



Módulo de Segurança de Hardware

Thales nShield Edge

PRINCIPAIS BENEFÍCIOS

OPERACIONAIS

- > Fornece uma solução de baixo custo, portátil, com flexibilidade operacional incomparável para laptops e máquinas virtuais, baseada na arquitetura exclusiva do Security World
- > Reduz o custo total para conformidade regulamentar (por exemplo, PCI DSS), bem como tarefas de gerenciamento de chave para o dia a dia, incluindo o backup e o gerenciamento remoto
- > Assegura com enorme garantia a continuidade dos negócios, com registro HSM simplificado e eficiente provisionamento de chave
- > Protege as chaves de autoridade de registro e fornece uma solução prática para ACs de raiz offline

DE SEGURANÇA

- > Oferece proteção certificada para operações de chaves criptográficas protegidas por hardware inviolável para melhoramento significativo da segurança em aplicações críticas
- > Estabelece forte separação de funções e controles duplos por meio de políticas sólidas de administração, incluindo autenticação baseada em funções multifator e autorização de quorum flexível

O nShield Edge é o módulo de segurança de hardware (HSM) com conexão USB (barramento serial universal) pertencente à família Thales, especializada em soluções de proteção de dados de alta segurança. O NShield Edge combina um HSM completo com um leitor de cartão inteligente em um dispositivo portátil, oferecendo backup seguro e controle de acesso duplo, para chaves de alto valor de uma organização em ambientes de baixo volume de transações. A plataforma de certificação independente realiza operações criptográficas e gerenciamento de chaves, como a criptografia e a assinatura digital, em nome de uma ampla variedade de aplicações comerciais e personalizadas e sistemas de segurança crítica, incluindo autoridades de certificação offline (ACs) para infraestruturas de chaves públicas (ICP), assinatura de código e gerenciamento remoto do HSM.

A conectividade USB do NShield Edge faz com que ele seja especialmente adequado para uso com laptops e máquinas virtuais, proporcionando níveis adequados de controles físicos e lógicos, onde os recursos baseados em software de segurança são considerados inadequados. Em face da evolução dos requisitos de conformidade e das normas gerais de diligência, o uso dos HSMs nShield oferecem uma medida concreta de segurança. Todos os HSMs nShield da Thales se caracterizam pela arquitetura de gerenciamento de chaves líder de mercado, o Security World, que permite a automatização de pesadas tarefas administrativas propensas a risco, garante a recuperação de chave e elimina pontos únicos de falha e processos dispendiosos e intensivos de backup manual.



Microsoft
GOLD CERTIFIED
Partner

ISV

ORACLE CERTIFIED
PARTNER

> Thales nShield Edge

Especificações Técnicas*

Capacidades Funcionais

- > Protege chaves criptográficas em hardware seguro
- > Suporta laptops e máquinas virtuais
- > Fornece acesso de duplo controle para chaves valiosas
- > Fornece solução prática para ACs de raiz offline
- > Protege chaves para autoridades de registro
- > Controla chaves utilizadas para assinatura de código
- > Facilita a operação remota do HSM nShield
- > Simplifica o desenvolvimento de aplicativos de HSM
- > Fornece disposição de chave segura, replicação, backup e recuperação
- > Suporta storage ilimitado de chaves protegidas e separação lógica/criptográfica de chaves de aplicativo
- > Oferece autenticação multifator "k de n"

Sistemas Operacionais Suportados

- > Físicos: Windows 2008, 2008 R2, XP, Vista, 7
- > Virtuais: VMware Server, VMware Workstation, Microsoft Hyper-V para Windows Server 2008 R2, MS Virtual PC para Windows 7

Interfaces de Programa Aplicativo (IPAs)

- > PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI e CNG
- > nCore (interface Thales de nível baixo para desenvolvedores)

Compatibilidade e Atualizações

- > Compatível com o Thales nShield Solo (PCI/PCle), o nShield Connect e o netHSM 500 e 2000
- > Software atualizável

Conectividade do Host

- > Porta USB (1.x, 2.x compatível)
- > Inclui 1 metro de cabo conector (USB tipo A para B)

Criptografia

- > Algoritmos de chave pública assimétrica: RSA (1024, 2048, 4096, 8192), Diffie-Hellman, DSA, El-Gamal, KCDSA, ECDSA, ECDH
- > Algoritmos simétricos: AES, ARIA, Camellia, CAST, DES, RIPEMD160 HMAC, SEED, 3DES
- > Hash/resumo de mensagem: SHA-1, SHA-2 (224, 256, 384, 512bit)
- > Implementação total de Suite B com Criptografia de Curva Elíptica (CCE) totalmente licenciada, incluindo Brainpool e curvas personalizadas

Segurança e Conformidade Ambiental

- > UL, CE, FCC
- > RoHS, WEEE
- > FIPS 140-2 Nível 2 e Nível 3, NIST SP 800-131A

Alta Disponibilidade

- > Storage de estado sólido completo

Gerenciamento e Monitoramento

- > Controle de acesso remoto multi-usuário/sem operador
- > Suporte de diagnósticos syslog
- > Monitoramento de desempenho por janelas
- > Interface de linha comando (ILC) / interface gráfica do usuário (IGU)
- > Monitoramento compatível SNMPv3

Características Físicas

- > 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: 340g (0,8lb)
- > Tensão de entrada: 5v CC alimentado por dispositivo host USB
- > Consumo de Energia: 700mW
- > Temperatura: operacional de 5°C a 45°C (40°F a 113°F) storage de -40°C a 70°C (40°F a 158°F)
- > Umidade: operacional de 10 a 85% (relativa, sem condensação a 35%) e de armazenamento 0 a 85% (relativa, sem condensação a 35%)

Disponibilidade e Desempenho

nShield EDGE está disponível em variantes FIPS de nível 3 e nível 2. Também é disponibilizado em uma Edição de Desenvolvedor não-FIPS. Todos os modelos possuem as mesmas características de desempenho.



Desempenho Assinatura	(tps)
1024bit RSA	12
2048bit RSA	2
4096bit RSA	0.2

O nShield Edge inclui cartões inteligentes e pastas para um storage conveniente.

T SERVICES

Gold Partner Brasil
info@tservices.com.br
+55 (11) 5095.5555
ou 0800.729.0669

* O desempenho pode variar conforme o sistema operacional, aplicativo, topologia de rede e outros fatores.

Thales e-Security

