed. ▪ "P2PE Solution and/or Component Validation Workflow at a Glance' flowchart diagram has been removed. ▪ Appendix A, "P2PE Domain Responsibility Scenarios," has been removed.	Restructure
Entire Document		▪ All references to Domains were updated throughout the document as applicable based on the revised numbering of 1 through 5. ▪ Domain 4 for Merchant-managed Solutions has been moved to (replaced the existing) Appendix A. As a result, the Domains were renumbered, with Domain 5 becoming Domain 4 and Domain 6 (plus Annex A and B) becoming Domain 5.	Restructure
Merchant as a Solution Provider/Merchant-managed Solution		Domain 4 for Merchant-managed solutions was moved to (replaced) Appendix A. This section was updated to replace references to Domain 4 with Appendix A as well as to reference the new Domain numbering of 1-5.	Restructure
N/A	Scope of Assessment	New section added.	Additional Guidance

P2PE v2.0	P2PE v3.0	CHANGE	TYPE
Definition of Secure Cryptographic Devices (SCDs) to be used in P2PE Solutions		Clarified (by adding) context regarding signing P2PE Applications, non-payment software, and whitelists.	Clarification
P2PE Solutions: Hardware Decryption or Hybrid Decryption		Removed text box regarding Hardware/Hardware and Hardware/Hybrid.	Removal
SCD Domain Applicability		▪ Added context for FIPS 140-3, as well as clarified (by adding) context for software and whitelist signing. ▪ Added emphasis on scope of assessing an SCD.	Evolving and Clarification
P2PE Solutions and Use of P2PE Applications and/or P2PE Non-payment Software		Assessment and validation context removed and moved to Program Guide.	Removal and Restructure
Alignment of P2PE Requirements with Entities Offering P2PE Services	N/A	Section has been removed and will be captured in the P2PE Program documents.	Removal and Restructure
Relationship between P2PE and other PCI Standards		Removed references to PA-DSS and added context for *FIPS 140-3.*	Removal and Evolving
P2PE Program Guide		▪ Changed context of “Designated Change” to “Delta Change.” ▪ Added context regarding Merchant-managed solutions (MMS).	Evolving and Clarification
At-a-glance P2PE Workflow and Implementation Diagrams		▪ Removed the diagram “P2PE Solution and/or Component Validation Workflow at a Glance.” ▪ Updated diagram “Example P2PE Implementation at a Glance” with revised domain renumbering structure.	Removal and Restructure
N/A	Technical Reference Section	New: A technical reference section has been added.	Additional Guidance

P2PE v2.0	P2PE v3.0	CHANGE	TYPE
DOMAIN 1			
Overview		▪ Minor revisions. ▪ Clarified (by adding) context regarding Domain 5 applying to SCDs used for signing non-payment software as well as the associated cryptographic keys and key management.	Clarification
1A-1.x, 1A-2.x		Clarified scope regarding clear-text account data	Clarification
1B-1.1		▪ Minor restructuring of requirement. ▪ Added context of POI vendor default passwords. ▪ Removed test procedure 1B-1.1.c.	Clarification, Evolving, and Restructure
1B-2.1 1B-2.2		Changed context of two-factor to multi-factor. Added clarity to note regarding remote access to a terminal management system (TMS) or similar system.	Clarification and Evolving
1B-2.4.x	1B-2.5x	Renumbered as follows: ▪ 1B-2.4.1 to 1B-2.5 ▪ 1B-2.4.2 to 1B-2.5.1 ▪ 1B-2.4.3 to 1B-2.5.2	Restructure
1B-3.1		Clarified (by changing) context of “authentication” to “verification.”	Clarification
1B-3.2		▪ Added a note listing the minimum elements of a “system build.” ▪ Removed test procedure 1B-3.2.c.	Additional Guidance
1B-3.4	N/A	Requirement removed.	Removal
1B-3.5	1B-3.4	1B-3.5 renumbered to 1B-3.4.	Restructure
1B-5.1		Test procedure 1B-5.1.c added.	New
1C-1.1	N/A	Requirement removed.	Removal
1C-1.2x	1C-1.1x	Requirements 1C-1.2 (and its sub-requirements) renumbered to 1C-1.1 and 1C-1.1.x.	Restructure

P2PE v2.0	P2PE v3.0	CHANGE	TYPE
1C-2		▪ Clarified context to note regarding requirements in Domain 5 applying to the SCD used for signing non-payment software as well as the associated cryptographic keys and key management. ▪ Clarified scope of clear-text account data.	Clarification
1C-2.x		▪ Clarified context by changing "application" to "non-payment software." ▪ Clarified context of using an SCD for signing.	Clarification
1D-1.1		Modified note to account for the "Delta Change" process detailed in the Program Guide.	Clarification
1D-1.2.1	N/A	Removed requirement.	Removal
1D-1.2.2	1D-1.2.1	Renumbered 1D-1.2.2 to 1D-1.2.1.	Restructure
1D-1.3	N/A	Removed requirement.	Removal
1D-1.4	1D-1.3	Renumbered 1D-1.4 to 1D-1.3.	Restructure
1E-1.1		Clarified context of "merchant location."	Clarification
DOMAIN 2			
Overview		Revised note removing references to PA-DSS and clarifying intent.	Evolving
2A-2.1, 2A-3.2		Clarified intent.	Clarification
2B-1.1.1		Clarified test procedure 2B-1.1.1.	Clarification
2B-4, 2B-4.1		▪ Removed Note under 2B-4. ▪ Added new note to 2B-4.1 and clarified intent of requirement.	Removal, Clarification, and Additional Guidance
N/A	2B-4.2	Added new Requirement 2B-4.2.	New
2C-2.1.2		Clarified intent regarding use of an SCD.	Clarification
DOMAIN 3			
3A-3.3		Added context of retention duration.	Evolving
3A-4x	N/A	3A-4 (including all sub-requirements) has been removed.	Removal

P2PE v2.0	P2PE v3.0	CHANGE	TYPE
3B-1.2		Clarifications added.	Clarification
DOMAIN 4			
Domain 4	Appendix A	Domain 4 for merchant-managed solutions (MMS) has been moved to Appendix A, replacing the existing Appendix A "P2PE Domain Responsibility Scenarios" in its entirety.	Restructure
DOMAIN 5			
Domain 5	Domain 4	▪ Domain 4 is now "Domain 4: Decryption Environment." ▪ Domain 4 for merchant-managed solutions (MMS) has been moved to Appendix A, replacing the existing Appendix A "P2PE Domain Responsibility Scenarios" in its entirety. ▪ All of v2 Domain 5 was renumbered to v3 Domain 4. All requirement references are essentially identical with the exception they are now preceded by a "4" instead of a "5."	Restructure
5A-1.1	4A-1.1	▪ Added context clarifying that approval listings must not be expired. ▪ Added context for FIPS 140-3.	Evolving
5A-1.1.3	4A-1.1.3	Added context to test procedure to check POI listing for implementation specific notes.	Evolving
5B-1.1	4B-1.1	Removed test procedure 5B-1.1.c.	Removal
5B-1.4	4B-1.4	Clarified intent and modified context.	Clarification and Evolving
At a Glance – Example P2PE Hybrid Decryption Implementation		Revised graphic to capture revised domain numbering.	Restructure
5D-1.14.4	4D-1.14.4	Revised context.	Evolving
5D-2.2	4D-2.2	Added note regarding password strength/complexity.	Additional Guidance

P2PE v2.0	P2PE v3.0	CHANGE	TYPE
DOMAIN 6			
Domain 6	Domain 5	▪ V2.0 Domain 5 content regarding the Decryption Environment was moved (renumbered) to Domain 4 in v3.0. ▪ Therefore, Domain 5 now contains the entirety of what was in Domain 6 plus Annexes A and B. In addition, Annex A and Annex B have been removed and all the "unique" requirements in both Annexes are now in Domain 5. ▪ All the requirements from Domain 6 that are now in Domain 5 that originate from the PCI PIN Standard have been renumbered identically to match between the P2PE and PIN Standards.	Restructure
Applicability of Domain 6 and Annexes to P2PE Solution Providers and Component Providers	N/A	Table removed.	Removal
Definitions and Annexes	Definitions and Annex	▪ Context regarding Annex A and Annex B has been removed. ▪ Annex C remains.	Restructure and Removal
6B-1.1	5-1	▪ Clarified that key generation must occur within an SCD. ▪ Added context for FIPS 140-3. ▪ Revised test procedure "c."	Clarification
6B-2.1.1	6-1.1	Clarified intent with revised wording.	Clarification
6B-2.1.2	6-1.2	Clarified context of key generation and revised guidance in the note.	Clarification
6B-2.1.3	6-1.3	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.	Evolving

P2PE v2.0	P2PE v3.0	CHANGE	TYPE
6B-2.1.4	6-1.4	▪ 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. ▪ Added additional guidance note.	Clarification, Evolving, and Additional Guidance
6B-2.2	6-2	▪ 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.	Clarification
6B-2.3	6-3	▪ 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. ▪ Clarified that printers used for printing key components must not be networked. ▪ Added context that printers used for printing key components must be managed under dual control, including use of a secure room.	Clarification and Evolving
6B-2.6	6-6	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.	Clarification
6B-3.2	7-2	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.	Evolving
6C-1.1	8-1	Clarified that it is the responsibility of both the sending and receiving parties to ensure these keys are managed securely during transport.	Clarification

P2PE v2.0	P2PE v3.0	CHANGE	TYPE
6C-1.4	8-4	Clarified that self-signed root certificates protect the integrity of the data within the certificate but do not guarantee the authenticity of the data.	Additional Guidance
6C-2	9	Clarified this requirement also applies to keys moved between locations of the same organization.	Clarification
6C-2.2	9-2	Clarified that key-compromise process involves both a documented analysis and confirmation.	Clarification
N/A	9-6	Added requirement for when components or shares of multiple keys are being sent simultaneously between the same sending and receiving custodians.	New
6C-3.1	10-1	▪ Fixed error in v2.0 for double-length key context. Only triple-length keys are allowed as indicated in Annex C. ▪ Added an additional test procedure	Clarification
6C-3.2	N/A	Removed due to redundancy with 6C-3.1 (now 10-1).	Removal
6C-3.3	N/A	Removed due to redundancy with 6A-1.1 (now 5A-1.1).	Removal
6D-1.1	12-1	Added new test procedure.	New
6D-1.2	12-2	Added additional context to test procedure “a.”	Evolving
6D-1.3	12-3	▪ 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.	Clarification and Additional Guidance
6D-1.5	12-5	Removed allowance for double-length MFKs.	Evolving
6D-1.7	12-7	Added context for AES DUKPT.	Evolving

P2PE v2.0	P2PE v3.0	CHANGE	TYPE
6D-2.2	13-2	▪ Added context that keyboards attached to an HSM shall never be used for the loading of clear-text secret or private keys or their components. ▪ Added note regarding replacing or disabling firmware and modified PEDs being managed in accordance with 13-9. ▪ Added test procedure "b."	Evolving, Additional Guidance, and New
6D-2.3	13-3	Added test procedure "c."	New
6D-2.4.1	13-4.1	Added note regarding PCI-approved KLDs.	Additional Guidance
6D-2.4.2	13-4.2	Added note regarding insufficient means to meet the requirement.	Additional Guidance
6D-3.1	14-1	Added context of authentication codes.	Clarification
6D-3.2	14-2	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). Added two future dated restrictions: ▪ **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.	Clarification and Evolving
6D-4.1	15-1	Added key-check value method that is optional for TDEA keys and mandatory for AES keys.	Additional Guidance
N/A	18-3	New requirement with phased implementation dates for key blocks.	New
6E-2.4	18-4 18-6	V2.0 used duplicate numbers for the different requirements below—this has been fixed by: ▪ 6E-2.4 in Annex B is now 18-4. ▪ 6E-2.4 in Annex A1 is now 18-6.	Restructure

P2PE v2.0	P2PE v3.0	CHANGE	TYPE
6E-2.5	18-5 18-7	V2.0 used duplicate numbers for the different requirements below—this has been fixed by: ▪ 6E-2.5 in Annex B is now 18-5. ▪ 6E-2.5 in Annex A1 is now 18-7.	Restructure
6E-3.1	19-1	Added context regarding derivation keys.	Evolving and Clarification
6E-3.2	19-2	Added context that private keys used for remote key distribution shall not be used in connection with any other purpose.	Clarification
6E-4.3	20-3	Added note to clarify 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.	Clarification
6E-4.4	20-4	Revised test procedure.	Clarification
6F-1	21	Added note to clarify 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.	Additional Guidance
6F-2	22	Added “key determined to be compromised” instead of “known or suspected compromise key.”	Clarification
6F-2.1	22-1.3	Added clarification to existing note.	Clarification
6F-5.1.4	25-1.4	Specified additional criteria for key custodians.	Evolving
6F-6.1	26-1	Added context that key-component logs must include the name and signature of a non-custodian (for that component/share) witness.	Evolving
6F-8.1	28-1	Clarified security-training requirements for key custodians.	Clarification
6G-1.1.1	29-1.1	Clarified intent regarding compromise.	Clarification
6G-1.1.1.1	29-1.1.1	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.	Evolving

P2PE v2.0	P2PE v3.0	CHANGE	TYPE
6G-1.3	29-3	Added an additional option for implementing physical protection of devices from the manufacturer's facility up to the point of key insertion and deployment.	Evolving
6G-3.1	31-1	Clarified that requirement for irrecoverable deletion of keys and keying material stored within SCDs removed from service applies to private and secret keys.	Clarification
6G-3.1.1	31-1.1	Added new note regarding dual control and the use of a "zeroize" type physical mechanism.	Evolving
6G-4.1.1	32-1.1	Added additional clarification and context to existing note.	Evolving
ANNEX A			
Domain 6 Normative Annex A: Symmetric-Key Distribution using Asymmetric Techniques	Domain 5	▪ Annex A (both A1 and A2) has been moved to and incorporated within Domain 5 as part of the Domain renumbering and restructuring. There is no longer an Annex A (neither A1 nor A2) in v3.0. ▪ The preamble text (now) in Domain 5 has been clarified that the symmetric-key distribution using asymmetric techniques requirements do not apply if the key loading is not performed remotely and authentication is provided by another method. ▪ Added additional guidance regarding *ANSI TR-34* as a methodology that is compliant with these requirements.	Restructure, Clarification, and Additional Guidance
6C-3.2	N/A	Removed due to redundancy with 6C-3.1 (now 10-1)	Removal
6D-4.3	15-3	Clarified in the note that authentication mechanisms may include ensuring the SCD serial number is listed in a table of "permitted" devices.	Clarification
6E-3.9.2	19-9.2	Clarified that a CA cannot sign certificates to both subordinate CAs and end-entity (POI) devices.	Clarification

P2PE v2.0	P2PE v3.0	CHANGE	TYPE
6E-3.12	19-12	Rewrote 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.	Clarification and Evolving
6F-1.4	21-4	Clarified context of using an SCD as well as key shares.	Clarification
6F-2.8	22-5	Updated requirement incorporating future dated requirement requiring 2048-bit RSA as the date is past.	Evolving
6F-5.2	25-2	Clarified that individual user IDs may be assigned to a role or group.	Clarification
6F-5.3.2 6F-5.3.3 6F-5.3.4	25-3.2 25-3.3 25-3.4	Clarified where requirements apply to CAs operated online.	Clarification
6F-5-8.3	25-8.3	Added context for *NIST SP800-63b.*	Evolving
6G-3.4	32-4	Modified to reflect that non-CA personnel must sign an access logbook when entering the Level 3 environment.	Clarification
6G-3.7.1	32-7.1	Added additional context regarding recording events and documentation.	Evolving
ANNEX B			
Domain 6 Normative Annex B: Key-Injection Facilities	Domain 5	Annex B has been moved to and incorporated within Domain 5 as part of the Domain renumbering and restructuring. In addition, the redundant requirements that were in both Domain 6 and Annex B have been removed—any KIF-specific context from Annex B has also been incorporated into Domain 5. There is no longer an Annex B in v3.0.	Restructure

P2PE v2.0	P2PE v3.0	CHANGE	TYPE
6A-1.2	1-2	Condensed requirement wording.	Clarification
6A-1.3	1-3	▪ Added context for FIPS 140-3. ▪ 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.	Additional Guidance
6A-1.4	1-4	Added context of getting approval numbers as well as reviewing the approval listings for any implementation-specific notes.	Evolving
6A-1.5	1-5	Clarified intent of requirement.	Clarification
6C-3.1	10-1	Clarified that key-conveyance requirements apply to between locations or systems within the same key-injection facility.	Clarification
6D-2.9	13-9	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.	Evolving
6G-1.2	29-2	Added note to clarify 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.	Additional Guidance
6G-1.4.2	29-4.2	Added context for existence of documentation of HSM configuration settings.	Evolving

P2PE v2.0	P2PE v3.0	CHANGE	TYPE
6G-4.10	32-9	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.	Evolving and New
6G-4.10.1	32-9.1	Added new note regarding secure rooms.	Evolving and New
N/A	32-9.12	Added new requirement for the retention of CCTV images.	New
ANNEX C			
Domain 6 Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms		Footnote “4” content has been clarified regarding scope, as well as applicability to base derivation keys (BDKs).	Clarification
APPENDIX A			
Appendix A		▪ V2.0 Appendix A content “P2PE Domain Responsibility Scenarios” has been removed in its entirety. ▪ Appendix A in v3.0 now consists of the v2.0 Domain 4 content for merchant-managed solutions. ▪ MMS requirements in v3.0 Appendix A are essentially identical as in v2.0 with the exception they are now preceded with an “MM-“ instead of a leading “4”—e.g., “4A-1” is now “MM-A-1.”	Restructure