Industria de tarjetas de pago (PCI)

Seguridad de la transacción con PIN (PTS) Punto de interacción (POI)

Resumen de cambios en los requisitos de la versión 5.1 a la 6.0

Junio de 2020

DECLARACIONES: La versión en inglés del texto en este documento tal y como se encuentra en el sitio web de PCI SSC deberá considerar se, para todos los efectos, como la versión oficial de estos documentos y, si existe cualquier ambigüedad o inconsistencia entre este texto y el texto en inglés, el texto en inglés en dicha ubicación es el que prevalecerá.

Introducción

Este documento incluye un resumen de cambios de los requisitos modulares PCI, PTS, POI v5.1 a v6.0. La Tabla 1 ofrece un panorama de los tipos de cambios incluidos en la versión 6.0. La Tabla 2 ofrece un resumen de los cambios importantes que se encontrarán en la versión 6.0.

Abreviaturas utilizadas en el documento

Abreviatura	Documento al que se refiere
SR	Requisito(s) de seguridad para los módulos PCI, PTS, POI
DTR	Requisito(s) de prueba derivados de los módulos PCI, PTS, POI

Tabla 1: Tipos de cambios

Tipo de cambio	Definición
Orientación adicional	Explicación, definición y/o instrucción para aumentar la comprensión u ofrecer más información o guía sobre un tema en particular.
Cambio de requisito	Para reflejar que se añadió, modificó, eliminó o reestructuró algún requisito

Nota: *Los cambios arriba mencionados no incluyen correcciones de gramática ni errores tipográficos ni otro cambio de redacción de las declaraciones existentes.*

Tabla 2: Resumen de cambios

Documento y referencia de requisitos	Cambio	Tipo
General	Se eliminó el cuestionario de vendedor PCI. Los laboratorios PCI solicitarán información utilizando métodos registrados que ofrecen un apoyo más eficaz para la recolección de datos.	Orientación adicional
General	Muchas de las preguntas frecuentes en cuestión técnica migraron según fue necesario en los Requisitos de prueba derivada o la Guía del programa de pruebas y aprobación de dispositivos.	Orientación adicional
SR General	Requisitos reorganizados en cuatro módulos de evaluación: ▪ Módulo de evaluación 1: Físico y lógico ▪ Módulo de evaluación 2: Integración Terminal POS ▪ Modulo de evaluación 3: Comunicaciones e interfaces ▪ Módulo de evaluación 4: Seguridad del ciclo de vida	Cambio de requisito
SR General	La fecha de vencimiento del firmware es a los tres años de su fecha de aprobación, sin embargo, no vencerá después del vencimiento de aprobación general del dispositivo. Cada tres años, un laboratorio validará el firmware según las DTR especificadas.	Cambio de requisito
SR General	Los conjuntos de chips POI v6 deben ser compatibles para ECC.	Cambio de requisito
SR General	Se migraron los requisitos de protocolos SRED y abiertos en módulos nuevos de evaluación y se eliminaron los protocolos abiertos y módulos SRED separados.	Cambio de requisito
SR General	Se añadió el seguimiento de la administración clave para la codificación de datos de cuentas.	Orientación adicional
SR General	Se permite la inclusión de MSR en SCRP para su uso en soluciones SPoC.	Cambio de requisito
SR A1/A2	Se dividió el requisito A1 en dos requisitos separados: 1) Mecanismos de detección de manipulaciones 2) Protección de entradas de teclado sensibles	Cambio de requisito
SR A6/A7	Se dividió el requisito A6 en dos requisitos separados: 1) Ataques invasivos para claves criptográficas 2) Ataques no invasivos para claves criptográficas	Cambio de requisito

Documento y referencia de requisitos	Cambio	Tipo
SR A9/E4.1-E4.3	Se eliminaron los requisitos de detección de remociones.	Cambio de requisito
SR E1	Se eliminó el requisito de integración	Cambio de requisito
SR B3	Se combinaron B5 y A10 en un solo requisito.	Cambio de requisito
B16.1	Requisito nuevo para introducir dominios de seguridad de software y sus evaluaciones.	Cambio de requisito
SR Apéndice B	Se modificó la aplicabilidad de requisitos para reflejar la reorganización, entre otros, los protocolos abiertos y SRED.	Orientación adicional
Introducción DTR	Se ofreció orientación adicional para los criterios de presentación de informes de laboratorio, entre otros, contenidos mínimos de los informes y actividades mínimas de prueba.	Orientación adicional
DTR – Todas las secciones	Solidez mejorada de los guiones de prueba en todo momento.	Cambio de requisito
DTR B9	Los valores de revisión AES pueden calcularse solo con la combinación de un bloque todo cero utilizando el algoritmo CMAC como se especifica en ISO 9797-1. TDES debe ser compatible con el mismo método y puede respaldar el método de legado desaprobado.	Cambio de requisito
DTR B9	Los dispositivos deben ser compatibles con bloques de claves según las especificaciones de ISO 20038 y/o el método de derivación de claves ANSI TR-31. Solo pueden existir los demás métodos especificados en la guía.	Cambio de requisito
DTR B9	El método de cálculo de claves TR-31 (variante) para los bloques de claves está desaprobado y ya no se permite.	Cambio de requisito
DTRs B9–B11	Se eliminó el soporte de claves fijas como una técnica aceptable de administración de claves para la codificación con PIN y de datos de cuentas. Lo anterior se aplica tanto a AES como a TDES.	Cambio de requisito
DTR Apéndice A	Se añadió la guía para dispositivos manuales con pantallas táctiles.	Orientación adicional

Documento y referencia de requisitos	Cambio	Tipo
DTR Apéndice E	Se actualizó el contenido de "Tamaños y fortalezas clave mínimos y equivalentes para los algoritmos aprobados".	Orientación adicional
DTR Apéndice F	Guía modificada para análisis de canales secundarios.	Orientación adicional
DTR Apéndice G	Apéndice nuevo: "Análisis de flujo de activos basado en dominios". Incorpora y reemplaza al apéndice anterior sobre el alcance del firmware.	Orientación adicional
DTR Apéndice H	Apéndice nuevo: "Guía de evaluación para CPU".	Orientación adicional
DTR Apéndice I	Ejemplo de disposición modificada de la Política de seguridad para cambios en DTR B20.	Orientación adicional