Payment Card Industry (PCI)

PTS POI Security Requirements

Summary of Changes from PCI PTS POI Version 3.1 to 4.0

June 2013

Document and Requirements Reference[1]	Page	Change	Type[2]
SR General	4	Purpose section – Added text describing version 4: *This version 4 additionally provides for:* • *Submission by the vendor for assessment and publication on the PCI website of a user-available security policy addressing the proper use of the POI in a secure fashion, as further delineated in requirement B20.* • *Greater granularity and robustness of the underlying PCI-recognized laboratory test procedures for validation compliance of a device to these requirements as detailed in the Derived Test Requirements.*	Additional Guidance
SR General	5	Main Differences from Prior Version Section updated. • *The reordering of the Core Physical Security Requirements* • *The restructuring of the Open Protocols module* • *The addition of a requirement for the vendor to provide a user-available security policy that will facilitate implementation of an approved POI device in a manner consistent with these requirements, including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements*	Additional Guidance
SR General	6	Modified process flow to include contactless readers.	Additional Guidance
SR General	8	Updated references in Related Publications	Additional Guidance
SR General	9-13	Modified Required Device Information. Optional Use of Variables and Evaluation Module Information sections for clarification of desired information.	Additional Guidance
SR Section A	15-17	Modified numbering and sequence of Core Physical Security Requirements.	Requirement change

Document and Requirements Reference[1]	Page	Change	Type[2]
SR A3 – version 3	-	Deleted v3 requirement A3 as redundant to other testing: *If the device permits access to internal areas (e.g., for service or maintenance), it is not possible using this access area to insert a bug that would disclose sensitive data. Immediate access to sensitive data such as PIN or cryptographic data is either prevented by the design of the internal areas (e.g., by enclosing components with sensitive data into tamper-resistant/responsive enclosures), and/or it has a mechanism so that accessing internal areas causes the immediate erasure of sensitive data.*	Requirement change
SR A7, B16 and E3.4	16, 19, 24	Modified text describing applicability of the display prompt control requirements.	Additional Guidance
SR B1	18	Added the highlighted text and rephrased the preceding text: *The device performs a self-test, which includes integrity and authenticity tests upon start-up and at least once per day to check whether the device is in a compromised state. In the event of a failure, the device and its functionality fail in a secure manner. The device must reinitialize memory at least every 24 hours.*	Requirement change
SR B4.1		Added a new Core requirement. Requirement previously existed only in K11.1: *The firmware must support the authentication of applications loaded onto the terminal consistent with B4. If the device allows software application and/or configuration updates, the device cryptographically authenticates updates consistent with B4.*	Requirement change
SR B16	20	Consolidated B16.1 and B16.2 into a single requirement addressing both acquirer and vendor controlled prompts that are updatable	Requirement change

Document and Requirements Reference[1]	Page	Change	Type[2]
SR B20	20	New Requirement - *A user-available security policy from the vendor addresses the proper use of the POI in a secure fashion, including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements. The security policy must define the roles supported by the POI and indicate the services available for each role in a deterministic tabular format. The POI is capable of performing only its designed functions, i.e., there is no hidden functionality. The only approved functions performed by the POI are those allowed by the policy.*	Requirement change
SR D4	22	Consolidated D4.1, D4.2, D4.3 and D4.4 into a single comprehensive requirement: *If the device encrypting the PIN and the ICC reader are not integrated into the same secure module, and the cardholder verification method is determined to be:* • *An enciphered PIN, the PIN block shall be enciphered between the device encrypting the PIN and the ICC reader using either an authenticated encipherment key of the IC card, or in accordance with ISO 9564.* • *A plaintext PIN, the PIN block shall be enciphered from the device encrypting the PIN to the ICC reader (the ICC reader will then decipher the PIN for transmission in plaintext to the IC card) in accordance with ISO 9564.* *If the device encrypting the PIN and the ICC reader are integrated into the same secure module, and the cardholder verification method is determined to be:* • *An enciphered PIN, the PIN block shall be enciphered using an authenticated encipherment key of the IC card.* • *A plaintext PIN, then encipherment is not required if the PIN block is transmitted wholly through a protected environment (as defined in ISO 9564). If the plaintext PIN is transmitted to the ICC reader through an unprotected environment, the PIN block shall be enciphered in accordance with ISO 9564.*	Requirement change

Document and Requirements Reference[1]	Page	Change	Type[2]
Open Protocols Module	26-31	Realigned and rephrased Open Protocol Module to align the testing by function as opposed to protocol specific.	Requirement change
SR H10 – version 3	-	Deleted v3 requirement H10 and specified compliance in Core requirement B9. *The security protocol makes use of a random generator that has been validated against NIST SP 800-22 or equivalent.*	Requirement change
SR K1.2	32	Split out separate requirement from existing requirement K1.1: *Failure of a single security mechanism does not compromise device security. Protection against a threat is based on a combination of at least two independent security mechanisms*.	Requirement change
SR K11 - version 3	-	Deleted requirement and specified compliance in Core requirement B1: *The device performs self-tests consistent with B1*.	Requirement change
SR K13	33	Rephrased: *The device's functionality shall not be influenced by logical anomalies consistent with B2.*	Requirement change
SR K14	33	K14 and K15 combined and rephrased to reflect new structuring of Open Protocols Module: *If the device is capable of communicating over an IP network or uses a public domain protocol (such as but not limited to Wi-Fi or Bluetooth), then requirements specified in DTR Module 3: Open Protocols Requirements have been met.*	Requirement change
SR K20 – version 3	-	Deleted in the same manner as requirement A3: *If the device permits access to internal areas (e.g., for service or maintenance), it is not possible using this access area to insert a bug that would disclose any secret or private keys or account data. Immediate access to secret or private keys or account data is either prevented by the design of the internal areas (e.g., by enclosing components with such data into tamper-resistant/responsive enclosures), and/or it has a mechanism so that accessing internal areas causes the immediate erasure of secret and private keys and account data.*	Requirement change
SR L2, L4, L5, L6 and L7	36-37	Minor updating of wording	Requirement change

Document and Requirements Reference[1]	Page	Change	Type[2]
SR M1	35	Requirement rewritten: *The POI should be protected from unauthorized modification with tamper-evident security features, and customers shall be provided with documentation (both shipped with the product and available securely online) that provides instruction on validating the authenticity and integrity of the POI.* *Where this is not possible, the POI is shipped from the manufacturer's facility to the initial key-loading facility or to the facility of initial deployment and stored en route under auditable controls that can account for the location of every POI at every point in time.* *Where multiple parties are involved in organizing the shipping, it is the responsibility of each party to ensure that the shipping and storage they are managing is compliant with this requirement.*	Requirement change
SR M2	35	Requirement rewritten: *Procedures are in place to transfer accountability for the device from the manufacturer to the facility of initial deployment. Where the device is shipped via intermediaries such as resellers, accountability will be with the intermediary from the time at which they receive the device until the time it is received by the next intermediary or the point of initial deployment.*	Requirement change
SR Appendix B: Applicability of Requirements	44-47	Modified to reflect aforementioned changes adding, moving and deleting requirements.	Additional Guidance
SR *Glossary*	48-58	Numerous additions to defined terms	Additional Guidance

Document and Requirements Reference[1]	Page	Change	Type[2]
DTR General	1-2	New Section added to define report and testing expectations **Minimal contents of reports and minimal test activities** All reports should include a separate POI report summary at the top. The summary should include: ▪ A device overview that summarizes the design and architecture and device features ▪ A review of the security-relevant features; including derivation of assets, threats and attacks ▪ A report summary that includes the tests (DTRs) performed with conclusions In support of some test steps, as directed by the test laboratory, the vendor must support the laboratory in various tasks (code review, fuzzing interfacing, DPA, etc.) to avoid prohibitively lengthy test activities. The vendor shall make source code available to the lab and provide assistance to make a systematic review of relevant security functions. Note that a copy of the Vendor Questionnaire shall be submitted to the Report Portal along with the test report and any other supporting documents including, where applicable, the *Open Protocols Module – Protocol Declaration Form.* For all DTRs, the tester shall state the following in writing: xxxxxx For all DTRs, the tester shall present sufficient information on direct tests and theoretical claims to validate conclusions. Every test should be supported by sufficient evidence for the evaluation conclusions placed in the report to be understood and confirmed. This includes but is not limited to: xxxxxx	

Document and Requirements Reference[1]	Page	Change	Type[2]
DTR A1	3-9	Added additional detailed steps and guidance for identification and testing of tamper protection mechanisms.	Additional Guidance
DTR A2	10	Clarified guidance: This requirement does not imply the need for redundant security mechanisms, but rather separate mechanisms of a different nature.	Additional Guidance
DTR A3	11-12	Added additional detailed steps and guidance for voltage and temperature extremes as a means to attack the device.	Additional Guidance
DTR A4	13-15	Added additional detailed steps to further identify locations of all types of sensitive information and functions and the adequacy of associated protection mechanisms.	Additional Guidance
DTR A5	16-17	Added additional detailed steps to identify if any characteristics (e.g., emanations) available for monitoring from the device can be used to obtain PIN data.	Additional Guidance
DTR A6	18-20	Added additional detailed steps and guidance for the determination of secret and private keys in the device using both physical means and the monitoring of emanations.	Additional Guidance
DTR A7	20-22	Added additional detailed steps for determination of the adequacy of physical protections of preventing alteration of display prompts	Additional Guidance
DTR A8	23-24	Added additional detailed steps for validation of visual observation deterrents.	Additional Guidance
DTR A9	25-26	Added additional detailed steps for validation of protections of the MSR from attacks to determine or modify magnetic stripe data	Additional Guidance
DTR A10	27-28	Added additional detailed steps for determining the adequacy of the EPP or ICCR's protections against Removal.	Additional Guidance
DTR A11	29	Added additional detailed steps for determining whether PINs can be determined during entry by audible tones.	Additional Guidance

Document and Requirements Reference[1]	Page	Change	Type[2]
DTR B1	30-31	Added additional detailed steps to validate the adequacy of self-tests for ensuring the authenticity and integrity of firmware, security mechanisms for signs of tampering, and whether the device is in a compromised state. Included former K11 from version 3 for Secure Reading and Exchange of Data and added Open Protocols code as applicable.	Additional Guidance
DTR B2	32-33	Added additional detailed steps to validate that the device's functionality is influenced by logical anomalies, including validation of all physical and logical interfaces.	Additional Guidance
DTR B3	34-36	Added additional detailed steps and guidance to validate the adequacy of the vendor's software development process for protecting the software from hidden and unauthorized or undocumented functions.	Additional Guidance
DTR B4	37-39	Added additional detailed steps to determine the adequacy of firmware authentication process.	Additional Guidance
DTR B5	43	Added additional detailed steps to assess protections against the differentiation of entered PIN data.	Additional Guidance
DTR B6	44-45	Added additional detailed steps to determine that internal buffers cannot be used to determine sensitive information.	Additional Guidance
DTR B7	46-48	Added additional detailed steps to validate device protections of sensitive services.	Additional Guidance
DTR B8	49-50	Added additional detailed steps to protect against the unauthorized use of sensitive services.	Additional Guidance
DTR B9	51-52	Added additional detailed steps and guidance to ensure it is generating numbers sufficiently unpredictable when used for security relevant functions. Scope now includes random numbers that are generated in connection with meeting requirements in the Open Protocols and Secure Reading and Exchange of Data Modules.	Additional Guidance/Requirement Change

Document and Requirements Reference[1]	Page	Change	Type[2]
DTR B10	53-54	Added additional detailed steps to validate the adequacy of device characteristics that prevent or significantly deter the use of the device for exhaustive PIN determination.	Additional Guidance
DTR B11	55-60,	Added additional detailed steps to validate the adequacy of key-management techniques	Additional Guidance
DTR B12	61-62	Added additional detailed steps to validate the PIN-encryption technique implemented	Additional Guidance
DTR B13	63-64	Added additional detailed steps to ensure that it is not possible to encrypt or decrypt any arbitrary data using any cryptographic key.	Additional Guidance
DTR B14	65	Added additional detailed steps to determine that clear-text PINs and clear-text cryptographic keys do not exist in unprotected environments.	Additional Guidance
DTR B15	66	Added additional detailed steps to validate that the entry of any other transaction data is separate from the PIN-entry process	Additional Guidance
DTR B16	67-69	Added additional detailed steps to validate the adequacy of the logical management of display prompts	Additional Guidance
DTR B17	70-72	Added additional detailed steps to ensure the device enforces the separation between applications	Additional Guidance
DTR B18	73-74	Added additional detailed steps to validate that the operating system contains only the software necessary for the intended operation and is configured securely and run with least privilege.	Additional Guidance
DTR C1	79	Added additional detailed steps to determine that the device prohibits unauthorized key replacement and key misuse	Additional Guidance
DTR D1	80-82	Added additional detailed steps to validate the ICCR's protections against the determination or modification of any sensitive data.	Additional Guidance
DTR D3	84	Added additional detailed steps to validate that the ICC reader is constructed so that wires running out of the slot can be observed	Additional Guidance

Document and Requirements Reference[1]	Page	Change	Type[2]
DTR D4	85-86	Added additional detailed steps to validate the PIN Protection During Transmission Between Device and ICC Reader	Additional Guidance
DTR E3.4	93-94	Added additional detailed steps to validate the user interface consistency	Additional Guidance
DTR E4.1	96-98	The device is protected against unauthorized removal	Additional Guidance
DTR K2	123	Added additional guidance for the logical and physical integration of a card reader into a PIN entry terminal.	Additional Guidance
DTR K3	124-126	Added additional detailed steps and guidance for the determination of secret and private keys in the device using both physical means and the monitoring of emanations	Additional Guidance
DTR K7	131	Added additional step to verify key uniqueness	Additional Guidance
DTR K8	132-133	Added additional detailed steps and guidance to validate that the device enforces that account data keys, key-encipherment keys, and PIN-encryption keys have different values and are appropriately used.	Additional Guidance
DTR K10	135-137	Added additional detailed steps and guidance to validate the adequacy of the vendor's software development process for protecting the software from hidden and unauthorized or undocumented functions.	Additional Guidance
DTR K11.1	138-140	Added additional detailed steps to validate that the firmware confirms the authenticity of all applications	Additional Guidance
DTR K12	142-144	Added additional detailed steps to determine the adequacy of firmware authentication process.	Additional Guidance
DTR K13	145-146	Added additional detailed steps to validate that the device's functionality is influenced by logical anomalies, including validation of all physical and logical interfaces.	Additional Guidance
DTR K15	148-149	Added additional guidance for the output of cleartext account data	Additional Guidance
DTR K15.2	151-152	Added additional detailed steps to determine that internal buffers cannot be used to determine sensitive information.	Additional Guidance

Document and Requirements Reference[1]	Page	Change	Type[2]
DTR K17	156-161	Added additional detailed steps to validate the adequacy of key-management techniques	Additional Guidance
DTR K19	163-164	Added additional detailed steps for voltage and temperature extremes as a means to attack the device.	Additional Guidance
DTR K20	165-166	Added additional detailed steps to ensure the device enforces the separation between applications	Additional Guidance
DTR K21	167-168	Added additional detailed steps to validate that the operating system contains only the software necessary for the intended operation and is configured securely and run with least privilege.	Additional Guidance
DTR K22	169-171	Added additional detailed steps to validate device protections of sensitive services.	Additional Guidance
DTR K23	172-173	Added additional detailed steps to protect against the unauthorized use of sensitive services.	Additional Guidance
DTRs B4.1, B20, K1.2, K14 and Open Protocols Module	Mult.	DTRs added/updated to reflect corresponding changes in Security Requirements as noted above.	Requirement change
DTR Appendix B	182-191	Updated attack calculation examples	Additional Guidance
DTR Appendix D	194	Added new Appendix to stipulate minimum and equivalent key sizes and strengths for approved algorithms	Additional Guidance
VQ General	vii	Updated references in Related Publications	
VQs Section A, B4.1, B16, B20, D4, Open Protocol Module, K14	Mult.	VQs added/updated/moved/deleted to reflect corresponding changes in Security Requirements as noted above.	Additional Guidance Requirement change
VQ A1, A3 thru A10	2-15	Additional questions reflecting more detailed DTR steps	Additional Guidance

Document and Requirements Reference[1]	Page	Change	Type[2]
VQ B1 thru B5, B7, B9, B11 thru B14, B17-B18	17-22, 24-25, 27, 28-33, 37-38	Additional questions reflecting more detailed DTR steps	Additional Guidance
VQ C1	40	Additional questions reflecting more detailed DTR steps	Additional Guidance
VQ D1, D2	41-43	Additional questions reflecting more detailed DTR steps	Additional Guidance
VQ K1.1, K3, K10, K12-13, K19-21	66-70, 73, 80, 82-84,92-94	Additional questions reflecting more detailed DTR steps	Additional Guidance
VQ Annex A: DTR Templates	99-102	New section added to capture information specified in the DTRs for use during laboratory evaluation	Additional Guidance
Annex B: Device Diagrams and Test Reports	103-	New section added to capture information specified in the DTRs for use during laboratory evaluation.	Additional Guidance

Document and Requirements Reference[1]	Definition
SR	PCI PTS POI Modular Security Requirements
DTR	PCI PTS POI Modular Derived Test Requirements
VQ	PCI PTS POI Modular Evaluation Vendor Questionnaire
Type[2]	**Definition**
Additional guidance	Provides clarification on intent of the requirement and additional guidance or information on the criteria applied.
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.	