securosys

The Hardware Security Modules exclusively for the Swiss Banking System

Primus HSM Models S4 / S6 / S6P

- Designed, developed, and manufactured in Switzerland
- Exclusively tailored for the Swiss banking system SIC
- Market-leading encryption and authentication performance
- Post-Quantum Cryptographic algorithms
- Remote administration with Decanus Terminal
- Flexible partitioning for application-specific key segregation
- Integrated two-factor authentication
- Tamper protection during transport, storage, and operation
- Simple setup, easy commissioning, configuration, and maintenance

The Securosys Primus HSM S-Series is exclusively tailored for SIX, the organization that operates the Swiss Interbank Clearing System. The Primus HSM S-Series secures the Swiss interbank clearing and settlement, as well as SECOM, the Swiss stock exchange. It delivers market-leading performance for highest requirements in safety, availability, flexibility, and tamper protection. Integrating the devices into existing systems is as effortless as the initial commissioning and setup.

Different performance classes and options

The Primus HSM models S4, S6 and S6P differ in performance and the maximum number of partitions (logical HSMs for multi-tenancy). All devices can be remotely administrated with the Decanus Terminal.

Applications

The Primus HSM S-Series performs a focused range of operations. Due to their industry-leading signature performance, they are ideally suited to secure financial transactions. The S-Series is mandated for access to SIC and eSIC transactions using the SASS application; it can also be used to secure SECOM transactions.

Functions

The Primus HSM S-Series generates keys, and stores and manages their distribution. Besides key management, they perform authentication and encryption tasks. Primus supports symmetric (AES) and asymmetric encryption (RSA, Diffie-Hellman, ECDSA), as well as hash (SHA-2, SHA-3) algorithms among others. Multiple Primus HSMs can be grouped together to support redundancy and load balancing (high availability clustering). They can be integrated seamlessly and easily into any network environment, having both copper and optical interfaces.

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, 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 CRYSTALS-Dilithium, CRYSTALS-Kyber, SPHINCS+

Key Generation

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

Key Management

- Key capacity: up to 12 GB
- 1 partition @ 240 MB secure storage upgradeable to max. partitions:

S6P	50
S6	10
S4	1

Operation

- Number of client connections not restricted

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

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
- Secure log and audit
- Enhanced diagnostic functions

Technical Data

Performance (transactions per second, concurrent)

Model	RSA 4096	RSA 3072	ECC521	ECC384
S6P	1000	2000	800	2000
S6	500	1000	400	1000
S4	25	50	25	50

Power

- Two redundant power supplies, hot pluggable 100 ... 240 V AC, 50 ... 60 Hz
- Power dissipation: 65 W (typ.), 100 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 Gbps (rear)
- 2 SFP+ slots for optical 10Gbps Ethernet modules (rear)
- 2 Console ports (RJ45, front/rear)
- 2 USB-A management ports (front/rear)
- 1 USB-C management port (rear)
- 3 Smart card slots

Controls

- 3 slots for Securosys security smart cards
- 4 LEDs for system and interface status (multicolor)
- Touch screen for configuration
- Console interface
- 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 -20...+60 °C; operation 0...+35 °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) 417×44×365 mm (1U 19" EIA standard rack)
- Weight 7.5kg

Certifications

- 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
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