securosys

Compare and decide:
Primus HSM X- or E-Series?

Securosys Primus HSM of X- and E-Series look different, but have many features in common:

- Simple setup, configuration and maintenance
- Tamper protection during transport, storage, and operation
- Scalable and flexible partitionable to your needs
- Designed, developed, and manufactured in Switzerland
- Various performance classes

Both device types are very versatile and provide the same firmware and connectivity. They are ideally suited to secure financial transactions as EBICS and PCI, access to the cloud (CASB) or key management in PKI environments.

The devices generate store and manage the distribution of encryption keys. Besides key management they also perform authentication and encryption tasks. They can be seamlessly and easily integrated into any network environment. Each Primus HSM can also be partitioned for multiple users (multi-tenancy).

This synopsis aims to show the differences and to help you for your decision for a device type. Below the most important criteria:

You need...	...then the device to suit you is ...
▪ imperatively two power supplies, hot pluggable for redundancy respectively hot pluggability	⇨ Primus X-Series
▪ highest availability	⇨ Primus X-Series
▪ highest encryption performance	⇨ Primus X-Series
▪ not imperatively highest performance	⇨ Primus E-Series

Front

X-Series

E-Series

Rear

X-Series

E-Series

On the backside of this factsheet you find specifications with the differences between the two series highlighted. Please also note the separate factsheets for the X- and the E-Series.

securosys

Security Features

Security architecture
- Multilevel 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 (TNRG)
- SP800-90 compatible random number generator

Key Management
- Ultra-secure vault for long term keys and certificates

	X-Series	E-Series
Key capacity	30 GB	6 GB
Partitions/capacity	up to 120 each 240 MB	up to 50 each 120 MB

Operation
- Unlimited number of users and backups
- Number of client connections not restricted

Anti Tampering 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

Networking Features

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

Network Management
- IPv4/IPv6
- Monitoring und Logging (SNMPv2, syslog)
- Enhanced test functions
- Event agent

Device Management
- Local configuration (Console)
- Remote configuration (Decanus)
- Integrated logging
- Firmware update
- Extensive diagnostics capabilities

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
E150	150	1100	180
E60	60	700	120
E20	20	350	60

Power
- Backup lithium battery
- Power supply:
  - **X-Series:** Two redundant power supplies, hot pluggable, choice: 100 ... 240 V AC, 50 ... 60 Hz, 36 ... 75 V DC
  - **E-Series:** 100 bis 240 V AC, 50 ... 60 Hz
- Power dissipation:
  - **X-Series:** 60 W (typ.), 80 W (max.)
  - **E-Series:** 35 W (typ.), 50 W (max.)
- Speciality
  - **X-Series:** Supercap for data retention

Controls
- Console interface
- **X-Series:** control unit with display
- Optional with terminal Decanus for remote control

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:
  - **X-Series:** 100 000h
  - **E-Series:** 80 000h
- Dimensions (w×h×l)
  - **X-Series:** 440 x 88 x 441 mm; fits in a 2HE 19" EIA standard rack
  - **E-Series:** 417 x 44 x 365 mm; fits in a 1 HE 19" EIA standard rack
- Weight: **X-Series** 13,5 kg, **E-Series** 5,8 kg

Certification
- FIPS140-2 Level 3 mode
- CC EAL 4+ certified root key storage
- CC EN 419221-5 eIDAS protection profile (in progress)
- CE, FCC, UL

Interfaces
- 4 Ethernet RJ-45 ports with 1 Gbit/s (rear)
- 1 RS-232 management port
- 1 USB management port
- **X-Series:** 3 smartcard slots

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