securosys

fact sheet

Primus HSM CyberVault Core

The Hardware Security Module with Unmatched Performance-Price Ratio

The Securosys Primus CyberVault Core (E2-Series) delivers enterprise-grade security at an unbeatable performance-to-price ratio. Designed, developed, and manufactured in Switzerland, this entry-level device provides high-performance cryptographic functionality while ensuring cost efficiency and ease of use.

Built as a standalone network appliance, it eliminates the limitations of PCIe-based HSMs, reducing additional hardware dependencies and potential points of failure. With flexible, in-field upgradeability, the CyberVault Core is ideal for securing financial transactions, managing cryptographic keys, and enabling secure cloud access. Its rapid setup, advanced tamper protection, and seamless integration make it the trusted choice for a wide range of security applications.

Key Benefits

Unbeatable Price-Performance Ratio

The CyberVault Core delivers full network appliance functionality at a PCIe card price level, eliminating embedded HSM limitations.

Seamless Integration

The Primus CyberVault Core HSM offers broad compatibility through fully documented APIs, including PKCS#11, CNG/KSP, Java, and REST. It features two dedicated partitions, each with 120MB storage space, ensuring secure, parallel access for multiple applications within any network environment.

Advanced Tamper & Transport Protection

Exceeds FIPS and Common Criteria standards with active tamper sensors, protecting even when unpowered.

Secure & Efficient Remote Management

Decanus enables secure remote administration of HSMs and partitions, reducing operational effort.

Optical Interface for High-Speed Connectivity

For enhanced networking flexibility, the CyberVault Core offers – besides four 1GB standard network ports – optionally also two 10 Gbps optical interface ports, ensuring high-speed connectivity in any IT network architecture.

Comprehensive Cryptographic Support

Supports RSA, ECC, EdDSA, and and optionally supports all NIST-selected post-quantum cryptographic algorithms, including ML-DSA, SLH-DSA, ML-KEM,
HSS-LMS, and XMSS, ensuring future-proof encryption.

Rapid Deployment & Low Maintenance

Quick setup with an intuitive wizard, reducing installation time, complexity, and maintenance efforts.

Designed, developed, and manufactured in Switzerland.

Security Features

Security Architecture

- Multi-barrier software and hardware architecture with supervision mechanisms
- Secure supply-chain

Encryption/Authentication (extract)

- Post-Quantum Cryptographic (PQC) algorithms (optional) ML-DSA, SLH-DSA, ML-KEM, HSS-LMS, XMSS
- RSA 1024-8192, DSA 1024-8192
- ECDSA 224-521, GF(P) arbitrary curves (NIST, Brainpool, ...)
- ED25519, Curve25519
- Diffie-Hellman 1024, 2048, 4096, ECDH
- SHA-3/SHA-2 (224 - 512), SHA-1, RIPEMED-160, Keccak
- HMAC, CMAC, GMAC, Poly 1305
- 128/192/256-Bit AES with GCM-, CTR-, ECB-, CBC-, MAC Mode
- Camellia, ChaCha20-Poly1305, ECIES

Key Generation

- Two hardware true random number generators (TRNG)
- NIST SP800-90 compatible random number generator

Key Management

- 2 partitions and 240MB total storage, fixed

Operation

- Number of client connections not restricted
- Unlimited number of backups

Anti-Tamper Mechanisms

- Several sensors to detect unauthorized access
- Active destruction of key material and sensitive data on tamper
- Transport and multi-year storage tamper protection by digital seal

Attestation and Audit Features

- Cryptographic evidence of audit relevant parameters (keys, configuration, hardware, states, logs, time-stamping)

Identity-based Authentication

- Multiple security officers (m out of n)
- Identification based on smart card and PIN

Networking Features

Software Integration

- JCE/JCA provider
- PKCS#11 provider, OpenSSLv3
- Microsoft CNG/KSP provider
- RESTful API

Networking

- IPv4/IPv6
- Interface bonding (LACP or active/backup)
- Active clustering of multiple units for load-balancing and fail-over
- Monitoring and log streaming (SNMPv2, syslog/TLS)

Device Management

- Local configuration (Console)
- Remote administration (Decanus Terminal)
- Local and remote firmware update
- Secure log and audit
- Enhanced diagnostic functions

Technical Data

Performance (transactions per second)

Signing	
RSA 2048 – 8192	25
EC 256	250
ED 25519	250
AES	250
ML-DSA-44	25
Key creation	
RSA 2048	6

Power

- Two redundant power supplies, hot pluggable 100 ... 240 V AC, 50 ... 60 Hz
- Power dissipation: 65 W (typ.), 100 W (max.)
- Backup lithium battery: Lithium Thionyl Chloride 0.65g Li, IEC 60086-4, UL 1642, 3.6V

Interfaces

- 4 Ethernet RJ-45 ports with1 Gbps (rear)
- 2 SFP+ slots for optical 10Gbps Ethernet modules (rear; optional)
- 1 Console ports (RJ45, rear)
- 1 USB-A management ports (rear)
- 1 USB-C management port (rear)

Controls

- 4 LEDs for system and interface status (multicolor)
- Console interface
- Optional Decanus Terminal for remote administration

Environmental Test Specifications

- EMV/EMC: EN 55022, EN 55024, FCC Part 15 Class B
- Safety: IEC 62368-1

Specifications

- Temperature ranges (IEC 60068-2-1 Ad, IEC 60068-2-2 Bd): storage -20 ... +60 °C; operation 0 ... +35 °C
- Humidity (IEC 60068-2-78 Cab): 40 °C, 93% RH, non-condensing
- MTBF (RIAC-HDBU-217Plus) at t_{amb}=25 °C: >100 000 h
- Dimensions (w×h×d) 417×44×365 mm (1U 19" EIA standard rack)
- Weight 7.5kg

Certifications

- FIPS140-3 Level 3 (in certification)
- Common Criteria EAL4+ (in certification)
  - CC EN 419221-5 eIDAS protection profile
- CE, FCC, UL

Front

Rear

Visit our website

HEADQUARTER
Securosys SA
Max-Högger-Strasse 2
8048 Zürich
Switzerland

+41 44 552 31 00
info@securosys.com
www.securosys.com

We strive to continuously improve our offerings and therefore reserve the right to change specifications without notice. Designed and manufactured in Switzerland.