



Módulos de Segurança de Hardware nShield® para uso geral



ENTRUST

SECURING A WORLD IN MOTION

Conteúdo

Segurança que você pode confiar	3
Família nShield	4
nShield Connect	4
nShield Edge	4
nShield Solo	4
nShield as a Service	4
Oferece suporte para diversas aplicações	5
Características da família nShield	5
Interfaces de serviços para internet em nuvem	5
Suporte em containers no local ou na nuvem	6
Gerenciamento de chave mais poderoso para seus dados na nuvem com o nShield BYOK	6
Operações racionalizadas usando o gerenciamento e monitoramento remoto	7
Configuração remota	7
Security World, a arquitetura mais flexível do mundo	7
CodeSafe - ambiente seguro de execução da nShield	8
Parcerias com líderes da indústria	9
Versatilidade e alto desempenho	10
Certificação de acordo com padrões da indústria	10
FIPS 140-2	10
Conformidade de acordo com o Common criteria e eIDAS	11



Segurança que você pode confiar

Os módulos de segurança de Hardware (HSMs) nShield da Entrust são dispositivos poderosos e resistentes a falsificações que protegem os dados mais sensíveis de sua empresa. Estes módulos com certificação FIPS 140-2 executam funções criptográficas como geração, gerenciamento e armazenamento de criptografia e assinatura de chaves, e também executam funções confidenciais dentro de seu ambiente protegido.

Os HSMs nShield são um complemento poderoso para seu pacote de segurança e ajudam a:

- Obter níveis mais altos de segurança de dados e confiança
- Cumprir e exceder importantes padrões de normas
- Manter serviços de alto nível e agilidade de negócios

Família nShield

Para servir adequadamente ao seu ambiente específico, a família HSMs nShield para diversos usos inclui os seguintes modelos:

nShield Connect

Programas conectados à rede

Os HSMs nShield Connect oferecem serviços criptográficos a aplicativos através da rede. Os HSMs nShield Connect estão disponíveis em duas séries: nShield Connect+ e o novo nShield Connect XC de alto desempenho

nShield Edge

Módulos portáteis baseados em interface USB

Os HSMs nShield Edge são dispositivos desktop projetados para sua conveniência e economia. O nShield Edge é ideal para desenvolvedores e oferece suporte a aplicações, como geração de chave de root de baixo volume.

nShield Solo

Cartões PCIe integrados para aplicativos ou servidores

Os HSMs nShield Solo são cartões PCI-Express de baixo perfil que oferecem serviços criptográficos a aplicativos hospedados em servidores. Os HSMs nShield estão disponíveis em duas séries: nShield Solo+ (clássico) e o novo nShield Solo XC de alto rendimento.

nShield as a Service

Soluções baseadas em assinatura para acessar os HSMs nShield na nuvem

O nShield as a Service fornece acesso aos HSMs nShield Connect XC com certificação FIPS 140-2 Nível 3 através de um modelo de assinatura. A solução oferece os mesmos recursos e funcionalidade dos HSMs locais combinados com os benefícios de uma implantação de serviço em nuvem. Isso permite que os clientes cumpram seus primeiros objetivos de nuvem e deixem a manutenção desses dispositivos para os especialistas da Entrust. Disponível como opções de serviço autogerenciado e totalmente gerenciado.



Suporte para diversas aplicações

Os clientes da Entrust usam os HSMs nShield para segurança básica em diversas aplicações para negócios, incluindo infraestruturas de chave pública (PKI), proteção de chave de criptografia SSL/TLS, assinatura codificada, assinatura digital e blockchain. O crescimento da Internet das Coisas gera uma demanda maior por dispositivos de identificação e certificados, os HSMs nShield continuarão a aceitar medidas críticas de segurança, como autenticação de dispositivo, usando certificados digitais.

Os HSMs nShield também aceitam diversos algoritmos criptográficos, incluindo algoritmos de criptografia com curva elíptica, os quais permitem transações rápidas perfeitamente adequadas para os atuais ambientes de computação compactos, bem como para os sistemas operacionais e APIs mais usados pela indústria.

Características da família nShield

Interfaces web-services favoráveis à nuvem

A solução opcional nShield Web Services Option Pack simplifica a interface entre aplicativos e HSMs executando comandos por meio de chamadas de serviço pela internet. Esta abordagem inovadora simplifica as implantações porque não há necessidade de integrar aplicativos diretamente com o nShield e acaba com a dependência de escolha de opções de tipo de arquitetura e sistema operacional. Uma solução para nuvem, a API Web Services Option Pack se conecta a aplicações hospedadas em nuvem e com data centers tradicionais.



Suporte em containers no local ou na nuvem

O nShield Container Option Pack permite o desenvolvimento e implantação racionalizados de aplicações ou processos em containers sustentados pelos módulos de segurança de hardware de alta garantia da Entrust. Esta opção fornece um conjunto de scripts pré-emballados que simplificam muito a integração dos HSMs nShield em um ambiente de aplicação de container, ao mesmo tempo em que oferece suporte às necessidades dinâmicas de escalonamento de aplicações e hosts em containers dos clientes.

Gerenciamento de chaves mais poderoso para os seus dados em nuvem com o nShield BYOK

O nShield BYOK (Bring Your Own Key) permite gerar chaves poderosas em seu HSM nShield local e exportá-las de maneira segura para seus aplicativos em nuvem, independentemente de você usar o Amazon Web Services, o Google Cloud Platform, o Microsoft Azure — ou todos os três. Com o BYOK nShield você aumenta a segurança de suas práticas de gerenciamento de chaves, obtém maior controle sobre suas chaves e garante que está compartilhando a responsabilidade de manter seus dados seguros em nuvem.

O nShield BYOK oferece as seguintes vantagens:

- Práticas de gerenciamento de chaves mais seguras que aumentam a segurança de seus dados sensíveis em nuvem

- Geração potente de chave usando o gerador de números aleatórios de alta entropia nShield protegido por hardware com certificação FIPS
- Maior controle das chaves — use seus próprios HSMs nShield em seu ambiente para criar e exportar com segurança as chaves para a nuvem

Para obter a maior garantia e controles rígidos sobre o transporte e uso de chaves criptográficas, use o nCipher BYOK com Microsoft Azure. Se você precisar de assistência no local com a integração e a implantação, por que não escolher nosso BYOK Deployment Service Package. Este pacote inclui um nShield Edge, integração fornecida pela equipe dos Serviços Profissionais da Entrust, e um ano de manutenção.

Para BYOK na Amazon Web Services e Google Cloud Platform, escolha o Cloud Integration Option Pack (CIOP) da Entrust. Este pacote de opções contém tudo o que você precisa para usar os seus HSMs nShield no local para gerar e arrendar suas chaves para o Amazon Web Services ou Google Cloud Platform. Além disso, o CIOP oferece suporte para o novo mecanismo de plataforma aberta Microsoft Azure BYOK.



Operações racionalizadas usando gerenciamento e monitoramento remotos

O nShield Monitor e o nShield Remote Administration, disponíveis para HSMs nShield modelos Solo e Connect, ajudam a cortar custos operacionais ao mesmo tempo em que lhe deixa informado e com comando em tempo integral sobre os estados do seu HSM.


- O monitoramento e gerenciamento remoto da Entrust oferece os seguintes benefícios:
- Otimização do desempenho, planejamento de infraestrutura e tempo de atividade do HSM através do nShield Monitor para informar à sua equipe sobre tendências de carga, estatísticas de uso, eventos de falsificações, avisos e alertas
- Reduzir custos de viagem e economizar tempo através do gerenciamento de HSMs com a poderosa e segura interface nShield Remote Administration

Configuração remota

Os modelos nShield Connect XC oferecem uma opção de console em série, simplificando a instalação física do HSM para rack, cabeamento e uso de energia. Todas as demais configurações de HSM e rede podem ser feitas remotamente. Isso facilita a implantação e reimplantação sem a necessidade de visitar o data center. Este recurso oferece suporte a um modelo de provedor/usuário em que o provedor controla a configuração da rede e o usuário tem controle total de seu material de chave.

Security World, a arquitetura mais flexível do mundo

O nShield Security World oferece suporte aos HSMs Entrust nShield criando um ambiente exclusivo e flexível de gerenciamento de chaves. Com o nShield Security World, você pode combinar modelos de HSM nShield para montar um ecossistema unificado que oferece escalabilidade, failover sem impactos e balanço de carga.



"Os HSMs Entrust nShield são de última geração e, portanto, nos permitiram usar um chip mais sofisticado e seguro em nossa tecnologia."

Bill Kavadas, diretor sênior de Sistemas de Informações, Memjet

O nShield Security World oferece interoperabilidade, independentemente da instalação de um ou centenas de HSMs, permite que você gerencie um número ilimitado de chaves e faz backup e restaura o material de chave automaticamente e remotamente.

O nShield Security World oferece as seguintes vantagens:

- Ajuda a dimensionar facilmente o estado de seu HSM nShield de acordo com o aumento da necessidade
- Preserva a resiliência de sistemas
- Economiza tempo e elimina back-ups de HSM desnecessários

CodeSafe - ambiente seguro de execução nShield


Além de proteger suas chaves confidenciais os HSMs nShield Solo e Connect oferecem um ambiente seguro para executar aplicativos proprietários. A opção CodeSafe possibilita desenvolver e executar códigos dentro dos limites FIPS 140-2 Nível 3 da nShield, protegendo suas aplicações contra possíveis ataques.

O CodeSafe ajuda a:

- Obter alta garantia pela execução de aplicações confidenciais e proteção de endpoints de dados de aplicações em um ambiente certificado
- Proteger aplicações confidenciais de segurança contra riscos, como ataques internos, malware e ameaças avançadas persistentes
- Eliminar o risco de alterações não autorizadas em aplicações ou contaminação por malware usando assinaturas codificadas


Parcerias com líderes da indústria

A Entrust tem parcerias com os principais provedores de tecnologia a fim de fornecer soluções aprimoradas para uma ampla gama de desafios da indústria de segurança e ajuda seus clientes a atingirem seus objetivos de transformação digital. Por meio do programa parceiro de tecnologia da Entrust, a Entrust colabora com parceiros para integrar os HSMs nShield em uma variedade de soluções de segurança, incluindo credenciamento e PKI, segurança de banco de dados, assinatura codificada, assinaturas digitais, gerenciamento de contas privilegiadas, entrega de aplicações, e nuvem e inteligência de big data. Os HSMs nShield apoiam as aplicações de segurança de nossos parceiros para fornecer o processamento criptográfico, a proteção e o gerenciamento de chaves mais fortes disponíveis, ao mesmo tempo em que facilitam a conformidade com as normas de segurança de dados do governo e da indústria.



"Estamos entusiasmados com as possibilidades que os novos recursos favoráveis à nuvem do nShield trazem, incluindo o nShield as a Service, oferecido aos nossos clientes. Esses novos recursos reconhecem que o mercado está mudando; que as organizações precisam dos recursos de HSMs de serviço completo na nuvem para liberar a inovação e os benefícios comerciais disponíveis."

Ed Wood, diretor de Gerenciamento de Produto, Cryptomathic



"O lançamento do nShield as a Service da Entrust oferece aos clientes da F5 opções de segurança aprimoradas com a capacidade de alcançar a soberania dos dados em um modelo baseado em assinatura. Mudar a segurança de uma despesa de capital para uma despesa operacional permite maior flexibilidade e rentabilidade para as organizações."

John Morgan, vice-presidente e diretor-geral de segurança, F5 Networks

Versatilidade e alto desempenho

Os HSMs nShield Connect e Solo estão disponíveis em três níveis de desempenho para se adequar ao seu ambiente, independentemente das suas taxas de transação serem moderadas ou sua aplicação exigir alto rendimento. O nShield as a Service, nossa solução baseada em assinatura para acessar os HSMs nShield na nuvem, é sustentada por nosso nShield Connect XC de mais alto desempenho.

Certificação de acordo com padrões da indústria

A adesão da Entrust a rigorosos padrões ajuda a demonstrar a conformidade em ambientes regulamentados e oferecer extrema confiança na segurança e integridade dos HSMs nShield. Abaixo está uma lista dos padrões que seguimos. As listas completas estão disponíveis em nosso site e em nossas folhas de dados.

FIPS 140-2

Reconhecido mundialmente, o FIPS 140-2 é um padrão NIST do governo americano que valida a robustez da segurança de módulos criptográficos. Todos os HSMs Entrust nShield possuem certificações FIPS 140-2 Nível 2 e Nível 3.





Conformidade de acordo com Common Criteria e eIDAS

nShield XC e nShield + HSMs são certificados pelo Common Criteria EAL 4+ e reconhecidos como dispositivos de criação de assinatura qualificados (QSCDs) de acordo com o regulamento eIDAS. Além disso, os HSMs nShield Solo XC e Connect XC são compatíveis com o Common Criteria Protection Profile EN 419 221-5 “Módulos criptográficos para serviços de confiança”. Os HSMs nShield são, portanto, capazes de servir como backbone de segurança para a digitalização de empresas e estados membros da UE. Isso inclui a habilitação de esquemas nacionais de identificação e serviços internacionais, serviços para documentos eletrônicos e assinatura de transações, além de serviços para autenticação, carimbo de data/hora, e-mail seguro e preservação de documentos a longo prazo. Embora essas certificações tenham sido estabelecidas como parte de uma regulamentação europeia, elas estão sendo adotadas por muitos países ao redor do mundo.

Para obter mais informações

Visite-nos em entrust.com/HSM para saber como podemos proteger suas informações e aplicações de negócios críticas, em suas próprias instalações, na nuvem e em ambientes virtuais.

Para saber mais sobre
os HSMs Entrust nShield
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    

