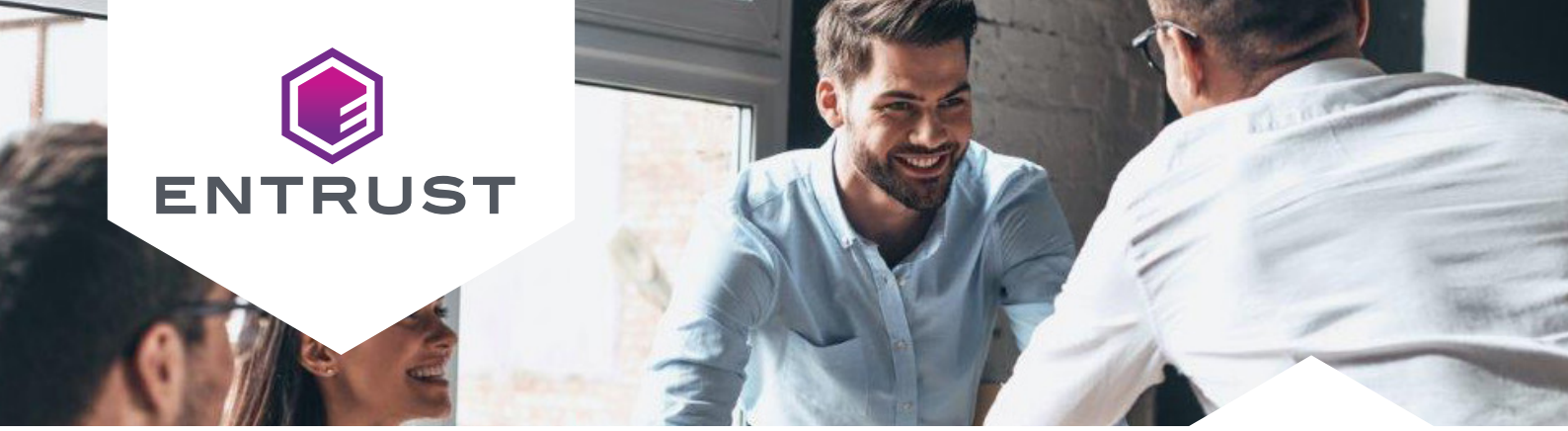


HSMs nShield Solo

Cartões PCI-Express certificados que fornecem serviços de chave criptográfica para servidores autônomos

DESTAQUES

Os módulos de segurança de hardware (HSMs) nShield Solo são cartões PCI-Express de baixo perfil e certificação FIPS que fornecem serviço criptográficos para aplicativos hospedados em um servidor ou dispositivo. Esses cartões resistentes à falsificações, realizam funções como criptografia, assinatura digital e geração e proteção de chaves em uma ampla variedade de aplicações, incluindo autoridades de certificação, assinatura de código, software personalizado e muito mais.

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

Arquitetura altamente flexível

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

Processam mais dados mais rapidamente

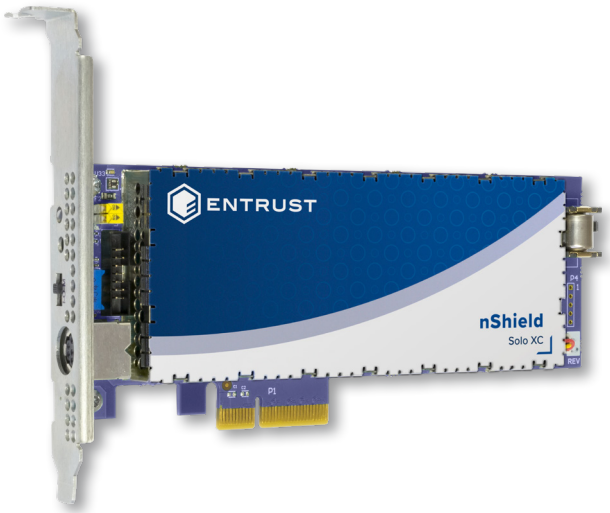
Os HSMs nShield Solo suportam altas taxas de transações, tornando-os ideais para empresas, varejo, IoT e outros ambientes onde a taxa de transferência é crítica.

Projeta suas aplicações e dados proprietários

A opção CodeSafe fornece um ambiente seguro para executar aplicativos confidenciais dentro dos limites do nShield.

PRINCIPAIS RECURSOS E BENEFÍCIOS

- Maximiza o rendimento e a disponibilidade, suportando alto número de transações criptográficas com escalabilidade flexível
- Suporta uma ampla variedade de aplicações, incluindo autoridades de certificação, assinatura de código e muito mais
- O nShield CodeSafe protege suas aplicações com o ambiente de execução seguro do nShield
- O nShield Remote Administration ajuda a cortar custos e reduzir viagens



SAIBA MAIS EM ENTRUST.COM/HSM

HSMs nShield Solo

ESPECIFICAÇÕES TÉCNICAS

Algoritmos criptográficos suportados

- Algoritmos assimétricos: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, 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
- Implementação completa da Suite B com ECC totalmente licenciado, incluindo Brainpool e curvas personalizadas

Plataformas suportadas

- Sistemas operacionais Windows e Linux, incluindo distribuições de RedHat, SUSE e principais provedores de serviços em nuvem executados como máquinas virtuais ou em contêineres
- Ambientes virtuais Solo XC suportados, incluindo VMware ESX, Microsoft Hyper-V, Linux KVM e Citrix XenServer

Interfaces de Programação de Aplicativos (APIs)

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI e CNG, nCore, e web-services (requer Web Services Option Pack)

Conectividade do host

- PCI Express versão 2.0; Solo+ conector: 1 via, conector Solo XC: 4 vias

Conformidade de segurança

- Certificação FIPS 140-2 Nível 2 e Nível 3
- Solo+: certificação Common Criteria EAL4+ (AVA_VAN.5)
- Solo+ reconhecido como Qualified Signature Creation Device
- Solo 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
- Solo XC: compatível com BSI AIS 20/31

Conformidade com as normas ambientais e de segurança

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

Gerenciamento e monitoramento

- nShield Remote Administration e nShield Monitor
- Garantia de registro de auditoria
- Suporte de diagnósticos ao padrão Syslog e monitoramento do desempenho no Windows
- Agente de monitoramento SNMP

MODELOS DISPONÍVEIS E DESEMPENHO

Modelos nShield Solo	500+	XC Base	6000+	XC Mid	XC High
Desempenho de assinatura RSA (tps) para comprimentos de chave recomendados					
2048 bit	150	430	3.000	3.500	8.600
4096 bit	80	100	500	850	2.025
Desempenho de assinatura com ECC prime curve (tps) para comprimentos de chame recomendados pelo NIST					
256 bit	540	680	2.400	7.515[1]	14.400[1]

Dimensões	Peso		Alimentação	
	Solo+	Solo XC	Solo+	Solo XC
56,2 Q 167,1 Q 15,4 mm	230 g	280 g	10 W	24 W
2,2 Q 6,6 Q 0,6in	0,5 lb	0,62 lb		

Nota 1: 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

ENTRUST

Entre em contato conosco:
HSMinfo@entrust.com