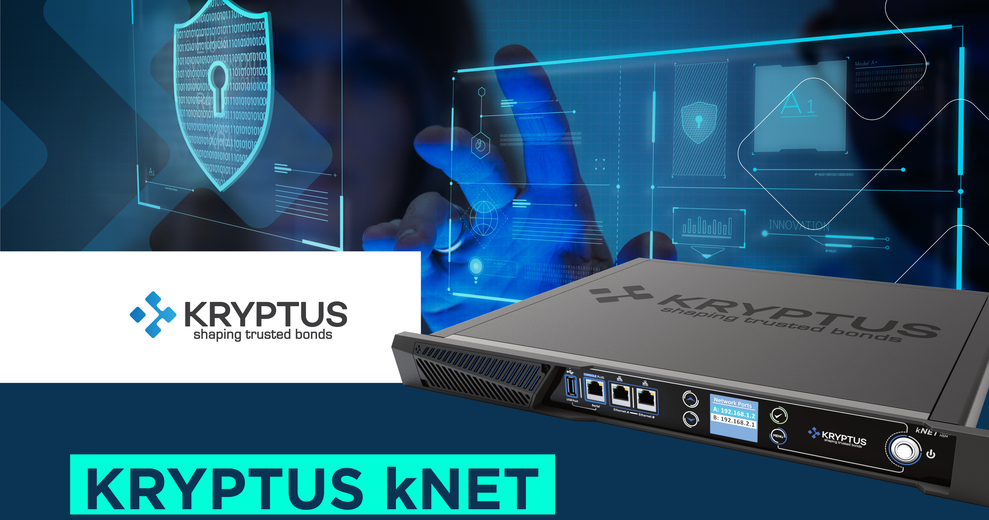

KRYPTUS
shaping trusted bonds

KRYPTUS kNET
NETWORK HSM

KRYPTUS kNET is a hardware security module (HSM) with Common Criteria EAL4+, FIPS 140-3 and MCT7 certification that protects critical applications by ensuring the security of sensitive keys and software with superior performance (up to 10,000 RSA 2048 signature transactions per second*).

Being fully interoperable and flexible for customizations, kNET allows for simple and seamless integration with existing applications while ensuring the secure execution of functionalities. It also enables a multi-tenant environment, contributing to reduced costs in system implementation and expansion.

Designed for high-availability environments, kNET is perfect for Data Protection, PKI, Payments, Blockchain, and cloud operations.

Certified Common Criteria EAL4+ · FIPS Level 3 Validated 140-3 · Strategic Defense Product · ICP Brasil

Highlights

- NIST CAVP Certified for Post-Quantum
- Common Criteria EAL 4+ Certified
- NIST FIPS 140-3 Level 3 Certified
- ICP-Brasil MCT7 NSH3 Certified
- High performance (up to 10,000 RSA 2048 signatures per second*)
- Cloud “trials” environment for POC
- Secure code execution
- Separation into virtual HSMs (up to 50 partitions)
- Remote management
- High availability (Dual Hot-Swap Power Supply and Dual Gigabit Ethernet)
- Automatic replication and load balancing
- KMIP (Key Management Interoperability Protocol) with native support (no drivers required)

SECURE CODE EXECUTION

The KRYPTUS kNET HSM allows clients to run their code in a tamper-proof environment, protecting the application logic and any critical security parameters. The application is verified by the HSM for its integrity and authenticity before each execution, ensuring that it has not been compromised or modified in any way. Once verified, the user can access their objects and perform cryptographic operations as defined in their secure application.

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: up to 50 virtual HSMs*
- Load balancing and high availability support
- Remote management via GUI (Windows, Linux)
- Available authentication modes: smartcard, USB token + PIN, User + Password, and Certificate + Key
- Two-factor authentication (TOTP, HOTP)
- Secure code execution
- Monitoring via SNMPv3 (with traps)

PHYSICAL SPECIFICATIONS

- 19” 1U form factor
- - 1x USB port (for backup export/import)
- Dual hot-swap power supply (100~240V), 50-60 Hz
- Dimensions (HxWxL): 44.42 x 486 x 360 mm
- Weight: 6,1 kgs
- Power Consumption: 60W typical
- Operating and storage temperature: 0°C – 40°C
- Relative Humidity: 5% to 95% (38°C) non-condensing
- Tamper-evident seals on external enclosure
- Tamper-detection of external enclosure opening
- Available authentication modes: smartcard, USB token + PIN, User + Password, and Certificate + Key

INTERFACES

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

SAFETY AND ENVIRONMENTAL COMPLIANCE

- FCC and RoHS

RELIABILITY

Field serviceable fan tray and dual-swap power supplies

CRYPTOGRAPHY

Asymmetric:
- ML-KEM (Post-quantum, FIPS 203)
- ML-DSA (Post-quantum, FIPS 204)
- SLH-DSA (Post-quantum, FIPS 205)
- RSA: Up to 8192 bits
- ECDSA: NIST curves (P-224, P-256, P-384, and P-521); Brainpool curves: Brainpool P224 (r1/t1), Brainpool P256 (r1/t1), Brainpool P320 (r1/t1), Brainpool P384 (r1/t1), and Brainpool P512 (r1/t1)
- EdDSA: Edwards curves (Ed25519, Ed448, and Ed521)
- ECIES: Using CBC, CTR, and GCM operation modes

Symmetric:
- AES: 128, 192, and 256 bits in ECB, CBC, CTR, and GCM operation modes
- DES and 3DES: Using ECB, CBC, and CTR operation modes
- Hash: SHA-1, SHA-2, and SHA-3 families
- MAC: HMAC SHA-1, HMAC SHA-2, HMAC-MD5, CBC-MAC, CMAC

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

APIs

- Native KMIP Support – No drivers needed
- PKCS#11
- Java (JCA/JCE)
- Microsoft CNG / CAPI
- OpenSSL Engine
- Integration with C++/, Java, Python and JavaScript

PERFORMANCE

- Up to 10.000 RSA 2048 Transactions per Second*
- Stores up to 2,5 million objects*

CERTIFICATION AND COMPLIANCE

- FIPS 140-3 Level 3
- ICP-Brasil MCT7 NSH3
- PCI Compliant (under certification)
- Common Criteria EAL 4+ augmented AVA_VAN.5 and ALC_FLR.3 eIDAS (EN-419221-5:2018)

*Exact capabilities depend on specific licensing and represent maximum capacities, subject to use cases. Standard performance options: TPSR2K0050 (up to 50 RSA2K/s), TPSR2K0400 (up to 400 RSA2K/s), TPSR2K2500 (up to 2,500 RSA2K/s), TPSR2K10K (up to 10,000 RSA2K/s). Storage options: MO2K (up to 2,000 objects), MO100K (up to 100,000 objects), MO2M5 (up to 2.5 million objects). Virtual HSM options: VH00 (without the capability), VH10 (up to 10 virtual HSMs), VH50 (up to 50 virtual HSMs). Customized capacities available upon request.

KRYPTUS
shaping trusted bonds

HQ
+55 (19) **3112-5000**
faleconosco@kryptus.com
www.kryptus.com
Rua Maria Teresa Dias da Silva 270
Campinas – SP, Brazil

EMEA
+41 **79 932 19 23**
kryptus.emea@kryptus.com
emea.kryptus.com
Rue Galilée 7, 1400, Yverdon
Switzerland

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

Follow us