THALES

Módulo de Segurança de Hardware

Thales nShield Solo

PRINCIPAIS BENEFÍCIOS

OPERACIONAIS

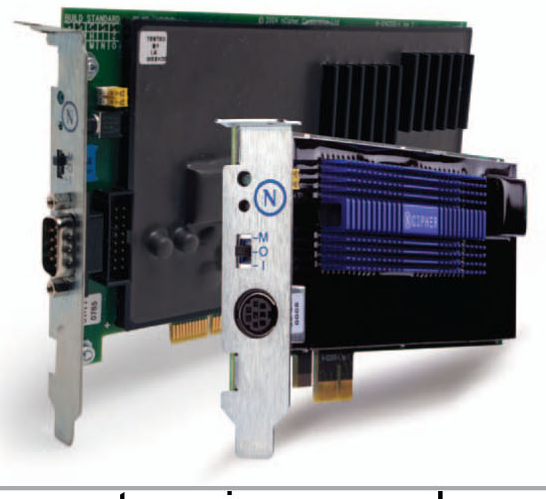
- Fornece uma aceleração criptográfica a um custo reduzido e flexibilidade operacional incomparável em ambientes em nuvem e Data Centers tradicionais, com base na arquitetura exclusiva do Security World
- Reduz o custo total para conformidade regulamentar (por exemplo, PCI DSS), bem como tarefas de gerenciamento 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
- Melhora a segurança e fornece aceleração criptográfica para aplicativos OEM

SEGURANÇA

- Oferece proteção certificada para operações e chaves criptográficas protegidas por hardware inviolável para melhoramento significativo da segurança em aplicações críticas
- Estabelece uma separação forte de funções e controles duplos através de políticas administrativas sólidas, incluindo uma autenticação multifator baseada na função e uma autorização flexível baseada em quórum
- Permite a execução segura de um código de aplicativo crítico para a segurança dentro dos limites de segurança do hardware

O nShield Solo é o principal módulo de segurança de hardware (HSM) da família Thales de soluções de proteção de dados de alta segurança. Os cartões Solo independentemente certificados são compatíveis com plataformas que oferecem interfaces de interconexão de componentes periféricos (PCI e PCI Express). O nShield Solo protege os sistemas de segurança crítica ao realizar o gerenciamento de chaves e operações criptográficas, como criptografia e assinatura digital em nome de uma ampla variedade de aplicativos comerciais e de negócios criados pelo cliente e sistemas de segurança crítica, incluindo infraestruturas de chave pública (PKIs), sistemas de gerenciamento de identidade, banco de dados, aplicações web, implantações de extensão para sistemas de nome de domínio (DNSSEC) e assinatura de códigos.

O nShield Solo oferece custo-benefício e controles físicos e lógicos dedicados para sistemas baseados em servidor onde os recursos de segurança baseados em software 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 dentro do Data Center tradicional e dos serviços baseados em nuvem. Todos os HSMs Thales nShield se caracterizam pela arquitetura de gerenciamento de chave líder do 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

T SERVICES

www.tservices.com.br

> Thales nShield Solo

Especificações Técnicas*

Capacidades Funcionais
- Suporte de aplicativo embutido para servidor cliente individual
- Chave segura onboard e storage/processamento de aplicativos
- Descarregamento/aceleração criptográfica
- Controle de acesso multinível autenticado
- Separação forte de funções (administrador e operador)
- Disposição de chave segura, replicação, backup e recuperação
- Storage ilimitado de chaves protegidas
- Agrupamento, balanceamento de carga e autenticação de multifator "k de n"
- Separação lógica/criptográfica ilimitada de chaves de aplicativos

Sistemas Operacionais Suportados
- Físicos: Windows, Linux, Solaris, IBM AIX, HP-UX

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

Compatibilidade e Atualizações
- Compatível com Thales nShield Connect, nShield Edge e netHSM 500 e 2000
- Software atualizável

Conectividade do Host
- Compatível com PCI 2.3; compatibilidade com 2.1, 2.2, PCI-X
- Compatível com rota única PCIe; compatível com 1.1, 2.0

Criptografia
- Algoritmos assimétricos de chave pública: 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, 512 bits)
- 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
- Critérios Comuns EAL4+

Alta Disponibilidade
- Storage de estado sólido completo
- MTBF – método de contagem de 2 peças para notificação Mil-Std 217F (consulte a tabela)

Gerenciamento e Monitoramento
- Controle de acesso remoto multi-usuário/sem operador
- Suporte de diagnósticos syslog
- Monitoramento do desempenho do Windows
- Interface de linha de comando (CLI)/interface gráfica do usuário (GUI)
- Monitoramento compatível SNMPv3

Características Físicas
- PCI padrão e fator de forma de PCIe de baixo perfil com leitor externo de cartão inteligente
- Temperatura: operação de 10 a 35°C (50 a 95°F), armazenamento entre -20 a 70°C (-4 a 158°F)
- Umidade: operacional de 10 a 90% (relativa, sem condensação a 35%) armazenamento 0 a 85% (relativa, sem condensação a 35%)
- Dimensões, peso, consumo máx. de energia e MTBF:

Modelos	Dimensões (mm/in)	Peso (g/lbs)	Alimentação (W)	MTBF (hrs)
PCI 500	107 x 129 x 15mm 4.2 x 5.1 x 0.6in	330g 0.7lb	14	193,000
PCIe 500, PCIe 6000	56.2 x 167.1 x 15.4mm 2.2 x 6.6 x 0.6in	230g 0.5lb	10	216,600
PCI 2000, PCI 4000	107 x 175 x 16.5mm 4.2 x 6.9 x 0.6in	340g 0.8lb	14	125,700

Economia de Servidores Autônomos
Ao proteger chaves criptográficas em servidores autônomos, o nShield Solo é a solução mais econômica. O nShield Solo pode ser implantado dentro de um cluster de servidores para permitir o balanceamento de carga e alta disponibilidade. Para clientes que implantam vários módulos do nShield Solo em um ambiente de Data Centers, a montagem em rack do SmartCard Reader está disponível.

Mantagem em rack opcional do nShield Leitor SmartCard.

Modelos Disponíveis e Desempenho
O nShield Solo está disponível em uma variedade de velocidades e fatores de forma:

Modelos	PCI 500	PCIe 500	PCI 2000	PCI 4000	PCIe 6000
Desempenho de assinatura (tps)					
1024bit RSA	500	500	2000	4000	6000
2048bit RSA	80	150	300	580	3000
4096bit RSA	15	65	20	40	500
Geração de chaves (tps)					
1024bit RSA	7	12.2	12	12	26.5
2048bit RSA	1	2.4	3.3	3.4	8.7
4096bit RSA	0.07	0.192	0.11	0.2	1.8

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.

Américas: 2200 North Commerce Parkway, Suite 200, Weston, Florida 33326 • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Ásia-Pacífico: Unit 4101, 41/F, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europa, Oriente Médio e África: Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com