HSM950

Secure Transaction Server

Description

The HSM950 (Hardware Security Module) is a scalable security module server capable of performing secure and encrypted online transactions, such as reloads and card validation. It uses a high-speed Security Access Module (SAM) carrier to distribute client requests across the network, ensuring client parallelism. It supports multiple parallel sessions, with at least 10 simultaneous connections, ensuring high concurrency.

HSM950 can support up to 4 carriers of 28 SAMs each, totaling 112 SAMs. The carriers are accessible from the front panel and can be easily replaced using a dedicated tool. SAMs can be logically divided into sub-carriers, allowing multiple applications to operate simultaneously in different configurations. This function enables adjusting sub-carrier sizes for better load balancing.

In addition to supporting sub-carriers, the integrated software balances network requests across security modules and sub-carriers, making client applications smoother, simpler, and more efficient. The internal SAM management software is written in C, which translates into high performance and stability in a 100 Mbps network, with minimal impact on APDU response time.

Application development is compatible with a binary API and source code libraries for C and Node.js.

The HSM950 can be rack-mounted in 19-inch racks using HRS100 brackets or placed on desks with rubber feet.

With all these features, the HSM950 is a powerful tool for implementing secure transaction systems with a high level of robustness and excellent support for cryptographic transaction processing (TPS) per module, depending on configuration and operating mode. It is designed to ensure high levels of security, availability, and operational control.

Applications

- Online authentication
- Online credit and debit transactions
- Remote reload
- System optimization allowing the elimination of local SAM in favor of a shared network

Technical Specifications

- **Power Supply:**
  - 90 V to 264 V – 50~60 Hz
- **Redundant power system**
- **Dimensions:**
  - 430 x 200 x 44 mm
- **Interfaces:**
  - Ethernet 10/100*
  - Ethernet 10/100/1000**
- **Protocols:**
  - APDU - Planeta Informática
- **Other Features:**
  - Easy expandability
  - Supports up to 112 SAMs
  - Can be rack-mounted or desktop installed
  - Easy tray replacement with a dedicated tool

    - Web interface for system management and operational monitoring

The Ethernet 10/100 interface corresponds to the standard version of the equipment.

** The 10/100/1000 (Gigabit Ethernet) interface is available in a specific product version.

Additional Specifications

The HSM950 consists internally of two hardware types: the main CPU and the SAM carriers. The multimodule SAM architecture provides high cryptographic performance, with a capacity of 2000 cryptographic transactions per second (TPS) with 4 modules depending on configuration and operating type.

Main CPU (Embedded Processing Unit)

- Quad-core ARM Cortex A53 1.5 GHz
- 2 GB RAM
- 16 GB internal storage
- 10/100 Mbps Ethernet port
- Runs an optimized Linux operating system
- Accessible via TCP/IP through the network interface
- Written in C
- Minimal impact on APDU response time on a 100 Mbps network
- Provides a web interface for system management and supervision, allowing monitoring of HSM operational indicators, such as:
    - Average transaction response time
    - Average number of commands processed per session
    - Verification of operational status and system uptime
    - Access to event history and system failure logs

SAM Carrier – MSH100

- Each carrier contains 7 ARM CPUs for 28 SAMs
- Each CPU is Cortex M4 32-bit running at 180MHz and controls 4 SAMs
- Supports Class A and B SAMs
- Automatic and on-demand PPS support
- TA1 speeds from 11h to 18h and from 91h to 97h
- Supports clock stop while SAM remains active
- Configurable speeds from 4 to 24 MHz, including 4, 4.8, 6, 8, 9.6, 12, 16, and 24MHz
- Supports T=0 and T=1
- Multi-CPU and multi-SAM architecture allows parallel processing on multiple cryptographic channels, increasing

Physical Security

The system can be integrated with tamper detection mechanisms, aligned with best security practices for cryptographic modules.

CC EAL5+ Certification

When using VSAMs, the HSM operates with a secure hardware-based core certified under Common Criteria EAL5+, ensuring a high level of cryptographic security and protection against advanced threats.

Package Contents

- HSM950
- Power cable

Accesories

- SAM Carrier – MSH100 (SAM carrier)
- HRS010 (I0209) (Rack mounting support)

Partnumber

- HSM950 (I0317)*
- HSM950-plus (I0344)**

Warranty

12 months