securosys

The affordable hardware security module

Primus HSM E-Series

- Market-leading price-performance ratio
- HSM Network Appliance as a replacement for PCIe cards
- 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

The E-Series of our Primus HSM offers high performance at an outstanding price. Connecting the devices to existing systems is just as easy as commissioning.

Different performance classes

The E-Series is available in various performance classes: E20, E60 and E150. It can be configured via the serial port or over the network with our Decanus remote terminal.

Applications

The devices of the E-Series are very versatile. Built as network appliances, they lack the disadvantages of PCIe-based solutions like software dependance of PCIe host systems and the host system itself. The E-Series is ideally suited to secure financial transactions such as EBICS and PCI, access to the cloud (CASB), key management in the PKI environment, and to protect blockchain systems and safeguard crypto asset management.

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 E-Series HSM can be remotely administrated with our Decanus Terminal.

securosys

Security Features

Security Architecture

- Multilevel security architecture
- Internal hardware supervision for error-free operations

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 1024-4096, ECDH
- SHA-2/SHA-3 (224-512), SHA-1, RIPEMD-160, Keccak
- HMAC, CMAC, GMAC, Poly1305
- Post-Quantum Cryptographic (PQC) algorithms option
  CRYSTALS-Dilithium, CRYSTALS-Kyber, SPINCS+

Key Generation

- Two hardware true random number generators (TNRG)
- NIST SP800-90 compatible random number generator

Key Management

- Key capacity: up to 6 GB
- E150 up to 50 partitions @ 120 MB capacity
- E60/E20 up to 10 partitions @ 120 MB capacity

Operation

- Number of client connections not restricted
- Unlimited number of backups

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

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
  using Decanus Terminal, or through virtual smart card

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)
- Monitoring and log streaming (SNMPv2, syslog/TLS)
- Active clustering of multiple units for load-balancing and fail-over

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
E150	200	1500	300	600
E60	60	700	120	600
E20	20	350	60	200

Power

- Power supply: 100 ... 240 V AC, 50 ... 60 Hz
  E150 with two redundant hot pluggable power supplies
- Power dissipation: 30 W (typ), 50 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 Gbit/s (rear)
- 1 RS-232 management port (rear)
- 1 USB management port (rear)

Controls

- Console interface
- 4 LEDs for system and interface status (multicolor)
- Optional Decanus Terminal for remote administration

Environmental Test Specifications

- EMV/EMC: EN 55022, EN 55024, FCC Part 15 Class B
- Safety: IEC 62386-1

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: 80 000 h
- Dimensions (w×h×d) 417 x 44 x 365 mm (1U 19" EIA standard rack)
- Weight 5,8 kg

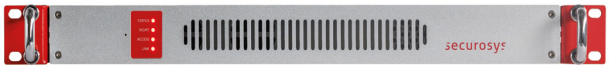
Certification

- 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 (E20, E60)

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