thalescpl.com

THALES

SafeNet-Java HSM

Hardware Security Module for Java Application Security

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

SafeNet Luna SP provides a secure platform for the deployment of web applications, web services, and Java applications that require the highest levels of trust. Luna SP combines a standard application server platform and a dedicated hardware security module (HSM) within a single appliance.

Protected Application Environment

Applications installed on Luna SP execute within a protected application container to ensure that application code and system code are isolated. Applications executing within this secure container have exclusive access to the integrated HSM.

Standard Tools for Rapid Development

Luna SP supports the J2SE development environment and is pre-populated with standard tools to simplify application development. A web server, SOAP stack, and J2SE-compliant XML web service container are preinstalled and optimized to support XML and web services applications. Custom applications can be developed quickly and easily, simplifying design and testing, shortening development cycles, and eliminating the need for proprietary development funds.

Secures Applications and their Cryptographic Keys

Luna 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. Developer-provided application code is digitally signed and securely installed on the Luna SP to assure code integrity and prevent the execution of unauthorized applications. Luna SP features an integrated FIPS 140-2 Level 3-validated HSM that provides hardware protection for cryptographic keys and processes.

Auditability, Authentication, and Policy Control

Luna 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.

Benefits

- Protected application execution environment
- Signed code prevents unauthorized execution
- Application auto restar
- Standard tools for rapid development
- Reduces system overhead
- Supports geographically dispersed administration of the Luna SP

Product Applications

HSM Server with non-Luna Clients

- Supporting higher level HSM functions (e.g., time stamping)
- Supporting on-demand clients (e.g., grid computing)
- Emulating non-Luna HSMs Trusted Intermediary
- SSL to SSL (e.g., Browser to Business Partner/System)
- Encrypted to SSL (e.g., Account Aggregation)
- SSL to Encrypted: (e.g., PIN Management)
- Encrypted to Encrypted: (e.g., PIN to magnetic stripe)

Trusted Web Service

- Secure web page (e.g., 3D Secure)
- Secure web service

Accelerated Application and Cryptographic Performance

Applications running on Luna SP take advantage of an optimized and streamlined appliance platform. This reduces system overhead and maximizes application performance. The integrated K6 cryptographic engine of Luna SP is capable of up to 7,000 RSA 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.

Flexible Backup and Disaster Recovery Options

Luna SP provides secure, auditable, and flexible options to simplify backup, duplication, and disaster recovery. Key backups can be performed locally or remotely to the Luna Backup HSM.

Two-Factor Authentication and the Remote PED

Luna SP uses two-factor, trusted path authentication with the PED (PIN Entry Device), a handheld authentication console, to control access to HSM administration functions and applications. The PED can also be used for remote management and administration. The Remote PED connects to a Windows workstation via USB, and communicates over a secure network connection to the integrated HSM inside the Luna SP. Remote management with the PED offers the security administrator the ability to remotely authenticate to any HSM role for centralized management of administrative functions.

Network Shareable for Easy Deployment

Ethernet connectivity enables flexible deployment and scalability. Built-in TCP/IP support ensures that Luna SP deploys easily into existing network infrastructures and communicates with other network devices.

Technical Specifications

Java Service Environment

Luna SP includes the following tools to support customer Java services:

- Java J2SE (JVM)
- Xerxes (XML parsing)
- Apache Tomcat (application and web server)
- Apache Axis (SOAP)

Cryptographic APIs

- JCA/JCE

Cryptography

- Full Suite B support
- Asymmetric: RSA (1024-8192), DSA (1024-3072), Diffie-Hellman, KCDSA, Elliptic Curve Cryptography (ECDSA, ECDH, ECIES) with named, userdefined, and Brainpool curves
- Symmetric: AES, RC2, RC4, RC5, CAST, DES, Triple DES, ARIA, SEED
- Hash/Message Digest/HMAC: SHA-1 SHA-2 (224-512), SSL3-MD5-MAC, SSL3-SHA-1-MAC
- Random Number Generation: FIPS 140-2-approved DRBG (SP 800-90 CTR mode)

Physical Characteristics

- Standard 1U 19" rack mount chassis
- Dimensions: 19" x 21" x 1.725" (482.6mm x 533.4mm x 43.815mm)
- Weight: 28lb (12.7kg)
- Input Voltage: 100-240V, 50-60Hz
- Power Consumption: 180W maximum, 155W typical
- Temperature: operating 0°C – 35°C, storage -20°C – 60°C
- Relative Humidity: 5% to 95% (38°C) non-condensing

Security Certifications

- FIPS 140-2 Level 3v

Safety and Environmental Compliance

- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE

Host Interface

- Dual Gigabit Ethernet ports

Reliability

- Mean Time Between Failure (MTBF) 66,561 hrs

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> thalescpl.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com