

# SafeNet Luna XML

## XML Interface Hardware Security Module (HSM)

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 due to complex security API's. Luna XML has a zero footprint on the host application server - providing for rapid, independent, flexible, and highly scalable deployments. Fast, Easy, Secure.

### Benefits

Easy to deploy and integrate

Simple programming interface

Platform independent

Total network scalability

Enables secure B2B and B2C business applications

Clientless

Secure application connection authentication

Reduced development time

### Ease of Integration

SafeNet Luna XML has a Web services cryptographic interface, using XML/SOAP as the messaging interface. It is easy to use and requires no prior knowledge of existing API's, 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.

In addition, 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. Luna XML 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.

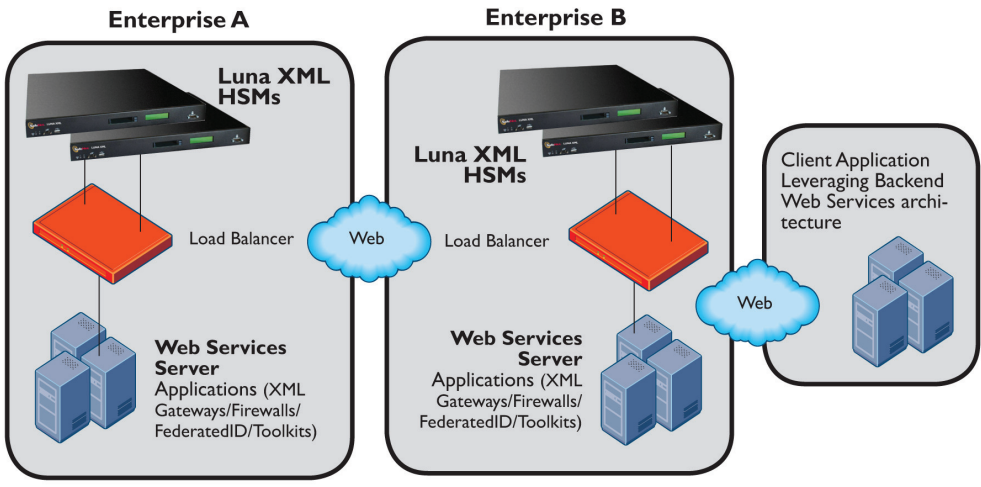
### High Availability and Scalability

SafeNet Luna XML scales as a Web service to meet your demands as applications grow. Core configuration parameters are upgradeable via software, allowing 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.

### 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.





Sample Deployment in XML Environment

**About SafeNet, Inc.**

SafeNet is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property, and digital identities, and offers a full spectrum of products, including hardware, software, and chips. UBS, Nokia, Fujitsu, Hitachi, Bank of America, Adobe, Cisco Systems, Microsoft, Samsung, Texas Instruments, the U.S. Departments of Defense and Homeland Security, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. In 2007, SafeNet was taken private by Vector Capital. For more information, visit [www.safenet-inc.com](http://www.safenet-inc.com).

**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, 384
- 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

**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)

**Regulatory Certifications**

- FIPS 140-2 Level 3
- UL 1950 (EN60950) & CSA
- C22.2 Safety Compliant
- FCC Part 15 — Class B
- RoHS Compliant



[www.safenet-inc.com](http://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](mailto:info@safenet-inc.com)

**EMEA Headquarters:**

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

**APAC Headquarters:**

Tel.: +852 3157 7111, Email: [info.apac@safenet-inc.com](mailto:info.apac@safenet-inc.com)

For all office locations and contact information, please visit [www.safenet-inc.com/company/contact.asp](http://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.