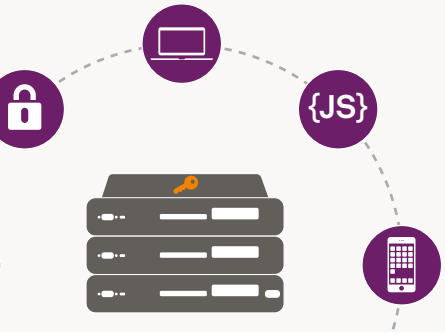

Product Brief

SafeNet Java HSM

Hardware Security Module for Java Application Security

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

Protected Application Environment

Applications installed on SafeNet Java HSM 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

SafeNet Java HSM 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

SafeNet Java HSM 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 SafeNet Java HSM to assure code integrity and prevent the execution of unauthorized applications. SafeNet Java HSM features an integrated FIPS 140-2 Level 3-validated HSM that provides hardware protection for cryptographic keys and processes.

Benefits

- Protected application execution environment
- Signed code prevents unauthorized execution
- Application auto restart
- Standard tools for rapid development
- Reduces system overhead
- Supports geographically dispersed administration of the SafeNet Java HSM

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

Auditability, Authentication, and Policy Control

SafeNet Java HSM 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.

Accelerated Application and Cryptographic Performance

Applications running on SafeNet Java HSM take advantage of an optimized and streamlined appliance platform. This reduces system overhead and maximizes application performance. The integrated K6 cryptographic engine of SafeNet Java HSM 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

SafeNet Java HSM 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

SafeNet Java HSM 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 SafeNet Java HSM. 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 SafeNet Java HSM deploys easily into existing network infrastructures and communicates with other network devices.

Technical Specifications

Java Service Environment

SafeNet Java HSM 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, user-defined, 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

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com
Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free