HSMs nShield Edge

Dispositivos certificados com conexão USB que fornecem serviços de chave criptográfica para aplicações desktop

DESTAQUES

Os módulos de segurança de hardware (HSMs) nShield Edge são dispositivos com recursos completos, com certificação FIPS e conectados por USB, que oferecem criptografia, geração e proteção de chaves, além de conveniência e economia.

- Maximiza a rentabilidade. O nShield Edge é o HSM mais econômico da família nShield
- Suporta uma ampla variedade de aplicações, incluindo autoridades de certificação, assinaturas codificadas e muito mais
- Proporciona alta segurança. Os HSMs nShield Edge são certificados pelo FIPS 140-2 até o Nível 3

Ideais para ambientes de transações de baixo volume

Suporta ambientes de geração e desenvolvimento de chaves off-line, ao mesmo tempo em que oferece suporte completo a algoritmos e APIs. Ideal para implantações Traga Sua Própria Chave (BYOK) que exigem geração de chaves criptográficas com garantia FIPS 140- de nível 2 antes de exportá-las com segurança para a nuvem.

Altamente portáteis

O design pequeno e leve, com interface USB conveniente, suporta uma variedade de plataformas, incluindo laptops e outros dispositivos portáteis.

Econômico e escalável

O HSM mais econômico da família nShield, o nShield Edge oferece um HSM de ponto de entrada, ao mesmo tempo que oferece a opção de dimensionar seu ambiente conforme suas necessidades aumentam. A arquitetura única do Security World da Entrust permite combinar modelos HSM nShield para construir uma propriedade mista que ofereça escalabilidade flexível, compartilhamento de chaves, failover perfeito e balanço de carga.

SAIBA MAIS EM ENTRUST.COM/HSM

HSMs nShield Edge

ESPECIFICAÇÕES TÉCNICAS

Algoritmos criptográficos com suporte (incluindo implementação completa do NIST Suite B)	Sistemas operacionais	Interfaces de Programação de Aplicativos (APIs)	Compatibilidade e Capacidade de upgrade	Conformidade de Segurança
• Algoritmos assimétricos: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH e Edwards (X25519, Ed25519ph) • Algoritmos simétricos: AES, Arcfour, ARIA, Camellia, CAST, DES, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, 3DES • Hash/resumo de mensagem: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160 e RIPEMD160	• Microsoft Windows 7 x64, 10 x64, Windows Server, 2012 R2 x64, 2016 x64, 2019 x64 • Red Hat Enterprise Linux AS/ES 6 x64, x86 e 7 x64; SUSE Enterprise Linux 11 x64 SP2, 12 x64, 15.1 x64 • Oracle Enterprise Linux 6.10 x64, 7.6 x64	• PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI e CNG, nCore, Web Services (requer pacote de opções de web-services)	• Porta USB (1.x, 2.x compatível)	• FIPS 140-2 Nível 2 e Nível 3

Conformidade com as normas ambientais e de segurança	Gerenciamento e monitoramento	Características físicas	Desempenho:
• UL, CE, FCC, RCM, e Canada ICES RoHS2, WEEE	• Garantia de registro de auditoria	• Dispositivo de área de trabalho portátil com leitor de cartão inteligente integrado • Dimensões com suporte aberto 120 x 118 x 27 milímetros (4,7 x 4,6 x 1 pol.) • Peso: 340 g (0,8 lb) • Tensão de entrada: 5v CC alimentado por dispositivo host USB • Consumo de energia: 700 mW	• Desempenho de assinatura para comprimentos de chave recomendados pelo NIST: • 2048 bit RSA: 2 tps • 4096 bit RSA: 0,2 tps

MODELOS E DESEMPENHO DISPONÍVEIS

- O nShield Edge está disponível nas variações FIPS Nível 2 e Nível 3
- Uma edição de desenvolvedores não-FIPS também está disponível

Saiba mais

Para saber mais sobre os HSMs Entrust nShield, visite **entrust.com/HSM**. Para saber mais sobre as soluções digitais da Entrust para identidades, acesso, comunicações e dados, visite **entrust.com**

Saiba mais em
entrust.com/HSM

Entre em contato conosco:
HSMinfo@entrust.com