securosys

The Hardware Security Module for highest performance

Primus HSM X Cyber Vault

- Market-leading encryption and authentication performance
- The fastest HSM in the market:
  - Over 50 000 concurrent transactions per second
  - Scalable to over 1 000 000 concurrent transactions per second
- Post-Quantum Cryptographic algorithms
- Tamper protection during transport, storage, and operation
- Simple setup, easy commissioning, configuration, and maintenance
- Scalable and flexibly partitionable to your needs
- Designed, developed, and manufactured in Switzerland

The Securosys Primus X Cyber Vault delivers market-leading performance and meets the highest requirements in safety, availability, flexibility and tamper protection. Integrating the devices to existing systems is as effortless as the initial commissioning and setup.

Outstanding performance

With an impressive performance of over 50,000 transactions per second (TPS) and its scalability in a clustered environment to over one million TPS, the Primus X Cyber Vault sets a new benchmark in the industry. It also supports post-quantum cryptography (PQC) and enables hybrid signatures – while maintaining the same throughput.

The devices are ideally suited to secure high volumes of financial transactions, blockchain systems and crypto asset management, among others.

Functions

The Primus X Cyber Vault generates keys, stores them and manages their distribution. Besides key management, the devices perform authentication and encryption tasks. Primus X Cyber Vault supports PQC algorithms, symmetric (AES) and asymmetric encryption (RSA, Diffie-Hellman, ECDSA), as well as hash (SHA-2, SHA-3) algorithms among others. Multiple Primus HSMs can be grouped together (high availability clustering) to support redundancy and load balancing. They can be integrated seamlessly and easily into any network environment, having both copper and optical interfaces up to 10 Gbps. The devices can be remotely administered with our Decanus Control Terminal, and they come with a standardized backup function via USB and WebDav.

Security Features

Security Architecture

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

Encryption/Authentication (extract)

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

Key Generation

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

Key Management

- Key capacity: up to 30 GB
- Up to 1000 partitions

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, Apache, Nginx, p11-kit
- Microsoft CNG/KSP
- REST (TSB module)

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 (GUI, Console)
- Remote administration (Decanus Terminal)
- Local and remote firmware update
- Network attached storage data transfer (WebDAV)
- Secure log and audit
- Enhanced diagnostic functions

Technical Data

Performance (transactions per second)

Model	RSA 4096	RSA 3072	RSA 2048	ECC256
X2P RSA	2’000	5’000	12’000	15’000
	ECC521	ECC384	ECC256	
X2P EC	10’000	15’000	30’000	

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)
- 2 Console ports (RJ45, front/rear)
- 2 USB-A management ports (front/rear)
- 1 USB-C management port (rear)
- 3 Smart card slots

Controls

- 3 slots for Securosys security smart cards
- 4 LEDs for system and interface status (multicolor)
- Touch screen for configuration
- 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

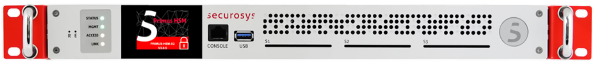
- FIPS140-3 Level 3 (in progress)
- CC EN 419221-5 eIDAS protection profile (in progress)
- CE, FCC, UL

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

HEADQUARTER
Securosys SA
Max-Högger-Strasse 2
8048 Zürich
SCHWEIZ
+41 44 552 31 00
info@securosys.com
www.securosys.com

GERMANY & EU
Securosys
Deutschland GmbH
Darrestrasse 9
87600 Kaufbeuren
DEUTSCHLAND
+49 8341 438620
info@securosys.de
www.securosys.de

APAC
Securosys
Hong Kong Ltd.
Unit 704B Sunbeam Centre
27 Shing Yip Street
Kwun Tong
Hong Kong
+852 8193 1646
info-apac@securosys.com
www.securosys.com



Front

Rear