Payment Card Industry (PCI)

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

Summary of Requirements Changes from Version 5.1 to 6.0

June 2020

Introduction

This document provides a summary of changes from the PCI PTS POI Modular Requirements v5.1 to v6.0. Table 1 provides an overview of the types of changes included in Version 6.0. Table 2 provides a summary of material changes to be found in Version 6.0.

Document Abbreviations Used

Abbreviation	Document Referenced
SR / SRs	PCI PTS POI Modular Security Requirements
DTR / DTRs	PCI PTS POI Modular Derived Test Requirements

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
General	Eliminated PCI Vendor Questionnaire. PCI laboratories will solicit information using proprietary methods that provide more efficient support for the gathering of that information.	Additional Guidance
General	Migrated as applicable many technical FAQs into the Derived Test Requirements or the Device Testing and Approval Program Guide.	Additional Guidance
SR General	Reorganized requirements into four Evaluation Modules: ▪ Evaluation Module 1: Physical and Logical ▪ Evaluation Module 2: POS Terminal Integration ▪ Evaluation Module 3: Communications and Interfaces ▪ Evaluation Module 4: Life Cycle Security	Requirement Change
SR General	Firmware expires three years from date of approval, but shall not expire past the overall approval expiration of the device. Every third year the firmware must be laboratory validated against specified DTRs.	Requirement Change
SR General	POI v6 chipsets must provide support for ECC.	Requirement Change
SR General	Migrated SRED and Open Protocols requirements into new evaluation modules and eliminated separate Open Protocols and SRED modules.	Requirement Change
SR General	Added tracking of Key Management for Account Data Encryption.	Additional Guidance
SR General	Allow the inclusion of MSRs in SCRPs for use in SPoC solutions.	Requirement Change
SR A1 / A2	Split requirement A1 into two separate requirements: 1) Tamper-Detection Mechanisms 2) Protection of Sensitive Keypad Inputs	Requirement Change
SR A6 / A7	Split requirement A6 into two separate requirements: 1) Invasive Attacks for Cryptographic Keys 2) Non-invasive Attacks for Cryptographic Keys	Requirement Change
SR A9 / E4.1-E4.3	Eliminated Removal Detection Requirements.	Requirement Change

Document and Requirements Reference	Change	Type
SR E1	Eliminated integration requirement	Requirement Change
SR B3	Combined B5 / A10 into a single requirement.	Requirement Change
B16.1	New requirement to introduce Software Security Domains and assessment thereof.	Requirement Change
SR Appendix B	Modified Applicability of Requirements to reflect restructure, including for Open Protocols and SRED.	Additional Guidance
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 B9	AES check values can only be calculated by MACing an all-zero block using the CMAC algorithm as specified in ISO 9797-1. TDES must support the same method and may support the deprecated legacy method.	Requirement Change
DTR B9	Devices must support key blocks as specified by ISO 20038 and/or the ANSI TR-31 key-derivation method. Other methods can only exist as specified in the guidance.	Requirement Change
DTR B9	The TR-31 key-calculation (variant) method for key blocks is deprecated and no longer allowed.	Requirement Change
DTRs B9 – B11	Fixed-key support has been eliminated as an acceptable key-management technique for both PIN and account data encryption. This applies to both AES and TDES.	Requirement Change
DTR Appendix A	Added guidance for handheld devices with touch screens.	Additional Guidance
DTR Appendix E	Updated content in “Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.”	Additional Guidance
DTR Appendix F	Modified guidance for side channel analysis.	Additional Guidance

Document and Requirements Reference	Change	Type
DTR Appendix G	New Appendix: “Domain-Based Asset Flow Analysis.” Incorporates and supersedes prior appendix on firmware scoping.	Additional Guidance
DTR Appendix H	New Appendix: “Evaluation Guidance for CPUs.”	Additional Guidance
DTR Appendix I	Modified Security Policy Layout Example for changes in DTR B20.	Additional Guidance