

payShield 10K

O módulo de segurança de hardware (HSM) que torna seguros pagamentos no mundo todo

payShield 10K

- Simplifica a instalação em dark data centers
- Oferece alta disponibilidade e resiliência
- Oferece maior suporte a aplicações móveis e de cartão em tempo hábil
- Suporta atualizações de desempenho sem alteração de hardware
- Mantêm a compatibilidade com versões anteriores de todos os HSMs legados de pagamentos da Thales



Especificações técnicas

O payShield 10K é um módulo de segurança de hardware (HSM) para pagamentos usado amplamente em todo o ecossistema global de pagamento por emissores, provedores de serviços, compradores, processadores e redes de pagamento. Ele desempenha um papel de segurança fundamental na emissão de credenciais de pagamentos seguros, autenticação do usuário, autenticação de cartões e proteção de dados confidenciais tanto para pagamentos presenciais quanto digitais à distância.

Casos de uso comuns

- Emissores de credenciais de pagamento - cartões, elementos seguros móveis, wearables, dispositivos conectados e aplicações de host card emulation (HCE)
- Roteamento de PIN
- Criptografia ponto a ponto (P2PE)
- Tokenização de segurança (para conformidade com o PCI DSS)
- Tokenização de pagamento com tecnologia EMV
- Autorização para pagamentos móveis e com cartão
- Gerenciamento de chaves com POS, mPOS e SPoC
- Validação de criptograma PIN e EMV
- Carregamento remoto de chave

Escolha dos integradores

- Integração com todas as autorizações de pagamento mais importantes e alternando aplicações
- Informações sobre os parceiros de tecnologia podem ser encontrados em:
www.thalessecurity.com/partners/technology-partners

Suporte para pagamentos com cartão/móveis

- O payShield 10K tem uma gama abrangente de funções que aceita as necessidades das principais marcas de pagamento (American Express, Discover, JCB, Mastercard, UnionPay e Visa) em várias áreas, incluindo:
 - Funções de verificação de cartão e PIN para todas as principais marcas de pagamento
 - Autorização e envio de mensagens para transações EMV
 - Autorização de transações de pagamentos móveis e gerenciamento de chaves
 - Carregamento remoto de chaves em caixa eletrônico e dispositivos de POS
 - Gerenciamento de chaves regional/nacional (incluindo Austrália, Alemanha e Itália)
 - Suporte ao gerenciamento de chaves Mastercard On-behalf (OBKM)
 - Preparação e personalização de dados com tarja magnética e EMV, incluindo provisionamento móvel
 - Geração e impressão de PIN

Algoritmos criptográficos

- Chave DES e DES Triplo com comprimento de 112 e 168 bit
- Chave AES com comprimento de 128 bit, 192 bit e 256 bit
- RSA (até 4096 bits)
- HMAC, MD5, SHA-1 e SHA-2

Padrões para serviços financeiros

- ISO: 9564, 10118, 11568, 13491 e 16609
- ANSI: X3.92, X9.8, X9.9, X9.17, X9.19, X9.24, X9.31, X9.52 e X9.97
- ASC X9 TR-31 e X9 TG-3/TR-39
- APACS 40 e 70

Segurança física

- Design resistente a violações e reativo
- Dados confidenciais apagados imediatamente em caso de violação
- Alarme acionado por movimento, tensão e temperatura

Segurança lógica

- Opções de múltiplas chaves mestras (LMK) – variante e bloqueio de chaves
- Autenticação com dois fatores (2FA) de responsáveis pela segurança usando cartões inteligentes
- Autorização de controle duplo – chaves físicas ou cartões inteligentes
- Configurações de segurança mais fortes implementadas por padrão
- Trilhas de auditoria com controle do usuário sobre o escopo dos eventos registrados

Modelos e opções do produto

- Unidades duplas de fornecimento de energia hot swap e padrão de ventilação em todos os modelos
- Variações dos níveis de desempenho – 25, 60, 250, 1000 e 2500 chamadas por segundo (cps)
- Opções de gerenciamento e monitoramento remoto por meio de payShield Manager, payShield Monitor e payShield Trusted Management Device (TMD)
- Opções para criptografia com preservação de contato (format preserving encryption - FPE)
- Múltiplas opções LMK – até 20 partições por HSM

Conectividade host

- TCP/IP & UDP (1Gbps) – duas portas
- Opção de gerenciamento de comunicação host segura para sessões de autenticação TLS em porta host Ethernet

Certificados de segurança

- FIPS 140-2 Nível 3 (subsistema de segurança) em progresso
- PCI HSM v3 (versões selecionadas de software)

Características físicas

- Padrão de montagem: em rack 1U de 19"
- Dimensões: 482,6 x 736,6 x 44,5 mm (19 x 29 x 1,75")
- Peso: 15,9 kg (35 Lbs)
- Fonte elétrica: 90 a 264 VAC
- Consumo de energia: 60 W (máximo)
- Temperatura operacional: de 0° C a 40° C
- Temperatura de transporte: -25° C a 70° C
- Temperatura de armazenamento: -5° C a 45° C
- Umidade: 10% a 90% (sem condensação)

Conformidade com as normas ambientais e de segurança

- UL, UL/CA, UL-AR, CE, BIS, FCC, Canada ICES, RCM, KC e VCCI
- RoHS2, REACH e WEEE