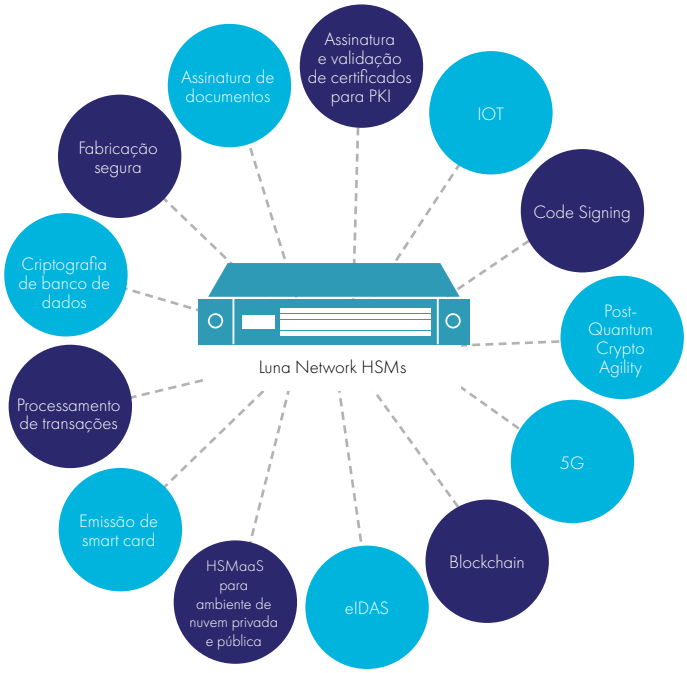
thalesgroup.com

THALES

Thales Luna Network HSM

Proteja seus dados confidenciais e aplicativos críticos armazenando, protegendo e gerenciando suas chaves criptográficas com Thales Luna Network Hardware Security Modules (HSMs) - dispositivos de alta segurança, resistentes a violações e conectados à rede com o melhor desempenho do mercado.

Entre em contato conosco para saber como você pode integrar os Luna Network HSMs em uma ampla gama de usos para acelerar operações criptográficas, proteger o ciclo de vida da chave criptográfica e fornecer uma base de confiança para toda a sua infraestrutura de criptografia.



O que você precisa saber:

Desempenho superior:

- Atenda aos seus requisitos de alta taxa de transferência com mais de 20.000 operações ECC e 10.000 operações RSA. São 20.000 operações ECC e 10.000 operações RSA por segundo para casos de uso de alto desempenho.
- Menor tempo de latência para maior eficiência

Conformidade e segurança do mais alto nível:

- As chaves sempre permanecem no hardware inviolável com certificação FIPS
- Entre em conformidade com LGDP, PCI-DSS, GDPR, eIDAS, HIPAA e outras leis
- Padrão de proteção para a nuvem
- Diversos papéis para uma eficiente separação de funções
- MofN de multiplo papéis com autenticação multifatorial para maior segurança
- Auditoria segura de logging
- Entrega de alta segurança com modo de transporte seguro
- Chaves de alta qualidade através do sistema Quantum RNG

Redução de custos e economia de tempo:

- Gerenciamento remoto de HSMs - não é necessário ir ao centro de dados
- Redução de custos e encargos de auditoria e conformidade
- Automatização de sistemas empresariais para gerenciar HSMs via REST API
- Administração de recursos com eficiência, compartilhando HSMs entre vários aplicativos ou usuários
- Políticas de segmentação flexíveis para atender às suas necessidades de gerenciamento de chaves e conformidade
- Maior portabilidade, maior eficiência e menos sobrecarga usando o SafeNet Luna Client em um container
- Funcionalidade dos módulos
  - Estende a funcionalidade nativa do HSM
  - Desenvolve e implanta códigos personalizados dentro dos limites seguros do HSM

Especificações técnicas

Sistemas operacionais aceitos

- Windows, Linux, Solaris e AIX
- Virtual: VMware, Hyper-V, Xen e KVM

Suporte de API

- PKCS#11, Java (JCA/JCE), Microsoft CAPI e CNG e OpenSSL
- REST API para administração

Criptografia

- Suporte completo para Suite B
- Assimétrico: RSA, DSA, Diffie-Hellman, Criptografia de Curva Elíptica (ECDSA, ECDH, Ed25519, ECIES) com curvas Brainpool nomeadas e definidas pelo usuário, KCDSA e outros
- Simétrico: AES, AES-GCM, Triple DES, DES, ARIA, SEED, RC2, RC4, RC5, CAST e outros
- Hash/Message Digest/HMAC: SHA-1, SHA-2, SM3 e outros
- Derivação de chave: SP800-108 Counter Mode
- Encapsulamentos de chave: SP800-38F
- Geração de números aleatórios: projetado para atender às normas AIS 20/31 até DRG.4 usando fonte de ruído real baseada em HW juntamente com a norma NIST 800-90A CTR-DRBG.
- Criptografia de carteira digital: BIP32
- Mecanismo de criptografia 5G para autenticação de assinantes: Milenage, Tuak e Comp 128

Certificados de segurança

- FIPS 140-2 nível 3 – senha e multifatorial (PED)
- eIDAS CC EAL4+ (AVA_VAN.5 and ALC_FLR.2) contra o perfil de proteção 419221-5*

Interface de hospedagem

- 4 entradas Gigabit Ethernet com Port Bonding ou 2 conetividades de rede de fibra de 10G e 2 Port bonding de 1G
- IPv4 e IPv6

Características físicas

- Equipamento de montagem padrão 1U 19 in.
- Dimensões: 19" x 21" x 1,725" (482,6 mm x 533,4 mm x 43,815 mm)
- Peso: 28 lb (12,7 kg)
- Voltagem de entrada: 100-240 V, 50-60 Hz
- Consumo de energia: 110 W (máximo), 84 W (típico)
- Dissipação de calor: 376BTU/hr (máxima), 287BTU/hr (típica)
- Temperatura: operacional (0°C – 35°C), armazenamento (-20°C – 60°C)
- Umidade Relativa: 5% a 95% (38°C) não-condensável

Conformidade com as normas ambientais e de segurança

- UL, CSA e CE
- FCC, CE, VCCI, C-TICK e KC Mark
- RoHS2 e WEEE
- TAA

Segurança

- Fontes de alimentação removíveis sem desconexão
- Componentes que podem ser consertados no local
- Tempo médio entre falhas (MTBF) 171,308 horas

Gerenciamento e monitoramento

- Recuperação de desastre HA
- Backup e restauração de hardware localmente ou em nuvem
- SNMP e Syslog

* em avaliação

Modelos disponíveis

Escolha entre duas séries de Luna Network HSMs, cada uma com 3 modelos diferentes para atender às suas necessidades.

Série Luna A: autenticação de senha para gerenciamento fácil.

A700	A750	A790
Memória de 2 MB	Memória de 16 MB	Memória de 32 MB
Segmentações: 5	Segmentações: 5	Segmentações: 10
Máximo de segmentações: 5	Máximo de segmentações: 20	Máximo de segmentações: 100

Desempenho padrão:	Desempenho empresarial:	Desempenho máximo:
RSA-2048: 1.000 tps	RSA-2048: 5.000 tps	RSA-2048: 10.000 tps
ECC P256: 2.000 tps	ECC P256: 10.000 tps	ECC P256: 22.000 tps
AES-GCM: 2.000 tps	AES-GCM: 10.000 tps	AES-GCM: 17.000 tps

Série Luna S: autenticação multifatorial (PED) para casos de uso que necessitam de maiores garantias.

S700	S750	S790
Memória de 2 MB	Memória de 16 MB	Memória de 32 MB
Segmentações: 5	Segmentações: 5	Segmentações: 10
Máximo de segmentações: 5	Máximo de segmentações: 20	Máximo de segmentações: 100

Desempenho padrão:	Desempenho empresarial:	Desempenho máximo:
RSA-2048: 1.000 tps	RSA-2048: 5.000 tps	RSA-2048: 10.000 tps
ECC P256: 2.000 tps	ECC P256: 10.000 tps	ECC P256: 22.000 tps
AES-GCM: 2.000 tps	AES-GCM: 10,000 tps	AES-GCM: 17.000 tps

tsp = transações por segundo

Sobre a Thales

As pessoas em quem você confia para proteger sua privacidade confiam na Thales para proteger seus dados. Em termos de segurança de dados, as organizações enfrentam cada vez mais momentos decisivos. Seja na criação de uma estratégia de criptografia, migração para a nuvem ou cumprimento de normas de conformidade, você pode confiar na Thales para proteger sua transformação digital.

Tecnologia decisiva para momentos decisivos.

© Thales - Dezembro 2019 • BB, v30

> thalesgroup.com <

Américas – Thales eSecurity Inc. 2125 Zanker Rd, San Jose, CA 95131 USA • Tel.:+1 888 744 4976 ou +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Ásia-Pacífico – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 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