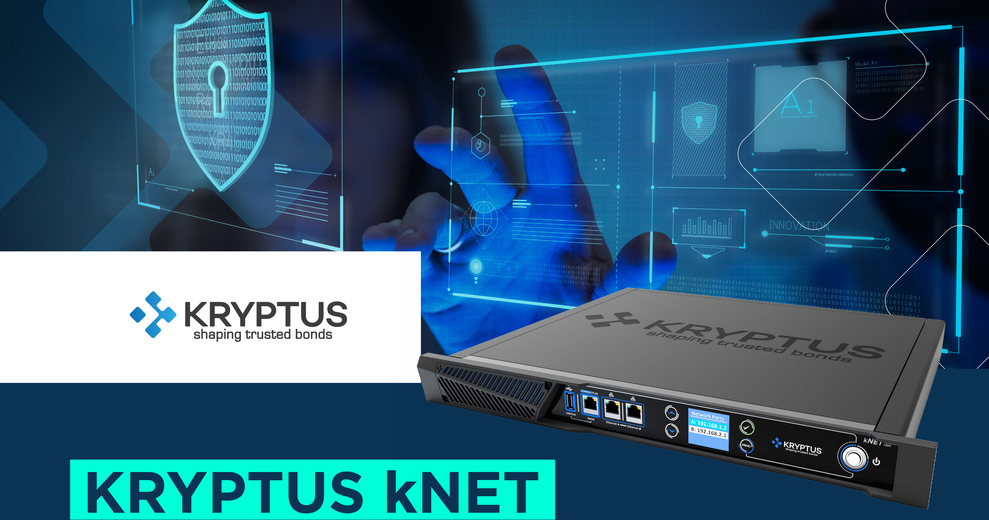

KRYPTUS
shaping trusted bonds

KRYPTUS kNET

ENTRY

KRYPTUS kNET é um Módulo de segurança de hardware (HSM) com certificação Common Criteria EAL4+, FIPS 140-2 e MCT7 que protege aplicativos críticos garantindo a segurança de chaves e softwares sensíveis com desempenho de nível superior (até 10.000 transações de assinatura 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 funcionalidades e possibilita um ambiente multi-tenant, que contribui para a redução de gastos com implementação e expansão de sistemas. Preparado para ambientes de alta disponibilidade kNET é perfeito para aplicações de Proteção de Dados, PKI, Pagamentos, Blockchain e operações em nuvem.

Certified Common Criteria EAL4+

FIPS Level 3 Certified 140-2

PED

ICP Brasil

Highlights

- Certificado NIST CAVP para Pós-quântico
- Certificado Common Criteria EAL 4+
- Certificado NIST FIPS 140-2 L3
- Certificado ICP Brasil MCT7 NSH3
- Alto desempenho (até 10.000 assinaturas RSA 2048 por segundo*)
- Ambiente "trials" na nuvem para POC
- 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)
- Replicação automática e balanceamento de carga
- KMIP (Key Management Interoperability Protocol) com suporte nativo (sem necessidade de drivers)

EXECUÇÃO SEGURA DE CÓDIGO

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, o usuário poderá acessar seus objetos e realizar operações criptográficas definidas em seu aplicativo seguro.

HSMs VIRTUAIS

A capacidade de criar HSMs virtuais (até 50*) executados no hardware kNET permite o isolamento real em cenários multi-tenant, separando conjuntos de chaves, partes interessadas e aplicativos da maneira mais segura possível.

ESPECIFICAÇÕES TÉCNICAS

CAPACIDADES

- Multi tenant: até 50 HSM virtuais*
- Balanceamento de carga e suporte de alta disponibilidade
- Gestão remota através de GUI (Windows, Linux, OS X)
- Modos de autenticação disponíveis: smartcard, token USB + PIN, Usuário + Senha e Certificado + Chave
- Autenticação de segundo fator (TOPT, HOPT)
- Execução segura de código
- Monitoramento por SNMPv3 (com armadilhas)

ESPECIFICAÇÃO FÍSICA

- Fator de forma de 19" 1U
- 1x porta USB (para exportação/importação de backup)
- Fonte de alimentação dupla hot swap (100~240V) 50-60 Hz
- Dimensões (HxWxL): 44,42 x 486 x 360 mm
- Peso: 6,1 kg
- Consumo de energia: 60W típico
- Temperatura de funcionamento e armazenamento: 0°C - 40°C
- Umidade relativa: 5% a 95% (38°C) sem condensação
- Selos à prova de intrusão no gabinete externo
- Detecção de intrusão na abertura do gabinete externo
- Modos de autenticação disponíveis: smartcard, token USB + PIN, Usuário + Senha e Certificado + Chave

INTERFACES

- 2 Interfaces de rede RJ45 - 10/100/1000 Mbps
- Painel frontal com display LCD
- Porta do console serial no painel frontal
- Porta USB

SEGURANÇA E CONFORMIDADE AMBIENTAL

- FCC e RoHS

CONFIABILIDADE

Bandeja do ventilador que pode ser reparada em campo e fontes de alimentação de troca dupla

CRIPTOGRAFIA

Assimétrica:
- ML-DSA (Post-quantum)
- ML-KEM (Post-quantum)
- RSA: Até 8192 bits;
- ECDSA: Curvas NIST (P-224, P-256, P-384 e P-521); Curvas Brainpool: Brainpool P224 (r1/t1), Brainpool P256 (r1/t1), Brainpool P320 (r1/t1), Brainpool P384 (r1/t1) e brainpool P512 (r1/t1);
- EdDSA: Curvas de Edwards (Ed25519, Ed448 e Ed521)
- ECIES: Utilizando os modos de operação CBC, CTR e GCM

Simétrica:
- AES: 128, 192 e 256 bits nos modos de operação ECB, CBC, CTR e GCM
- DES e 3DES: utilizando os modos de operação ECB, CBC e CTR

- Hash: Famílias SHA-1, SHA-2 e SHA-3

- MAC: HMAC SHA-1, HMAC SHA-2, HMAC-MD5, CBC-MAC, CMAC

Pagamentos:
- DUKPT
- Translate PIN
- Reformat PIN
- TR31
- Calculate CVV
- Generate EMV Cryptogram

APIs

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

PERFORMANCE

- Até 10.000 RSA 2048 transações por segundo*
- Armazena até 2,5 milhões de objetos*

CERTIFICAÇÃO E COMPLIANCE

- FIPS 140-2 nível 3
- FIPS 140-3 nível 3 (em certificação)
- ICP-Brasil MCT7 NSH3
- PCI Compliant (em certificação)
- Common Criteria EAL 4+ aumentado AVA_VAN.5 e ALC_FLR.3 eIDAS (EN-419221-5:2018)

*As capacidades exatas dependem de licenciamentos específicos e representam capacidades máximas, dependentes de casos de uso. Opções padrão para desempenho: TPSR2K0050 (até 50 RSA2K/s), TPSR2K0400 (até 400 RSA2K/s), TPSR2K2500 (até 2.500 RSA2K/s), TPSR2K10K (até 10.000 RSA2K/s). Opções para armazenamento: MO2K (até 2 mil objetos), MO100K (até 100 mil objetos), MO2M5 (até 2,5 milhões de objetos). Opções para HSMs virtuais: VH00 (sem a capacidade), VH10 (até 10 HSM virtuais) VH50 (até 50 HSMs virtuais). Capacidades customizadas sob consulta.

KRYPTUS
shaping trusted bonds

HQ
+55 (19) **3112-5008**
faleconosco@kryptus.com

Rua Maria Teresa Dias da Silva 270
Campinas – SP, Brazil

GLOBAL OPERATIONS
+41 **79 932 19 23**
kryptus.emea@kryptus.com

Rue Galilée 7, 1400
Yverdon-les-Bains, Switzerland

www.kryptus.com

bsi ISO 9001 Quality Management Systems CERTIFIED FS 598154
ISO/IEC 27001 Information Security Management CERTIFIED IS 719722
ISO/IEC 27701 Privacy Information Management CERTIFIED PM 789059
ISO/IEC 20000-1 IT Service Management CERTIFIED ITMS 822730

NATO AQAP 2110

EED EMPRESA ESTRATÉGICA DE DEFESA

Follow us