Payment Card Industry (PCI)

PIN Transaction Security (PTS) Point-of-Interaction (POI)

Summary of Requirements Changes from Version 4.1 to 5.0

September 2016

Introduction

This document provides a summary of changes from the PCI PTS POI Modular Requirements v4.1 to v5.0. Table 1 provides an overview of the types of changes included in Version 5.0. Table 2 provides a summary of material changes to be found in Version 5.0.

Document Abbreviations Used

Abbreviation	Document Referenced
SR / SRs	PCI PTS POI Modular Security Requirements
DTR / DTRs	PCI PTS POI Modular Derived Test Requirements
VQ	PCI PTS POI 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	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 B4	Added requirement that devices must support firmware updates	Requirement Change
SR K1.2	Eliminated requirement for Independent Security Mechanisms and added guidance to SR K-1.1	Requirement Change
SR K12	Added requirement that devices must support firmware updates	Requirement Change
SR M1	Clarified the device must be protected from unauthorized modification with tamper detection characteristics and is not restricted to just tamper evidence	Requirement Change
DTRs Introduction	Provided additional guidance for lab reporting criteria, including minimal contents of reports and minimal test activities.	Additional Guidance
DTRs – All Sections	Enhanced robustness of test scripts throughout	Requirement Change
DTR A1	Eliminated ten hours minimum for exploitation time.	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 B20	Updated to reflect additional required information to be included in the POI security policy.	Requirement Change
DTR D1	Eliminated ten hours minimum for exploitation time	Requirement Change

Document and Requirements Reference	Change	Type
DTR Appendix B	Updated Physical Attack Costing Potential Formulas to reflect a more granular approach for attack times and expertise	Additional Guidance
DTR Appendix C	Added new appendix detailing equipment classification for physical attack costing purposes for use with Appendix A	Additional Guidance
DTR Appendix F	Added new guidance for side channel analysis.	Additional Guidance
DTR Appendix G	Added new guidance for Firmware Scoping	Additional Guidance
VQ	Modifications and additions to reflect changes above.	Additional Guidance