

HSM SP

Network-Attached Hardware Security Module

HSM SP (formerly named Luna SP) allows developers to securely deploy web applications, web services, and other Java applications in a protected hardened security appliance.

Deploy Secure Applications Anywhere with Ease

HSM SP is designed for reliable deployment of security applications anywhere on your network. HSM SP leverages standard Java development tools to simplify development of custom applications and reduce integration and testing cycles. Its programmability and security make it easy to develop custom applications, integrate them into an appliance, and deploy them securely in a very short time. Enterprises deploying security applications can streamline development processes, eliminate hardware duplication, and reduce ongoing operational costs with HSM SP.

The Programmability of an Application Server with the security of an HSM

HSM SP provides a secure platform for the deployment of web applications, web services, and Java applications that require the highest levels of trust by combining a standard application server platform and a dedicated Hardware Security Module (HSM) within a single security appliance. The HSM SP's application server is security hardened and optimized to take advantage of the integrated HSM and its specialized hardware features.

Standard Tools for Rapid Development

HSM SP supports the J2S development environment and is pre-populated with standard tools to simplify application development. A Web server, SOA P stack, and J2SE compliant XML Web service container are preinstalled and optimized to support XML and Web Services applications running on HSM SP. Custom applications can be developed quickly and easily, simplifying design and testing, shortening development cycles, and eliminating the need for propriety development funds.

Protected Application Environment

Applications installed on HSM SP execute within a protected application container to ensure that application code and system code are isolated.



Applications executing within this trusted environment have exclusive access to the HSM SP integrated HSM through a policy layer separating the application from the HSM.

Secures Applications and their Cryptographic keys

HSM SP increases application security by providing a trusted execution environment that protects an application's sensitive software components and cryptographic keys from physical, logical, and operational threats. Customer-provided application code is digitally signed and securely installed on the HSM SP to assure code integrity and prevent the execution of unauthorized applications.

HSM SP 2.0 features an integrated FIPS 140-2, Level 3 validated HSM that provides hardware protection for cryptographic keys and processes.

Auditability, Authentication, and Policy Control

HSM SP combines proven hardware key management with rigorous logging features to provide non-repudiable audit records of access and cryptographic key usage. Split administrative roles, including M of N multi-person authentication, and flexible security policy management, maintain tight control over sensitive administrative functions, including code loading and management of cryptographic keys.

Maximum Application and Cryptographic Performance

Applications running on HSM SP take advantage of a streamlined appliance platform with the minimal set of services. This reduces system overhead and maximizes application

Benefits

Protected Application Execution Environment

Signed Code Prevents Unauthorized Execution

Application Auto Restart

Standard Tools for Rapid Development

Reduces System Overhead

Prevents Unauthorized Execution





Technical Specifications

Java Service Environment

HSM SP includes the following tools to support custom Java services:

- Java J2SE (JVM)
- Xerces (XML parsing)
- Apache Tomcat (Application and Webserver)
- Apache Axis (SOA P)

Cryptographic APIs

- JCE/JCA

Regulatory Standards Certifications

- FIPS 140-2 Level 3 validated
- RoHS compliant
- U/L 1950 (EN60950) & CSA C22.2 compliant
- FCC Part 15 - Class B
- ISO - 9002 Certification

Cryptographic Performance

- Luna SP 1.5 – Over 1200 1024-bit RSA cryptographic operations per second
- Luna SP 2.0 – 3000 & 7000 tps
- HSM SP 2.0.3 3000 & 7000 tps

Cryptographic Algorithms

Asymmetric Key

- Diffie-Hellman (1024-4096 bit)
- RSA (512-4096 bit)

Digital Signing

- RSA (1024-4096 bit), DSA (512-1024 bit)

Symmetric Keys

- 3DES, AES, RC2, ARC4, RC5

Hash Digest

- SHA-1, SHA-2, (160, 256, 512), MD-5

Message Authentication Codes

- HMAC -MD5, HMAC -SHA-1, SSL3-MD5-MAC, SSL3-SHA-1-MAC

Physical Characteristics

Connectivity

- 2x 10/100 Ethernet, CAT5, UTP Local administration serial console port

Dimensions

- 19.0" x 20.6" x 3.45" (482.6mm x 523.2mm x 87.7mm) 35lb (15.9kg)
- 1U full-length 19" rackmount chassis (Luna SA 4.0 model) (ANSI/EIA-310-compliant)

Power Requirements

- 1.5A@120V Max

Temperature

- Operating 0°C to 40°C,
- Storage -20°C to +65°C

FIPS

RoHS

	FIPS	RoHS
IU Rackmount Chasis	✓	✓
Transactions Per Second	>1200	4000**
Cryptographic APIs	✓	
ECC	✓	✓
ECDSA	✓	✓
JRE 1.5	✓	✓
PED	✓	✓
PED II	✓	✓

** Performance 4000s/s1, 2* 1 – based on uncongested network transacted operations
2 – devices must be running version 4.0 of software or later

performance. HSM SP's integrated K5 Cryptographic Engine is capable of up to 4,000 transactions per second to eliminate cryptographic processing bottlenecks.

Tamper-Protected Hardware

Integrated physical security measures include tamper-evident seals, intrusion detection switches, and shielded connectors designed to resist physical attacks.

Simplified Administration

HSM SP features a Secure Command Line Interface to simplify remote system administration and streamline maintenance. A local console port is offered for initial configuration or direct system administration.

Two-Factor Authentication

HSM SP uses two-factor, trusted path authentication with the HSM PED (PIN Entry Device), a handheld authentication console, to control access to HSM administration functions and applications.

Ethernet-Attached for Flexibility

HSM SP connects to standard TCP/IP (Internet Protocol) networks to ensure ease of deployment into existing network infrastructure.

Two Ethernet interfaces with integrated firewalls can be used for services or administrative access.



www.safenet-inc.com

Corporate Headquarters:

4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel.: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524,
Email: info@safenet-inc.com

EMEA Headquarters:

Tel.: +44 (0) 1276 608 000, Email: info.emea@safenet-inc.com

APAC Headquarters:

Tel.: +852 3157 7111, Email: info.apac@safenet-inc.com

For all office locations and contact information, please visit
www.safenet-inc.com/company/contact.asp

©2008 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners.
PB-HSM SP-11.25.08