



Features and Benefits

Security Features

- Two-factor Authentication of security officers using optional smart cards
- Physical lock and/or smart cards control authorisation levels
- Tamper-resistant & Tamper-responsive (e.g. Detection of cover removal, unauthorised access attempt, memory erase)
- Device Function's Access Customisation - Disable functions not required by the application to minimise potential risks
- Audit Logs

Operational Features

- Industry leading performance. Achieve up to 15000 t.p.s⁽¹⁾ using a single Cryptosec Banking⁽²⁾
- Remote HSM Manager eliminates the requirement of security admin travels thereby reducing costs.
- Robust features in the form of dual power supplies and dual Giga-Ethernet ports to maximise uptime.
- Software-updates. Stay up to date with periodical updates. Standards and regulatory changes require frequent system updates. Obtain peace of mind with all-included update service.
- Detailed documentation and dedicated support to ease the deployment process.

Cryptosec Banking

Network-attached cryptographic server for banking and payment cards

Overview

Cryptosec Banking is a high-performance network-attached financial cryptographic server equipped with full functionality to ensure transaction security and key storage. The server integrates all the standard commands and functions of the banking and security sectors, including EMV.

The Cryptosec Banking solution is a reliable HSM and is used extensively by numerous banks across the world. It complies with the latest EMV standards applicable to smart cards, contactless cards and mobile transactions, and is compatible with the main Payment Card software applications e.g. Card Verification, ATM Interchange, Cash Card Reloading, Data Integrity, Chip Card Transaction Processing, etc.

Cryptosec Banking is the only HSM designed for the financial sector offering full functionality based on standards without any future costs for the addition of new cryptographic functions or commands. Thanks to the continuous updates, our customers are not required to replace their servers every few years due to standard or functionality obsolescence.

All these features when combined with the superior performance (up to 15000 t.p.s.) and excellent cost-benefit ratio to maximize ROI, make Cryptosec Banking the smartest choice HSM for the banking sector.



Payment Systems

- PIN and smart card verification functions for VISA/MasterCard/American Express.
- EMV 3.X and 4.X transactions and messaging, including encryption command sequences and digital signatures: DAC and IDN calculation/validation, ARQC verification and ARPC generation.
- PIN functions: PIN calculation and verification (DUKPT), PIN management, offset calculation and PIN translation, Printing of PINs in blind envelopes.
- Validation codes: code calculation and verification, CVC calculation and verification.

Specifications

Key Management

- RSA Remote Key Transport
- DUKPT for PIN and Data Encryption
- Master/Session Key Scheme

Cryptographic Algorithms

- Symmetric:
 - DES & Triple-DES (Key lengths 112 or 168 bit)
- Asymmetric
 - RSA (up to 2048 bit)
- Hashing & MAC
 - SHA-1
 - SHA-2 (224, 256, 384, 512)
 - MD5
 - 3DES X9, 3DES X9.19 (Retail-MAC)
 - HMAC-SHA-1, HMAC-SHA-2

Certifications

- FIPS 140-2 Level 3 crypto module
- Meets FIPS 46, 81, 180-3, 186-3 and 198 standards
- ISO 9564, 10118, 11568, 13491, 16609
- ANSI X3.92, X9.8, X9.9, X9.17, X9.19, X9.24, X9.31, X9.52, X9.97, X9 TR-31, X9 TG-3/TR-39
- NIST SP800-20, SP800-90(A)
- Support of FIPS 198-1 HMAC

Host Connectivity

- TCP/IP (Dual Gigabit Interface)
- Asynchronous (VT-100 Terminal)

Electrical and Physical Characteristics

- Networking: Dual Gig-E (100/1000 Mbps)
- Power: Dual Power supply for resilience
- Dimension: 2U 19" rack
- Operating Temperature: 10°C to 35°C
- Operating Humidity: 10 % to 90% non-condensing
- Environment Temperature: -20°C to 60°C
- Power Requirements: AC 100 to 240 V (50/60 Hz)
- Power Consumption: 100W

⁽¹⁾ Performance may vary depending on type of transaction and external factors such as network connectivity.

⁽²⁾ Realsec recommends deployment of minimum 2 units to avoid data loss and reduce recovery times in case of unexpected disaster.

⁽³⁾ Crytosec Banking is compatible with most applications offering support for Thales payShield 9000.

Applications Supported⁽³⁾

ACI: BASE24, Postilion

Aconite: Affina Enterprise, Mobile Application Manager

BPC: SmartVista

Clear2Pay: Open card System

CompassPlus: TranzWare Online, TranzWare Card Factory

CR2: BankWorld, CardWorld

CreditCall: CardEase Mobile

CSFi: SWITCHWARE

Euronet: Integrated Transaction Management

First Data: VisionPlus

FIS: Connex, Cortex

Gemalto: Ezio on Mobile

Jack Henry Banking: jhaPassPort

Lusis: Tango

OpenWay: Way4, Way4 Data Preparation and Card Personalisation

Prime Factors: Bank Card Security System

Royal Gate: Paygate

RS2: Bankworks, Bankworks Issuing

Tieto: Payment Suite, Card Suite

TII Smart Solutions: TranServer

TPS: IRIS Enterprise Switch

TSYS: Prime, Prime Issuer

Wincor Nixdorf: ProcClassic/Enterprise



Ultra Electronics

AEP

Knaves Beech Business Centre

Loudwater

High Wycombe

Buckinghamshire, HP10 9UT

Main Switchboard: +44 (0)1628 642 600

Email: info@ultra-aep.com

www.ultra-aep.com

www.ultra-electronics.com

