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 (number corresponds to RSA-4096 signatures per second). 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, or to protect blockchain systems, crypto assets management.

Functions

The devices generate encryption keys, store and manage the distribution of these keys. Besides key management, they also perform authentication and encryption tasks. Multiple Primus HSM can be grouped together to support redundancy and load balancing. Each Primus HSM can also be partitioned for multiple users (multi-tenancy). Primus supports symmetric (AES, Camellia), asymmetric (RSA, ECC, Diffie-Hellman), and hashing (SHA-2, SHA-3) cryptographic algorithms. They can be seamlessly and easily integrated into any network environment.

securosys

Security Features

Security architecture
- Multilevel security architecture
- Intern hardware supervision for error-free operations

Encryption/Authentication
- 128/192/256-Bit AES with GCM-, CTR-, ECB-, CBC-, MAC-mode
- Camellia, 3DES (legacy)
- RSA 1024-8192, DSA 512-8192
- ECDSA 224-521, GF(P) arbitrary curves, ED 25519
- DSA 2048-8192
- Diffie-Hellman 1024-4096, ECDH
- SHA-2/SHA-3 (224-512), SHA-1, RIPEMD-160, Keccak, HMAC, CMAC, GMAC
- Upgradeable to quantum computer-resistant algorithms

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

Key Management
- Key capacity: up to 6 GB
- Ultra-secure vault for long term keys and certificates
- Up to 50 partitions @ 120 MB capacity

Operation
- Unlimited number of 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

Identity based authentication
- Multiple security officers (2 out of *n*)
- Identification based on Smartcard and PIN using Decanus remote, or through virtual Smartcard

Networking Features

Software integration
- JCE/JCA Provider
- PKCS#11, OpenSSL
- Microsoft CNG

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

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

Technical Data

Performance (per second, concurrent)

	RSA 4096	ECC 256	ECC 521	AES (Mbit)
E150	150	840	300	>180
E60	60	560	200	>180
E20	20	280	100	> 60

Power
- Power supply:
  - 100 ... 240 V AC, 50 ... 60 Hz
- Power dissipation: 30 W (typ) ... 50 W (max)
- 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 (rear)
- 1 USB management port (rear)

Controls
- Console interface
- 4 LEDs for system and interface status (multicolored)
- Optional remote control Decanus

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

Certification
- FIPS140-2 Level 3 mode
- CC EAL 4+ certified root key storage
- CE, FCC, UL

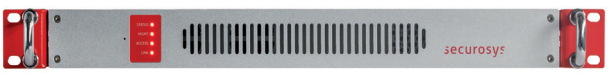
We strive to continuously improve our offerings and therefore reserve the right to change specifications without notice.
Designed and manufactured in Switzerland

HEADQUARTERS
Securosys SA
Förrlibuckstrasse 70
8005 Zürich
SWITZERLAND
+41 44 552 31 00

info@securosys.ch
www.securosys.ch

GERMANY & EU
Securosys
Deutschland GmbH
Darrestrasse 9
87600 Kaufbeuren
GERMANY
+49 8341 438620

info@securosys.de
www.securosys.de



Front


Rear