securosys

The hardware security module for highest requirements

Primus HSM X-Series

- Designed, developed, and manufactured in Switzerland
- Market-leading encryption performance
- Highest availability
- Tamper protection during transport, storage, and operation
- Simple setup, configuration, and maintenance
- Integrated two-factor authentication
- 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: X200, X400, X700, X1000 and X2000. In its highest performance version, the Primus X2000, the devices are capable to perform 2000 RSA-4096 operations per second. Multiple Primus HSM can be grouped together to support redundancy and load balancing.

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 (AD CS), 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, p11-kit, OpenSSL, Apache, Nginx.

Functions

The devices generate keys, store and manage the distribution of these keys. Besides key management, they also perform authentication and encryption operations. Each Primus HSM can also be partitioned for multiple users (multi-tenancy). Primus HSM support symmetric (AES, Camellia), asymmetric (RSA, ECC, Diffie-Hellman), and hashing (SHA-2, SHA-3) cryptographic algorithms. They can be integrated seamlessly and easily into any network environment. The Primus X-Series HSM can be remote controlled with our Decanus Remote Control Terminal.

securosys

Security Features

Security architecture
- Multilevel military grade security architecture
- Multi-barrier software and hardware architecture with supervision mechanisms

Encryption/Authentication
- 128/192/256-Bit AES with GCM-, CTR-, ECB-, CBC-, MAC Mode
- Camellia, 3DES (legacy), ChaCha20-Poly1305
- 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
- Upgradeable to quantum computer-resistant 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
- Ultra-secure vault for long term keys and certificates
- 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

Firmware
- Local firmware update on device or optionally on Decanus Remote Control Terminal

Identity-based authentication
- Multiple security officers (2 out of m)
- Identification based on Smartcard and PIN

Networking Features

Software integration
- JCE/JCA Provider
- PKCS#11, P11-Kit, OpenSSL, Apache, Nginx
- Microsoft CNG

Network Management
- IPv4/IPv6
- Monitoring and logging (SNMPv2, syslog)

Device Management
- Local configuration, remote configuration (Decanus)
- Integrated logging
- Firmware update
- Enhanced diagnostic functions

Technical Data

Performance (per second, concurrent)

	RSA 4096	ECC 256	ECC 521
X2000	2000	8000	3000
X1000	1000	3000	550
X700	700	3000	550
X400	400	3000	550
X200	200	2000	350

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 Chlorid 0.65g Li, IEC 60086-4, UL 1642, 3.6V

Interfaces
- 4 Ethernet RJ-45 ports with1 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 (multicolored)
- 1 liquid crystal display for management information
- Console interface
- Optional Decanus Remote Control Terminal

Environmental Test Specifications (target)
- EMV/EMC: EN 55022, EN 55024, FCC Part 15 Class B
- Safety: IEC 60950

Specifications
- Temperature ranges (IEC 60068-2-1 Ad, IEC 60068-2-2 Bd): storage -25...+70 °C; operation 0...+40 °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 EAL 4+ certified root key storage
- CC EN 419221-5 eIDAS protection profile (in progress)
- CE, FCC, UL

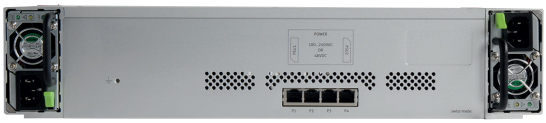
We strive to continuously improve our offerings and therefore reserve the right to change specifications without notice. Designed and manufactured in Switzerland

HEADQUARTER
Securosys SA
Förrlibuckstrasse 70
8005 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