Setor de cartões de pagamentos (PCI)

Segurança em transação de PIN (PTS)
Ponto de interação (POI)

Resumo das Alterações de Requisitos da Versão 5.1 para 6.0

Junho de 2020

TERMO DE RECONHECIMENTO: A versão em inglês deste documento, conforme disponibilizada no site da PCI SSC, para todos os efeitos, é considerada a versão oficial destes documentos e, na medida em que houver ambiguidades ou inconsistências entre a redação do presente texto e do texto em inglês,a versão em inglês disponibilizada no local mencionado prevalecerá

Introdução

Este documento apresenta um resumo das mudanças dos Requisitos Modulares da PCI PTS POI v5.1 para v6.0. A Tabela 1 apresenta uma visão geral dos tipos de alterações incluídas na Versão 6.0. A Tabela 2 apresenta um resumo das alterações materiais a serem encontradas na Versão 6.0.

Abreviaturas de documentos utilizadas

Abreviatura	Documento referenciado
SR/SRs	Requisitos de segurança modular da PCI PTS POI
DTR/DTRs	Requisitos de teste derivados modulares da PCI PTS POI

Tabela 1: Tipos de alteração

Tipo de alteração	Definição
Orientação adicional	Explicação, definição e/ou instrução para aumentar a compreensão ou fornecer mais informações ou orientações sobre um determinado tópico.
Alteração de requisito	Para refletir a modificação de adição, supressão ou reestruturação dos requisitos

Nota: *As alterações acima não incluem correções de erros gramaticais ou tipográficos ou outra reformulação de instruções existentes.*

Tabela 2: Resumo das alterações

Documentos e referência de requisitos	Alteração	Tipo
Geral	Questionário de fornecedor de PCI eliminado. Os laboratórios da PCI solicitarão informações usando métodos proprietários que ofereçam suporte mais eficiente para a coleta dessas informações.	Orientação adicional
Geral	MUITAS dúvidas técnicas frequentes migradas, conforme aplicável, para os requisitos de teste derivados ou guia do programa de teste e aprovação de dispositivos.	Orientação adicional
SR geral	Requisitos reorganizados em quatro módulos de avaliação: ▪ Módulo de avaliação 1: físico e lógico ▪ Módulo de avaliação 2: integração de terminal POS ▪ Módulo de avaliação 3: comunicações e interfaces ▪ Módulo de avaliação 4: segurança do ciclo de vida	Alteração de requisito
SR geral	O firmware expira em três anos após a data de aprovação, mas não deve expirar após a expiração geral da aprovação do dispositivo. A cada três anos, o firmware deve ser validado em laboratório de acordo com DTRs especificados.	Alteração de requisito
SR geral	Os chipsets POI v6 devem oferecer suporte para ECC.	Alteração de requisito
SR geral	Requisitos de SRED e protocolos abertos migrados para novos módulos de avaliação e protocolos abertos eliminados e módulos sred separados.	Alteração de requisito
SR geral	Adição de rastreamento de gerenciamento de chave para criptografia de dados de conta.	Orientação adicional
SR geral	Permitir a inclusão de MSRs em SCRPs para uso em soluções SPoC.	Alteração de requisito
SR A1/A2	Dividir o requisito A1 em dois requisitos distintos: 1) Mecanismos de detecção de violação 2) Proteção de entradas sensíveis no teclado	Alteração de requisito
SR A6/A7	Dividir o requisito A6 em dois requisitos distintos: 1) Ataques invasivos a chaves criptográficas 2) Ataques não invasivos a chaves criptográficas	Alteração de requisito

Documentos e referência de requisitos	Alteração	Tipo
SR A9/E4.1-E4.3	Requisitos de detecção de remoção eliminados.	Alteração de requisito
SR E1	Eliminado requisito de integração	Alteração de requisito
SR B3	B5/A10 combinados em um único requisito.	Alteração de requisito
B16.1	Novo requisito para introduzir domínios de segurança de software e a avaliação deste.	Alteração de requisito
SR Apêndice B	Aplicabilidade de Requisitos modificada para refletir a reestruturação, inclusive para protocolos abertos e SRED.	Orientação adicional
Introdução a DTRs	Orientação adicional fornecida para critérios de relatórios de laboratório, incluindo conteúdo mínimo de relatórios e atividades de teste mínimas.	Orientação adicional
DTRs — Todas as seções	Maior robustez dos scripts de teste por toda parte.	Alteração de requisito
DTR B9	Os valores da verificação AES somente podem ser calculados aplicando-se MAC a um bloco somente com zeros utilizando-se o algoritmo CMAC, conforme especificado na ISO 9797-1. O TDES deve ser compatível com o mesmo método e pode ser compatível com o método antigo obsoleto.	Alteração de requisito
DTR B9	Os dispositivos ser compatíveis com blocos de chaves, conforme especificado pela ISO 20038 e/ou pelo método de derivação de chaves ANSI TR-31. Outros métodos somente podem existir conforme especificado na orientação.	Alteração de requisito
DTR B9	O método de cálculo de chave TR-31 (variante) para blocos de chave está obsoleto e não é mais permitido.	Alteração de requisito
DTRs B9 – B11	O suporte de chave fixa foi eliminado como uma técnica de gerenciamento de chaves aceitável para criptografia de dados de PIN e conta. Isto aplica-se tanto ao AES como ao TDES.	Alteração de requisito
DTR Apêndice A	Orientação adicionada para dispositivos portáteis com telas sensíveis ao toque.	Orientação Adicional

Documentos e referência de requisitos	Alteração	Tipo
DTR Apêndice E	Conteúdo atualizado em “Principais tamanhos e pontos fortes mínimos e equivalentes para algoritmos aprovados”.	Orientação adicional
DTR Apêndice F	Orientação modificada para análise de canal lateral.	Orientação adicional
DTR Apêndice G	Novo Apêndice: “Análise de fluxo de ativos baseada em domínio”. Incorpora e substitui o apêndice anterior no escopo do firmware.	Orientação Adicional
DTR Apêndice H	Novo apêndice: “Orientação de avaliação para CPUs”.	Orientação Adicional
DTR Apêndice I	Exemplo de layout de política de segurança modificada para alterações no DTR B20.	Orientação Adicional