securosys

Factsheet

Primus HSM X Cyber Vault

The Hardware Security Module that combines performance and cyber security innovation

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 into existing systems is as effortless as the initial commissioning and setup.

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-volume transactions.

Market-Leading Encryption

The Primus X Cyber Vault sets itself apart as one of the fastest HSM on the market, handling over 50,000 concurrent transactions per second (TPS). It can be scaled to over 1,000,000 concurrent transactions per second in clustered environments, impressively demonstrating its undisputed pioneering role.

Adaptability

The versatility of the Primus X Cyber Vault makes it the top choice for securing high-volume financial transactions, blockchain systems, crypto asset management, and more.

Tamper and Transport Protection

Ensure the integrity of your data during transport, storage, and operation, providing a secure foundation for critical infrastructure.

Optical Interface for Seamless Integration

Easily integrate into any network environment with support for copper and optical interfaces up to 10 Gbps.

Hybrid Operations

Our approach to a save transition to PQC stands out by incorporating hybrid signatures that utilize both classical and PQC algorithms while maintaining consistent throughput. This comprehensive approach supports the integration of RSA or ECC/ED with PQC signatures like ML-DSA, SLH-DSA, AES encryption/decryption, and key exchange protocols ML-KEM.

Remote Management

Decanus enables seamless, highly secure, and efficient remote management of your HSM and partitions.

High-Availability Clustering

Group multiple Primus HSMs together to support redundancy and load balancing, ensuring continuous operation in mission-critical environments.

Designed, developed, and manufactured in Switzerland.

securosys

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
ML-DSA, SLH-DSA, ML-KEM, HSS-LMS, XMSS

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
/ 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)
/ CC EN 419241-2 Sole Control (SAM)
/ CE, FCC, UL

Front

Rear

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

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

EUROPA
Securosys
Deutschland GmbH
Darrestrasse 9
87600 Kaufbeuren
Germany

+49 8341 438620
info@securosys.de
www.securosys.de

APAC
Securosys
Hong Kong Ltd.
11/F - 12/F & Roof Floor,
133 Wai Yip Street,
Kwun Tong,
Hong Kong

+852 8193 1646
info-apac@securosys.com
www.securosys.com

Visit our website

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