

Payment Card Industry (PCI) PTS POI Security Requirements

Summary of Changes from PCI PTS POI Version 3.0 to 3.1

September 2011

Document and Requirements Reference ¹	Page	Change	Type ²
SR General	4,5,7,9	Added text to reflect additions of non-PIN acceptance devices and secure card readers as approval classes	Additional Guidance
SR General	6	Modified process flow to reflect additions of non-PIN acceptance devices and secure card readers as approval classes	Additional Guidance
SR <i>Evaluation Module 2: POS Terminal Integration</i> Introduction	23	Added text clarifying applicability of module	Additional Guidance
SR F4	25	Corrected requirement statement to correctly encompass link layer as in scope	Requirement change
The following requirements were added to the SRED module from the Core module to ensure coverage of these requirements for non-PIN acceptance POIs which are not required to go through the Core module.			
SR K12	34	If the device allows updates of firmware, the device cryptographically authenticates the firmware and if the authenticity is not confirmed, the firmware update is rejected and deleted.	Requirement change
SR K18	35	The key-management techniques implemented in the device are consistent with B11.	Requirement change
SR K20	35	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 K21	35	Environmental or operational conditions cannot be altered to compromise the security of the device, or cause the device to output clear-text account data. (An example includes subjecting the device to temperatures or operating voltages outside the stated operating ranges.)	Requirement change

Document and Requirements Reference ¹	Page	Change	Type ²
SR K22	35	If the device supports multiple applications, it must enforce the separation between applications consistent with B17.	Requirement change
SR K23	35	The following features of the device's operating system must be in place: <ul style="list-style-type: none"> ▪ The operating system of the device must contain only the software (components and services) necessary for the intended operation. ▪ The operating system must be configured securely and run with least privilege. ▪ The security policy enforced by the device must not allow unauthorized or unnecessary functions. ▪ API functionality and commands that are not required to support specific functionality must be disabled (and where possible, removed). 	Requirement change
SR K24	36	Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, account data, and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive data.	Requirement change
SR K25	36	Sensitive services are protected from unauthorized use consistent with B8.	Requirement change
SR K11.1	34	Combined prior K12 with K11.1 The firmware must confirm the authenticity of all applications loaded onto the terminal consistent with B4. If the device allows software application and/or configuration updates, the device cryptographically authenticates all updates consistent with B4.	Requirement change
SR K18 (old) – deleted to reflect addition of K24 and K25 above	35	If the device allows access to sensitive functions to support account data encryption, the access to this functionality must be protected using an authentication credential that is unique per device.	Requirement change

Document and Requirements Reference ¹	Page	Change	Type ²
SR L8	38	Controls exist over the repair process and the inspection/testing process subsequent to repair to ensure that the device has not been subject to unauthorized modification.	Requirement change
SR Glossary	49	Modified Secure Components definition to include protection of account data	Additional Guidance
SR Appendix B: Applicability of Requirements	44-7	Modified to reflect requirements applicable to the Secure Card Reader Approval Class	Additional Guidance
DTR B1	16	Synchronized guidance with FAQs on use of SHA-2 vs. SHA-1.	Additional Guidance
DTR B4	20	Added guidance for modules authenticating software.	Additional Guidance
DTR B11	29	Synchronized guidance with FAQs on allowed key loading mechanisms for unattended devices.	Additional Guidance
DTR B13	34	Synchronized guidance with FAQs on key uniqueness checking.	Additional Guidance
DTR B18	42	Added additional guidance on implementation of least privilege and what constitutes sensitive functionality	Additional Guidance
DTR D4	49	Synchronized guidance with FAQs on where authentication of public keys used for offline transactions must occur.	Additional Guidance
DTR E4.1	63-4	Added additional guidance and test validation steps for unauthorized removal detection.	Additional Guidance
DTR F4	70	Corrected requirement statement to correctly encompass link layer as in scope	Requirement change
DTR K1.1	96	Added guidance on protection of contactless account data	Additional Guidance
DTR K9	105	Added guidance on scope of requirement regarding remote access	Additional Guidance
DTR K11	107	Synchronized guidance with FAQs on use of SHA-2 vs. SHA-1.	Additional Guidance
DTR K19	126	Added guidance of PAN exhaustion attack prevention.	Additional Guidance
DTR Appendix B	145	Synchronized guidance with FAQs on use of parts in attack potential calculations.	Additional Guidance

Document and Requirements Reference ¹	Page	Change	Type ²
DTRs K11.1, K12, K18, K20, K21, K22, K23, K24, K25	Mult.	DTRs added/updated to reflect corresponding changes in Security Requirements as noted above.	Requirement change
VQ E4.1	47	Added question regarding whether the integrated devices possesses secure components previously assessed under A11.	Additional Guidance
VQs K11.1, K12, K18, K20, K21, K22, K23, K24, K25	Mult.	VQs added/updated to reflect corresponding changes in Security Requirements as noted above.	Requirement change

Document and Requirements Reference¹	Definition
SR	PCI PTS POI Modular Security Requirements
DTR	PCI PTS POI Modular Derived Test Requirements
VQ	PCI PTS POI Modular Evaluation Vendor Questionnaire
Type²	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 for the addition of non-PIN acceptance devices to testing or for additional general criteria not impacting testing
<p><i>Note: The changes above do not include those that are corrections of grammar or typographical errors or other rephrasing of existing statements.</i></p>	