Payment Card Industry (PCI)

PTS POI Security Requirements

Summary of Changes from PCI PTS POI Version 5.0 to 5.1

March 2018

PCI PTS POI Summary of Changes

This document provides a summary of changes to the PTS POI version 5.0 family of documents from version 5.0 to version 5.1. Section 1 below provides an overview of the types of changes included in Version 5.1. Section 2 on the following pages provides a summary of material changes.

Section 1: Documents and Change Types

Abbreviation	Document Title
SR	*PCI PTS POI Modular Security Requirements*
DTR	*PCI PTS POI Modular Derived Test Requirements*
VQ	*PCI PTS POI Modular Evaluation Vendor Questionnaire*
PG	*PCI PTS POI Device Testing and Approval Program Guide*

Change Type	Definition
Additional Guidance	Explanation, definition, and/or instruction to increase understanding or provide further information or guidance on a particular topic.
Requirement Change	To reflect the addition or modification or deletion of requirements.

Note: *The changes above do not include those that are corrections of grammar or typographical errors or other rephrasing of existing statements.*

Section 2: Summary of Material Changes

Document and Reference	Change	Type
Security Requirements		
SR – Related Publications	Added additional ANSI and NIST reference documents.	Additional Guidance
SR – Required Device Information	Added check box for new Secure Card Reader PIN (SCRP) approval class.	Additional Guidance
SR – Evaluation Module Information	Split out Key Management – PIN Encryption between TDEA and AES.	Additional Guidance
SR – D1	Stipulated that new SCRP approval class requires an attack potential of 26 for identification and initial exploitation, with a minimum of 13 for exploitation.	Requirement Change
SR – K24	Added new requirement for secure enablement tokens required from the Software-based PIN on COTS (SPoC) monitoring system for operation of the SCRP.	Requirement Change
SR – Appendix B	Amended Applicability of Requirements for new SCRP approval class.	Additional Guidance
SR – Glossary	Added “Authentication Code,” “Commercial off-the-shelf (COTS),” ” Key-distribution host (KDH),” “Monitoring System,” “Monitor Token,” “SCRP,” and “SPoC”. Modified “Check Value.”	Additional Guidance
Derived Test Requirements		
DTR – General	Made additional modifications to introduction and throughout test steps to define report and testing expectations and to harmonize language.	Additional Guidance
DTR A1	Added additional guidance: *SCRPs must be capable of providing information to a query from the payment application to indicate if in a tamper state.* Added additional test step for physical protections of microprocessors.	Additional Guidance/ Requirement Change
DTR A4	Modified and added additional detail to test steps for use of acoustic capture in determining PIN data.	Additional Guidance

Document and Reference	Change	Type
DTR A5	Added additional guidance and a test step to reflect: *SCA tests shall be performed in accordance with Appendix F including the scope of side-channel testing necessary to validate the device's compliance based on the identification of relevant keys below and taking into consideration the appropriateness of testing re-use and demonstrably effective countermeasures.*	Additional Guidance
DTR A8	Modified and added additional detail to test steps for MSR testing, including combined ICCR/MSR readers and for attacks installing a second MSR reader.	Additional Guidance
DTR B1	Added clarification to guidance: *The device must perform an internal self-test automatically at least once every day, in addition to power-up (excludes wake-up from hibernation mode).*	Additional Guidance
DTR B2/K13	Added additional test step to clarify expectation for usage of ASLR.	Additional Guidance
DTR B3/K10	Added additional guidance for code considered firmware for SCRs and SCRPs: *Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware under PCI requirements, except for SCRs intended for use with COTS devices and SCRPs, where all code is considered firmware.*	Additional Guidance

Document and Reference	Change	Type
DTR B4/K12	Added additional guidance and a test step for information that must be provided by SCRs used with COTS devices and for SCRPs, and how that information must be secured during conveyance: *For SCRPs and SCRs intended for use with commercial-off-the-shelf devices—e.g., mobile phones and tablets—the SCRPs and SCRs must respond with their model name/number, hardware version, firmware version(s), and a unique device identifier to a query from the payment application on the COTS device.* *If done between physically and logically disparate components it must use a secure channel as follows:* ▪ *Each secure channel must provide mutual authentication to uniquely identify each component prior to exchanging sensitive data, as well as protect against MITM and replay attacks.* ▪ *Mutual authentication between the communicating components must be based on cryptography that aligns with Appendix E of this document, "Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms."* ▪ *Cryptographic keys used to establish secure channels between components and for data encryption must be unique, except by chance.*	Additional Guidance
DTR B5	Added additional guidance for touchscreens: *Digit presses on touch-screen devices should never be displayed.*	Additional Guidance
DTR B9	Added additional guidance and modified test step for use of SCRP for entropy: *B9 is mandatory for the SCRP approval class in order to provide a source of entropy for the payment application. It is a requirement that any random numbers used on the COTS device for security purposes must be seeded from a value provided from the RNG on an external SCRP.*	Additional Guidance

Document and Reference	Change	Type
DTR B11/K17	Added guidance from existing FAQs and added test steps for remote key distribution using asymmetric techniques. Added test step for cryptographic keys used by SCRP in provisioning process, including that SCRPs shall only support encrypted key loading methods.	Additional Guidance/ Requirement Change
DTR B12	Added additional guidance and test steps for PIN-block formats and key-management techniques required or additionally allowed to be used by SCRPs.	Additional Guidance/ Requirement Change
DTR B20	Added additional guidance: *The Security policy should include the following sections:* ▪ *General Description (DTRs B20.2 – B20.6)* ▪ *Installation and Guidance (DTRs B20.7–B20.18)* ▪ *Operation and Maintenance (DTRs B20.19 – B20.27)* ▪ *Security (DTRs B20.28 – B20.33)* *This is the minimum information that must be presented. Additional information may be presented.* *See Appendix H for an example of an acceptable Security Policy layout.*	Additional Guidance
DTR D1	Added requirements for SCRP to test step, indicating attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for exploitation.	Requirement Change
DTR D4	Added additional guidance for PIN blocks used with SCRP: *For an SCRP, this requirement is applied without consideration of the conveyance of the PIN from the payment application on the COTS device. The conveyance of the PIN from the payment application on the COTS device to the SCRP shall always use ISO format 4 for that conveyance.* *SCRPs with ICCRs shall support both enciphered and plaintext PIN for offline PIN authentication.*	Additional Guidance

Document and Reference	Change	Type
DTR F1	Added additional guidance for open protocol interfaces: *Where the interface is supplied by an OEM module:* ▪ *If the module is under the control of the firmware and runs in the same space as the firmware, the OEM interface module must still be assessed to ensure that secure pairing (for wireless technologies listed above) is provided for and that secure communications is enforced by the interface.* ▪ *If an independent OEM module is used:* – *The protocol and the pairing mechanism must be assessed; and* – *The security of the link between the module and the firmware must be assessed.* ▪ *If the OEM module shares resources with the rest of the device, a vulnerability assessment is required to ensure that the OEM module cannot adversely impact the function of the device.* *OEM modules that are found to have unaddressed exploitable vulnerabilities may result in the removal of the entire POI device approval.* ***Note:** If the device implements an IP stack, the device must support TLS 1.2 or higher. When the TLS protocol is supported, this needs to be evaluated under Section I, "Operational Testing" and corresponding PCI Technical FAQs.*	Additional Guidance
DTR H3	Added additional guidance for key management used with open protocols: ***Note:** This does not supersede any criteria in B11 or K17 but rather is required for any device implementing protocols evaluated under Open Protocols—i.e., key-related Security Protocols, such as SSL/TLS, SSH, VPN technologies.* *This requirement applies to all declared Security Protocols defined in Section F1.*	Additional Guidance
DTR K1	Added additional guidance prohibiting whitelists for SCRs used with COTS devices and SCRPs: *An SCR intended for use with a COTS device or an SCRP shall not release account data in the clear, even via a whitelist mechanism.*	Additional Guidance

Document and Reference	Change	Type
DTR K1.1	Added additional guidance for analysis of ICCRs: *DTRs A1.8, A1.11, and A1.13 must be completed for the ICCR where any specific references to "PIN" are to be read as "account data."* Modified test step to call out testing for contactless and manual PAN entry.	Additional Guidance
DTR K4	Added guidance from existing FAQs on key management for SRED: *Double-length TDES keys used in connection with SRED can only be used in unique-key-per-transaction implementations as defined in ISO 11568 for key derivation or transformation—e.g., DUKPT. Double-length TDES keys are not permitted for use in SRED in Master/Session or Fixed key implementations.*	Additional Guidance
DTR K11.2	Added guidance and test step on documentation and usage of APIs: *The vendor must provide to the PCI PTS laboratory a guidance document that states the exact scope of the PTS evaluated firmware (down to the level, including version, of libraries and binaries). This shall include all security-relevant APIs to confirm that they are used by the application rather than the application using its own cryptographic primitives and key management.*	Additional Guidance/ Requirement Change
DTR K16	Added additional guidance for use of surrogate PANs by SCRPs: *SCRPs must tokenize the PAN data to send to the payment application on the COTS device for use in formatting the ISO format 4 PIN block. An example of an acceptable PAN token is one described in ANSI X9.119-2 using a format-preserving scheme.*	Additional Guidance
DTR K24	Added test steps for new requirement for secure enablement tokens required from the Software-based PIN on COTS (SPoC) monitoring system for operation of the SCRP.	Requirement Change
DTR – Appendix A1.1	Added clarification text on use of polarizers in touchscreens.	Additional Guidance
DTR – Appendix F	Added additional clarification for side channel analysis testing.	Additional Guidance
DTR – Appendix H	New appendix with Security Policy Template.	Additional Guidance

Document and Reference	Change	Type
Vendor Questionnaire		
VQs – Sections A, B, D, and K and Annex A	New and modified questions in support of changes and additions in DTRs enumerated above.	Additional Guidance/ Requirement Change
Program Guide		
PG – Section 1	Modified *Related Publications* text.	Additional Guidance
PG – Section 2	Modified the Device Management Requirements text to be consistent with SR and DTR documentation.	Additional Guidance
PG – Section 3	Added a reporting requirement for PTS vendors on firmware maintenance and modifications: *As of 1 May, the vendor must complete and submit to PCI an Attestation of Validation (AOV) confirming adherence to the program guide—i.e., either the firmware has not been amended or the changes made are within the wildcard parameters or the changes were submitted for evaluation. For devices supporting open protocols, the vendor must provide evidentiary materials that an auditable record of an ongoing vulnerability assessment process exists by providing a copy of the vendor's sign-off form specified in Requirement G1. This applies to all unexpired approvals that exist for the vendor as of 31 December of the prior year. Failure to submit the annual AOV means further report submissions by the vendor will not be processed. An AOV is not required for devices that are End of Life as enumerated in Section 5.*	Requirement Change
PG – Section 10	Added acronym definitions for COTS, SCR, SCRP, SPoC, and SRED.	Additional Guidance
PG – Appendix A	▪ Modified SCR approval class description. ▪ Added SCRP approval class description. ▪ Stipulated approval expiry for SCRPs as five years after date of approval. ▪ Specified that for new approvals, SCRPs must always use the most current version of the Security Requirements. ▪ Added SCRP to *Specific Features per Approval Class.* ▪ Added FAQ text for requiring ISO Format 4 PIN blocks on POI v4.	Additional Guidance

Document and Reference	Change	Type
PG – Appendix D	Added reporting form for existing requirement on firmware maintenance and modifications.	Requirement Change