Luna® XML Central XML Interface Hardware Security Module (HSM)

PRODUCT BRIEF

Benefits

- Easy to deploy and integrate
- Simple programming interface
- Platform independent
- Complete network scalability
- Enables secure B2B and B2C applications
- Secure application connection authentication
- Reduced development time

Typical Applications

- Web-based B2B and B2C applications
- Web Services hosting
- Applications or transactions handling identity, value, or other proprietary information.

Examples include:

- Federated sign-on automation
- Electronic payments, clearing and transfers
- Document, media, and software security authenticity and rights management
- ISV security applications - for almost any target application - database encryption, XML firewall, archiving, etc.
- Cryptographic applications in the SOA as well as traditional (non-SOA) environments

SafeNet Luna XML revolutionizes application security with the world's easiest to integrate and deploy hardware security module. Other HSMs take months to integrate with new applications because of complex security APIs. Luna XML has a zero footprint on the host application server - providing for rapid, independent, flexible, and highly scalable deployments. Fast, Easy, Secure.

Ease of Integration

Using an intuitive user interface, Luna XML appliances can be configured and made ready to deploy in a few minutes. SafeNet Luna XML has a Web Services cryptographic interface, with XML/SOAP as the messaging interface. It is easy to use and requires no prior knowledge of existing APIs, such as PKCS#11, Java JCA/JCE, and Microsoft CryptoAPI. This reduces application integration time from months to days. With a completely platform-independent interface and no extensive client installations required, Luna XML saves time and reduces costs.

Most Secure

The FIPS 140-2 Level 3-validated SafeNet Luna XML HSM protects critical cryptographic keys and accelerates sensitive cryptographic operations across a wide range of security applications. Further, integrated physical security measures include tamper-evident seals, intrusion detection switches, and shielded connectors designed to resist physical attacks.

Multi-level access control and authentication policies to Luna XML's administrative functions provide the highest degree of protection for sensitive cryptographic keys and prevent unauthorized system configuration changes. All this while still permitting flexible remote management and monitoring. Access to sensitive HSM administration functions is controlled through the SafeNet Luna PED II (PIN Entry Device), a handheld, two-factor authentication device connected directly to Luna XML.

Increased Performance

SafeNet Luna XML performs rapid processing of cryptographic commands. The product provides symmetric and asymmetric cryptographic performance to meet a wide variety of security application processing requirements, with: 1200 1024-bit RSA signings per second on one application server and up to 2200 for multiple application servers; and 700 XML signings on 1 KByte XML documents on one application server and up to 1000 XML signings for multiple application servers.

High Availability and Scalability

SafeNet Luna XML scales as a Web Service to meet your demands as applications grow. Core configuration parameters are upgradeable via software to allow Luna XML to adapt to new technology without the need to replace hardware. In addition, high levels of scalability, reliability, redundancy, and increased throughput can be easily achieved, as there are no restrictions on the number of HSMs that can work in unison.

Technical Specifications

Client API
- XML/Web Service API (XML/SOAP, XML/RPC)

Operating System
- Any operating system that communicates over TCP/IP and supports Web Services

Cryptographic Processing

Asymmetric Keys
- RSA 1024, 2048, 3072, 4096 IAW X 9.31
- ECDSA (Named Curve) IAW 9.32

Symmetric Keys
- AES 128x, 192x, 256
- TDES - 2 key and 3 key

Digital Signing
- RSA 1024, 2048, 3072, 4096 with SHA-1 IAW X 9.31
- RSA 1024, 2048, 3072, 4096 with SHA-1, SHA-256, 384, 512
- IAW PKCS#1 V.1.5 and PSS
- ECDSA (NIST curves) with SHA-1, SHA-256, 512
- DSA with SHA-1
- DSA (512-1024 bit)

XML Cryptography
- XML Sign - IAW XML DSig
- XML Verify- IAW XML DSig
- XML Encrypt - IAW XML Enc
- XML Decrypt - IAW XML Enc

Regulatory Certifications
- Includes a FIPS 140-2 Level 3 cryptographic module inside
- UL 1950 (EN60950) & CSA
- C22.2 Safety Compliant
- FCC Part 15 — Class B
- RoHS Compliant

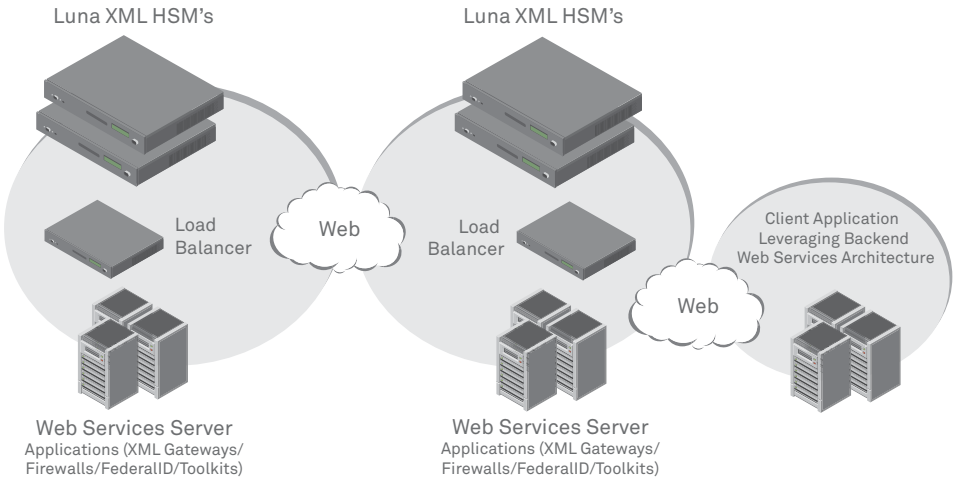
Physical Characteristics

Host Connectivity
- 2x 10/100/1000 Ethernet
- Luna PED authentication port
- Local serial console port
- Luna Token PC-Card slot

Dimensions
- 1U full-length 19" rackmount chassis
- 19.0" x 20.6" x 1.725"
- Weight 35 lbs (15.9 kg)

Power Requirements
- 1.5A @ 120V Max

Removable Storage
- PC Card Type 11 Slot, 5V (+/-0.25V)



Sample Deployment in XML Enviornment

Platform Independent Client

The interface between Luna XML and a client application is based on SOAP over HTTPS, defined in a standard Web Services Description Language (WSDL). Luna XML client applications can be developed in any programming language on any platform: from a small handheld device to a mainframe computer. This feature gives customers ultimate power and flexibility to develop client applications based on their requirements and to their favorite platforms, programming languages and tools.

SOAP Cryptographic Operations

- Generate RSA/DSA/ECDSA key pairs
- Generate AES/DES/DES2/DES3 symmeric keys
- Generate Random Numbers
- Generate Certificate Signing Requests
- Delete/View/List Objects
- Extract/Inject Keys and X.509 Certificates
- Add/Delete/Update/View Users
- Encrypt/Decrypt
- Sign/Verify
- xmlEncrypt/xmlDecrypt
- xmlSign/xmlVerify

Enterprise Data Protection

SafeNet Luna XML is a key component of SafeNet's comprehensive enterprise data protection solution to reduce the cost and complexity of regulatory compliance, data privacy, and information risk management. SafeNet Enterprise Data Protection (EDP) is the only solution that secures data across the connected enterprise, from core to edge, with protection of data at rest, data in transit, and data in use. Unlike disparate, multi-vendor point solutions that can create limited "islands" of security, SafeNet EDP provides an integrated security platform with centralized policy management and reporting for seamless, cost-efficient management of encrypted data across databases, applications, networks, and endpoint devices. For more information, visit www.safenet-inc.com/EDP

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