



# KNET HSM: PAYMENTS

Payment institutions can rely on KRYPTUS' KNET HSM for Payments to ensure a robust infrastructure that complies with security standards. Approved by the strictest international standards and highly flexible, KNET can be adapted to different business models.

KRYPTUS KNET HSM is able to follow technological developments in a fast manner, reducing operation costs. The solution combines the strictest security standards and high processing with up to 10,000 transactions per second (TPS) – all in a single device.

KNET is designed to meet all auditing requirements for current and emerging security standards, such as FIPS and PCI.

Its certified Level 3 FIPS 140-3 cryptographic module has been fully tested and validated by customers in the payment industry who have undergone PCI audits.

KNET supports several cryptographic algorithms, such as AES, Triple DES, RSA, ECDSA, EdDSA, ECIES, and Hash, among others, in addition to featuring post-quantum algorithms validated by NIST, including ML-KEM, ML-DSA, and SLH-DSA.

The solution features a TR-31 key block – an added layer of security for quick identification of false keys.



## ADVANTAGES OF THE KRYPTUS KNET HSM

- Best cost/benefit ratio
- Local and responsive technical support
- FIPS certificate
- PCI Compliance
- Features ready for integration

**Guaranteed interoperability between payment HSMs**

## PAYMENT APPLICATIONS



- Tokenization of payment services
- Issuance and secure processing of EMV cards
- EMV cryptogram verification and generation
- Preparation of data from EMV chip cards (credit, debit, meal vouchers, with contact and contactless);
- Management of EMV certificates for Private Label cards using public and private keys



- Authorization of transactions by encrypted keys
- TR-31 key blocks for secure exchange of keys between devices
- Translate/Reformat PIN feature for PIN Format unlocking and change in Transactions
- PAN encryption
- Point-to-point encryption (P2PE)
- Message authentication (MAC, CMAC, HMAC, Hash)



- Script updates on cards without remission using all HSM security and the EMV standard:
  - Unblock PIN
  - Change PIN
  - Application Block
  - Application Unblock
  - Put Data
  - Update Record
  - DUKPT keys derivation



**HQ**  
+55 (19) **3112-5000**

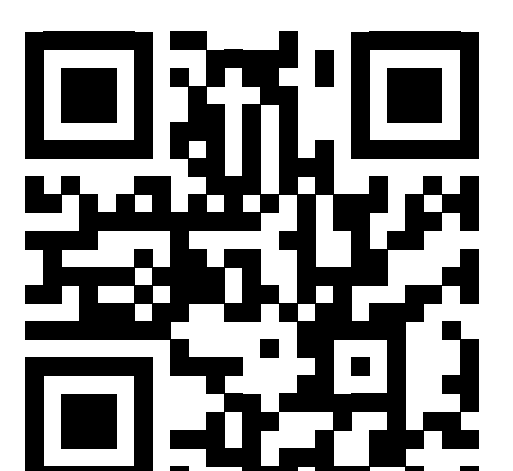
faleconosco@kryptus.com  
www.kryptus.com

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



Follow us  
f @ in