securosys

The hardware security module for highest requirements

Primus HSM X-Series

- Designed, developed, and manufactured in Switzerland
- Market-leading encryption and authentication performance
- Tamper protection during transport, storage, and operation
- Highest availability
- Integrated two-factor authentication
- Simple setup, easy commissioning, configuration, and maintenance
- Scalable and flexible partitionable to your needs

The X-Series of our Primus HSM delivers market-leading performance for the highest requirements in safety, availability, flexibility and tamper protection.

Different performance classes

The X-Series is available in different performance classes: X400, X1000. In its highest performance version, the Primus X1000, the devices are capable to perform 1000 RSA-4096 operations per second.

Applications

The devices of the X-Series are very versatile. They are ideally suited to secure financial transactions such as EBICS and PCI, key management in the PKI environment, blockchain systems, crypto assets management, database encryption (TDE), code and document signing to ensure compliance, or access to the cloud (CASB). Any application can connect via API provider JCE/JCA, CNG (MS), PKCS#11 (OpenSSL, Apache, Nginx), or REST.

Functions

The devices generate keys, store them and manage their distribution. Besides key management, they perform authentication and encryption tasks. Primus HSMs support symmetric (AES, Camellia), asymmetric (RSA, ECC, Diffie-Hellman), as well as hash (SHA-2, SHA-3) algorithms among others. Each Primus HSM can also be partitioned for multiple users (multi-tenancy). 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. The Primus X-Series HSM can be remotely administrated with our Decanus Control Terminal.

securosys

Security Features

Security Architecture
- Multi-barrier software and hardware architecture with supervision mechanisms

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
- Post-Quantum Cryptographic (PQC) algorithms option CRYSTALS-Dilithium, CRYSTALS-Kyber, SPINCS+

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 and OpenSSLv3 provider
- 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	1000	3000	550	5000
X400	400	3000	550	2000

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)
- 1 liquid crystal display for management information
- 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 °C: 100 000 h
- Dimensions (w×h×d) 440 x 88 x 441 mm (2U 19" EIA standard rack)
- Weight 13.5 kg

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

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

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