

# securosys



## The Hardware Security Module exclusively for the Swiss Banking System Primus HSM S500

- Designed, developed, and manufactured in Switzerland
- Exclusively tailored for the Swiss banking system SIC<sup>4</sup>
- In cooperation with Swiss authorities
- Market-leading encryption and authentication performance
- Highest availability
- Tamper protection during transport, storage, and operation
- Simple setup, easy commissioning, configuration, and maintenance
- Integrated two-factor authentication
- Restricted feature set for the Swiss Interbank Clearing SIC<sup>4</sup>

This is our flagship Primus HSM. It was exclusively tailored for SIX, the organisation that operates the Swiss Interbank Clearing System. S500 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. Connecting the devices to existing systems is just as easy as their commissioning and setup.

### Applications

The Primus HSM S500 perform a focused range of operations. Due to their industry-leading signature performance they are ideally suited to secure financial transactions. The S500 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 S500 generate encryption keys and store and manage their distribution. Besides key management, they also perform other authentication and encryption tasks. Multiple Primus HSM can be grouped together to support redundancy and load balancing. Primus supports symmetric (AES, Camellia), asymmetric encryption (RSA, Diffie-Hellman), and hash (SHA-2, SHA-3) algorithms. They can be seamlessly and easily integrated into any network environment.

## Security Features

### Security architecture

- Military grade security architecture
- Multi-barrier software and hardware architecture with supervision mechanisms

### Encryption/Authentication (extract)

- 128- and 256-bit AES with GCM-, CTR-, GCTR-, ECB-, CBC-, MAC-modes
- Camellia
- RSA 1024, 2048, 3072, 4096, 8192
- DSA 256-8192
- Diffie-Hellman 1024, 2048, 4096
- SHA-2 (256 - 512), SHA-3

### Key Generation

- Two hardware true random number generators (TNRG)

### Key Management

- Key capacity: up to 30 GB

### Operation

- 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

### Identity based authentication

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

## Networking Features

### Software integration

- JCE/JCA Provider

### Network Management

- IPv4/IPv6
- Enhanced test functions
- Event agent

### Device Management

- Configuration, monitoring and logging (syslog, SNMP V2)
- Integrated logging
- Firmware update

### Load balancing / Fail Over

- Multiple units may be connected to provide load balancing by application software

## Technical Data

### Performance (per second, concurrent)

RSA 4096	RSA 3072
200	400

### Power

- Two redundant power supplies, hot pluggable  
100 ... 240 V AC, 50 ... 60 Hz
- Power dissipation: 60 W (typ.), 80 (max.)
- Ultra capacitors for data retention
- Backup lithium battery

### Interfaces

- 4 Ethernet RJ-45-ports with 1 Gbit/s (rear)
- 1 RS-232 management port (front)
- 1 USB management port (front)
- 3 smart card slots
- Physical key to open case

### Controls

- 3 slots for Securosys Security smart cards
- 4 LEDs for system and interface status (multicolored)
- 1 liquid crystal display for management information
- Panel for menu navigation and to trigger built in test equipment and emergency erasure

### Environmental Test Specifications

- 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, recommended 1...30 °C
- Humidity (IEC 60068-2-78 Cab): 40 °C, 93% RH, non-condensing
- MTBF (RIAC-HDBU-217Plus) at  $t_{amb}=25\text{ °C}$ : 100 000 h
- Dimensions (w×h×d) 440 x 88 x 441 mm (fits 2U 19" EIA standard rack - see photo below)
- Weight 13.5 kg

### Certification

- Reviewed by DDPS (Federal Department of Defence, Civil Protection and Sport)
- 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

Copyright ©2022 Securosys SA. All rights reserved.  
EV2.1



Front



Rear