Payment Card Industry (PCI)

PIN Transaction Security (PTS) Hardware Security Module (HSM)

Summary of Requirements Changes from Version 2.0 to 3.0

June 2016

Introduction

This document provides a summary of changes from the PCI PTS HSM Modular Requirements v2.0 to v3.0. Table 1 provides an overview of the types of changes included in Version 3.0. Table 2 provides a summary of material changes to be found in Version 3.0.

Document Abbreviations Used

Abbreviation	Document Referenced
SR / SRs	PCI PTS HSM Modular Security Requirements
DTR / DTRs	PCI PTS HSM Modular Derived Test Requirements
VQ	PCI PTS HSM Modular Vendor Questionnaire

Table 1: Change Types

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 modification, deletion, or restructuring of requirements

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

Table 2: Summary of Changes

Document and Requirements Reference	Change	Type
SR General, DTRs, and VQ	Added approval classes for key-loading devices and HSM remote administration platforms, together with supporting requirements, test scripts, and vendor questions.	Requirement Change
SR General	Added references to ISO 9797-1, ISO 18033-1, ISO 18033-5, NIST SP 800-38B, NIST SP 800-90A Revision 1, and NIST SP 800-131A Revision 1.	Additional Guidance
SR A2	Eliminated requirement for Independent Security Mechanisms and added guidance to SR A-1	Requirement Change
SR A3	Eliminated requirement for Response to Internal Access and added guidance to SR A-1	Requirement Change
SR B1	Added allowance for continuous error checking as an option to running self-tests at least once per day	Requirement Change
SR B4	Added requirement that devices must support firmware updates	Requirement Change
SR B4.1	Added new requirement for the firmware to authenticate applications loaded into the device consistent with B4, including updates and configuration changes.	Requirement Change
SR B8	Clarified enciphered key components can be treated the same as enciphered keys for key loading	Additional Guidance
SRs D1 – D5	Added Section D – Key-Loading Devices to support new approval classes.	Requirement Change
SRs E1 – E2	Added Section E – Remote Administration – Logical Security to support new approval classes.	Requirement Change
SRs F1 – F4	Added Section F – Devices With Message Authentication Capabilities to support new approval classes.	Requirement Change
SRs G1 – G4	Added Section G – Devices With Key Generation Functionality to support new approval classes.	Requirement Change
SRs H1 – H2	Added Section H – Devices With Digital Signature Functionality to support new approval classes.	Requirement Change

Document and Requirements Reference	Change	Type
SRs I1 – I8 and J1 – J8	The PCI test laboratories will now validate device management information via documentation reviews. Any variances to these requirements will be reported to PCI for review. However, this information will only be used for analysis at this time and will not impact whether a device receives an approval.	Requirement Change
SR J1	Clarified the device must be protected from unauthorized modification with tamper detection characteristics and is not restricted to just tamper evidence	Requirement Change
Appendices A and B	Added appendices to define applicability of requirements to approval classes for HSMs, key-loading devices, and remote administration platforms.	Additional Guidance
DTRs Introduction	Provided additional guidance for lab reporting criteria, including minimal contents of reports and minimal test activities.	Additional Guidance
DTRs Module 1: Core Requirements – Sections A, B, and C	Significantly enhanced test scripts based on leveraging applicable information from POI V4 and to support new approval classes.	Requirement Change
DTR A1	Eliminated ten hours minimum for exploitation time.	Requirement Change
DTR B1	Added additional guidance for how the HSM must detect hardware errors in order to prevent the return of incorrect results or the disclosure of sensitive information.	Additional Guidance
DTR B4.1	Added to support new requirement for software authenticity.	Requirement Change
DTR B9	Updated guidance to stipulate that PRNG designs (Deterministic Random Bit Generator, or DRBG) from NIST SP800-90A or ANSI X9.82 shall be used—specifically, HASH_DRBG, HMAC_DRBG or CTR_DRBG. DEA and 2-key TDEA, as well as DUAL_EC_DRBG are not acceptable for use in a DRBG.	Additional Guidance / Requirement Change
DTR B15	Updated to reflect new PIN translation options in ISO 9564 to reflect addition of criteria for AES PIN blocks and PAN Token translations.	Additional Guidance / Requirement Change

Document and Requirements Reference	Change	Type
DTR B15	Clarified that keys used to authenticate that it is a valid device or keys used to sign information like a device identifier may be shared between PCI and non-PCI modes	Additional Guidance
DTR C1	Updated to reflect additional required information to be included in the HSM security policy.	Requirement Change
DTR Sections D – H	Added to support new requirements for key-loading devices and remote administration platforms.	Requirement Change
DTR Module 4: Device Management Security Requirements	Added to support new requirement for the lab to validate this information via documentation reviews.	Requirement Change
DTR I1	Added stipulation that approval of delta submissions is contingent on evidence of an ongoing change control and vulnerability management process.	Requirement Change
DTR Appendix A	Updated Attack Costing Potential Formulas to reflect more granular approach for attack times and expertise	Additional Guidance
DTR Appendix B	Added new appendix detailing equipment classification for physical attack costing purposes for use with Appendix A	Additional Guidance
DTR Appendix C	Updated information on the configuration and use of the STS tool.	Additional Guidance
DTR Appendix D	Updated guidance on the use of Diffie-Hellman.	Additional Guidance
DTR Appendix E	Added new guidance for side channel analysis best practices	Additional Guidance
VQ	Modifications and additions to reflect changes above.	Additional Guidance