HSMs nShield Connect

A segurança de suas aplicações depende de onde você guarda as suas chaves

DESTAQUES

Capacidades abrangentes

Os módulos de segurança de hardware (HSMs) nShield Connect são dispositivos certificados por FIPS 140-2 e Common Criteria EAL4 + (EN 419 221-5) que oferecem serviços de chave criptográfica escaláveis e altamente disponíveis em redes.

- Altas taxas de transação criptográfica e dimensionamento flexível
- Integram-se com mais de 150 soluções de provedores de aplicações líderes
- Opção CodeSafe para proteção da sua aplicação e lógica comercial com o ambiente de execução segura do nShield

Os HSMs nShield Connect são plataformas resistentes à falsificações que executam funções como criptografia, assinatura digital e geração e proteção de chaves em uma gama de aplicativos, como:

- Autoridades Certificadoras
- Code signing
- Software personalizado
- Aplicações conteinerizadas e em nuvem
- Web-services
- Blockchain
- Criptografia de banco de dados

A série nShield Connect inclui nShield Connect+ e o nShield Connect XC de alto desempenho.

SAIBA MAIS EM ENTRUST.COM/HSM

HSMs nShield Connect

PRINCIPAIS RECURSOS E BENEFÍCIOS

Arquitetura altamente flexível

Nossa exclusiva arquitetura do Security World permite combinar modelos de HSM nShield para criar uma estrutura mista que ofereça escalabilidade flexível, failover sem impactos e balanço de carga perfeitos.

Processam mais dados mais rapidamente

Os HSMs nShield Connect suportam altas taxas de transações, tornando-os ideais para ambientes onde a taxa de transferência é crítica, como em empresas, varejo e IoT.

OPÇÕES DE RECURSOS REMOTOS PODEROSOS

Elimina visitas ao data center

Administração remota do nShield - habilita a apresentação remota segura de autorização de cartões inteligentes em HSMs remotos para executar tarefas de manutenção que incluem atualizações de firmware, inscrição de novos HSMs e reatribuição/ reconfiguração dos HSMs existentes. Folha de dados separada disponível.

Configuração remota - a versão do console serial do Connect XC permite a instalação simples pela equipe do data center, configuração de rede e definições de painel frontal.

O nShield Monitor fornece um único painel de todos os seus HSMs nShield, ajudando a otimizar as operações e aumentando o tempo de atividade. Folha de dados separada disponível.

Proteja as suas aplicações proprietárias

A opção CodeSafe fornece um ambiente seguro para aplicativos confidenciais no limite físico do nShield FIPS 140-2. Consulte a folha de dados CodeSafe para obter informações mais detalhadas.

MODELOS DISPONÍVEIS E DESEMPENHO

Modelos nShield Connect	500+	XC Base	1500+	6000+	XC Mid	XC High
Desempenho de assinatura com RSA (tps) para comprimentos de chave recomendados pelo NIST						
2048 bit	150	430	450	3.000	3.500	8.600
4096 bit	80	100	190	500	850	2.025
Desempenho de assinatura com ECC prime curve (tps) para comprimentos de chame recomendados pelo NIST						
256 bit	540	680	1.260	2.400	7.515[2]	14.400[2]
Licenças de cliente						
Incluídas	3	3	3	3	3	3
Máximo	10	10	20	ilimitado[1]	20	ilimitado[1]

Nota 1: requer licença de cliente da empresa.

Nota 2: o desempenho indicado requer a ativação rápida do recurso ECDSA RNG disponível gratuitamente mediante solicitação ao suporte da nCipher.

SAIBA MAIS EM ENTRUST.COM/HSM

HSMs nShield Connect

ESPECIFICAÇÕES TÉCNICAS

Algoritmos criptográficos com suporte (incluindo implementação completa do NIST Suite B)	Plataformas suportadas	Interfaces de Programação de Aplicativos (APIs)	Conectividade com o host	Conformidade de Segurança
• Algoritmos assimétricos: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA (incluindo NIST, Brainpool e secp256k1 curves), ECDH e Edwards (Ed25519 e 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	• Sistemas operacionais Windows e Linux, incluindo distribuições de RedHat, SUSE e principais provedores de serviços em nuvem executados como máquinas virtuais ou em containers	• PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI/CNG e web-services (requer Web Services Option Pack)	• Portas Duplas Gigabit Ethernet (dois segmentos de rede)	• FIPS 140-2 com certificação de Nível 2 e Nível 3 • Certificação IPv6 e com padrão USGv6 Ready • Connect XC: certificação eIDAS e Common Criteria EAL4 + AVA_ VAN.5 e ALC_ FLR.2 de acordo com o perfil de proteção EN 419 221-5, sob o esquema holandês NSCIB • Connect+: Certificação Common Criteria EAL4+ (AVA_VAN.5) • Connect+: reconhecido como Qualified Signature Creation Device • Connect XC: compatível com BSI AIS 20/31

Conformidade com as normas ambientais e de segurança	Alta disponibilidade	Gerenciamento e monitoramento	Características físicas
• UL, CE, FCC, RCM Canada ICES RoHS2, WEEE	• Todo o armazenamento de estado sólido • Componentes de manutenção em campo, fontes de alimentação dual hot-swap	• nShield Remote Configuration (disponível em modelos Connect XC configurados em console de série) • nShield Remote Administration (adquirido separadamente) • nShield Monitor (adquirido separadamente) • Garantia de registro de auditoria • Suporte de diagnósticos ao padrão Syslog e monitoramento do desempenho no Windows • Agente de monitoramento SNMP	• Montagem em rack 1U 19in. padrão Dimensões: 43,4 x 430 x 705 mm (1,7 x 16,9 x 27,8 in) • Peso: 11,5 kg (25,4 lb) • Potência de entrada: 100-240V CA com alternância automática 50-60 Hz • Consumo de energia: até 2,0 A a 110V AC, 60Hz | 1,0 A a 220 V AC, 50 Hz • Dissipação de calor: 327,6 a 362,0 BTU/h (carga completa) • Confiabilidade - MTBF (horas)[3], Connect XC: 107,384 horas, Connect+: 99,284 horas

Nota 3: calculada a temperatura operável em 25 graus usando o Padrão MTBF Telcordia SR-332 “Procedimento de Previsão de Confiabilidade para Equipamentos Eletrônicos”.

Para saber mais sobre o Entrust nShield HSMs

HSMinfo@entrust.com
entrust.com/HSM

SOBRE A ENTRUST CORPORATION

A Entrust mantém o mundo movendo-se com segurança, permitindo identidades, pagamentos e proteção de dados confiáveis.Hoje, mais do que nunca, as pessoas exigem experiências seguras e contínuas, quer estejam cruzando fronteiras, fazendo uma compra, acessando serviços de governo eletrônico ou entrando em redes corporativas. A Entrust oferece uma gama incomparável de soluções de segurança digital e emissão de credenciais no centro de todas essas interações. Com mais de 2.500 colegas, uma rede de parceiros globais e clientes em mais de 150 países, não é de admirar que as organizações mais confiáveis do mundo confiem em nós.

Saiba mais em
entrust.com/HSM

ENTRUST

Entre em contato conosco:
HSMinfo@entrust.com