



## Primus HSM X-Series

### Secure, Reliable, and Scalable Hardware Security Modules

The Securosys Primus HSM X-Series redefines standards for security, performance, and versatility in hardware security modules (HSM). Designed, developed, and manufactured in Switzerland, it combines tamper protection, highest availability, and integrated two-factor authentication with scalable, partitionable architecture to meet diverse security needs.

Offering exceptional encryption and authentication capabilities, the X-Series is available in various performance classes, including the high-speed Primus X1000, capable of executing 1000 RSA-4096 operations per second. Whether securing financial transactions, managing cryptographic keys, or enabling blockchain applications, the Primus X-Series delivers unmatched flexibility and seamless integration across any network environment.

#### High Performance Storage and Multi-Tenancy

With up to 120 partitions and 30GB storage space, the Primus X-Series HSM can securely store hundreds of thousands key objects, enabling efficient data management with key protection inside the HSM itself.

#### True Random Numbers Generation (TRNG)

High-entropy encryption keys are paramount to provide the highest security. Primus X HSM has multiple TRNG modules, built up with separate hardware components and get their randomness from different physical noise mechanisms.

#### Robust Tamper Protection

Ensure data integrity during transport, storage, and operation with advanced tamper protection that exceeds FIPS and Common Criteria standards. Active tamper sensors protect even when the HSM is unpowered, triggering alerts on any manipulation attempt.

#### Designed, developed, and manufactured in Switzerland.

#### API Integration and Built-in Security

Primus HSM provides a variety of APIs for secure integration and communication, supporting automatic failover, load balancing, and prioritization. High availability and clustering are built-in features, requiring no extra software or cost.

#### Remote Management

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

#### Crypto-Agile Architecture

Primus HSMs support a wide range of cryptographic algorithms, and is upgradeable to post quantum computer-resistant algorithms, ensuring robust security for diverse encryption needs.

#### Scalable Access

There is no limit to the number of users and clients that can securely access the Primus X-Series HSM, ensuring effortless expansion for your organization.

## 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, 3DES (legacy), 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
- / Upgradable to quantum computer-resistant (PQC) algorithms

### 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 120 partitions @ 240 MB secure storage

### 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 option)
- / Secure log and audit
- / Enhanced diagnostic functions

## Technical Data

### Performance (transactions per second)

Model	RSA 4096	ECC 256	ECC 521	AES 256
X1000	1'000	3'000	550	5'000
X400	400	3'000	550	2'000

### Power

- / Two redundant power supplies, hot pluggable, choice:
  - 100 ... 240 V AC, 50 ... 60 Hz
  - 36 ... 75 V DC
- / Power dissipation: 60 W (typ.), 80 W (max.)
- / Ultra capacitors for data retention
- / Backup lithium battery: Lithium Thionyl Chloride 0.65g Li, IEC 60086-4, UL 1642, 3.6V

### Interfaces

- / 4 Ethernet RJ-45 ports with 1 Gbit/s (rear)
- / 1 RS-232 management port (front)
- / 1 USB management port (front)
- / 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 -25 ... +70 °C;
  - operation 0 ... +40 °C, recommended 1 ... +30 °C
- / Humidity (IEC 60068-2-78 Cab): 40 °C, 93% RH non-condensing
- / MTBF (RIAC-HDBU-217Plus) at  $t_{amb}=25\text{ °C}$ : 100 000 h
- / Dimensions (w×h×d) 440 x 88 x 441 mm (2U 19" EIA standard rack)
- / Weight 13.5 kg

### Certifications

- / FIPS140-2 Level 3
- / CC EN 419221-5 eIDAS protection profile
- / CE, FCC, UL

#### 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



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. EV3.0