



## Primus HSM CyberVault (X2 models)

### The Hardware Security Modules that combine performance and cyber security innovation

The Securosys Primus CyberVault X2 models deliver market-leading performance while meeting the highest requirements of security, availability, flexibility, and tamper protection. Integrating into existing systems is seamless, ensuring effortless commissioning and setup.

Our approach to a secure post-quantum cryptography (PQC) transition stands through the use of hybrid signatures, combining classical cryptographic and PQC algorithms while maintaining consistent throughput. This ensures a smooth and future-proof migration. The Primus CyberVault series natively supports all NIST-selected post-quantum cryptographic algorithms, including ML-DSA, SLH-DSA, and ML-KEM as well as other PQC standards like HSS-LMS or XMSS. This is offered alongside the classical cryptographic algorithms RSA or ECC/ED.

The Primus CyberVault HSM series is designed for businesses of all sizes, offering scalability, high availability, and redundancy. The devices support clustering, load balancing, and failover mechanism,

#### Key Benefits and Model Differentiators\*

##### ★ CyberVault Pro

The **Pro** edition – like all models from the series – is equipped with a **2FA authentication mechanism and a user interface** for intuitive management. Performance and storage are fixed, making it a cost-efficient and reliable solution for **small to mid-sized businesses** that require **secure key management and encryption** without the need for extensive scalability.

##### ★ CyberVault Enterprise

The **Enterprise** edition provides the **highest flexibility** in the CyberVault series to best fit a company's need. It offers **upgrade options** for **enhanced performance, additional storage, or increased number of partitions**, allowing businesses to scale as their security infrastructure evolves. Designed for blockchain infrastructures or organizations requiring adaptability, the Enterprise model ensures long-term investment protection.

##### ★ CyberVault Max

The **Max** edition stands out as one of the **fastest HSMs on the market**, handling over **50'000 transactions per second (TPS)**. Designed for **high-performance environments**, it can scale up to **1'000 partitions and over 1'000'000 TPS** in clustered setups, delivering unmatched **speed, security, and reliability**. This makes it the ideal choice for **financial institutions or for anyone requiring demanding cryptographic workloads**.

##### ★ CyberVault Max Plus

The **Max Plus** edition pushes the limits of **hybrid performance** for PQC and classical algorithms combined, and an **impressive 30GB off-the-shelf storage**. This model is tailored for **organizations requiring high-speed cryptographic processing, and large-scale key storage**. It is the ultimate solution for businesses operating in highly regulated industries, large-scale cloud environments, or national security applications.

**+** Designed, developed, and manufactured in Switzerland.

\* For each model there are several additional features available. Please contact our sales team to learn more.

## Security Features

### Security Architecture

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

### Encryption/Authentication (extract)

- / Post-Quantum Cryptographic (PQC) algorithms  
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

Model	Partitions	Total Storage	Upgradeable to	
			Partitions	Total Storage
Pro	5	600MB	fixed	
Enterprise	10	2.4GB	250	30GB
Max	20	4.8GB	1000	30GB
Max Plus	100	30GB	1000	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 (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)

Signing	Pro	Enterprise	Max	Max Plus	
RSA 4096	400	500	1000	2'000	5'000
EC 256*	5'000	5'000	10'000	30'000	45'000
ED 25519	7'500	7'500	15'000	30'000	45'000
AES	7'500	7'500	15'000	30'000	45'000
ML-DSA-44	2'500	2'500	5'000	10'000	20'000

### Key creation

RSA 2048	20	40	60	80	80
----------	----	----	----	----	----

\*With maximum performance license.

### 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 with 1 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 certification)
- / Common Criteria EAL4+ (in certification)
  - CC EN 419221-5 eIDAS protection profile
  - CC EN 419241-2 Sole Control (SAM)
- / CE, FCC, UL

Visit our website



#### HEADQUARTER

Securosys SA  
Max-Högger-Strasse 2  
8048 Zürich  
Switzerland

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



Front



Rear

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

Copyright ©2025 Securosys SA. All rights reserved. Ev1.0