KRYPTUS
shaping trusted bonds

kNET network HSM

hsm.kryptus.com

KRYPTUS kNET HSM

KRYPTUS kNET é um Módulo de segurança de hardware (HSM) com certificação FIPS que protege aplicativos críticos garantindo a segurança de chaves e softwares sensíveis com desempenho de nível superior (até 30.000 transações RSA 2048 por segundo).

Por ser totalmente interoperável e flexível para personalizações, o kNET permite uma integração simples e perfeita com os aplicativos existentes, ao mesmo tempo que garante a execução segura das funcionalidade e possibilita um ambiente multi-tenant, que contribuem para a redução de gastos com implementação e expansão de sistemas.

Preparado para ambientes de alta disponibilidade kNET é perfeito para aplicativos PKI, Cloud, Payment e Blockchain.

SECURE CODE EXECUTION

O KRYPTUS kNET HSM permite que os clientes executem seus códigos em um ambiente à prova de violação, protegendo a lógica do aplicativo e quaisquer parâmetros de segurança críticos. O aplicativo é verificado pelo HSM quanto à sua integridade e autenticidade antes de cada execução, assegurando que a aplicação não seja comprometida ou modificada de nenhuma maneira. Uma vez verificada, a aplicação tem acesso privilegiado à seus objetos privados, no qual não podem ser acessados por aplicações externas.

HIGHLIGHTS

-Desempenho (Até 30.000 RSA 2048 TPS)

- FIPS 140-2 nível 3 (EFP/EFT)

-ICP Brasil MCT7 NSH3

-Execução segura de código

-Separação em HSM virtuais (até 50 partições)

-Gestão Remota

-Alta Disponibilidade (Fonte de alimentação dual Hot Swap e Dual Gigabit Ethernet)

-Balanceamento de carga

-KMIP (Key Management Interoperability Protocol) suporte nativo Sem necessidade de drivers

-Simulador de software do HSM para POC e Desenvolvimento de Aplicações.

fale.conosco@kryptus.com
+55 (19) 3112-5000

kryptus.com

KRYPTUS
shaping trusted bonds

Virtual HSMs

The ability to create Virtual HSMs (up to 50) running within the kNET hardware enables real insulation in multi-tenant scenarios, separating key-sets, stakeholders, and application in the most secure way.

TECHNICAL SPECS

FEATURES AND SERVICES

- Multi tenant : até 50 HSM virtuais
- Balanceamento de carga e suporte de alta disponibilidade
- Gestão remota através de GUI (Windows, Linux, OS X)
- Smartcard, token USB + PIN, Usuário + Senha
- Autenticação de segundo fator (TOPT, HOPT)
- Simulador de software para desenvolvimento e avaliação
- Execução segura de código
- Monitoramento por SNMPv3 (com armadilhas)

PHYSICAL SPECIFICATIONS

-Fator de forma de 19" 1U
- 1 x porta USB (Smart Card ,
- Fonte de alimentação dupla hot swap (100~240V)
- Interfaces Gigabit Ethernet Dual no painel frontal
- Display LCD no painel frontal
- Porta Serial no painel frontal
- Selos a prova de intrusão no gabinete externo
- Detecção de intrusão na abertura do gabinete externo

INTERFACES

- 2x RJ45 Network Interfaces - 10/100/1000 Mbps
- Front-panel LCD Display
- Front-panel Serial Console Port
- Porta USB

SEGURANÇA E CONFORMIDADE AMBIENTAL

- FCC and RoHS

CONFIABILIDADE

Manutenção em campo e fontes de alimentação de troca dupla

CRIPTOGRAFIA

Assimétrica:
- RSA (até to 8192 bits), DSA, ECIES, ECDSA (NIST e Brainpool e curvas secp256k1), EdDSA (Curva25519, Ed448-Goldilocks e E-521) e mais

Simetrica:
- AES, 3DES, DES, AES-GSM, e mais

Hash/HMAC/Message Digest:
- MD5, SHA-1, SHA-2, SHA-3, e mais

APIs

- Nativo KMIP – Sem necessidade de drivers
- PKCS#11
- Java (JCA/JCE)
- Microsoft CNG / CAPI
- OpenSSL Engine
- Integração com C++/, Java, Python e JavaScript

PERFORMANCE

- Até 30.000 RSA 2048 transações por segundo
- Armazena até to 2,5 milhões de objetos

CERTIFICAÇÃO E COMPLIANCE

- FIPS 140-2 nível 3+ (EFP/EFT)
- ICP-Brasil MCT7 NSH3
- PCI Compliance
- Common Criteria EAL 4+ augmented AVA_VAN.5 and ALC_FLR.3 eIDAS (EN-419-221-5 e EN 419 241-2)*

*Sob certificação

fale.conosco@kryptus.com
+55 (19) 3112-5000

kryptus.com

kNET network HSM