Approach to Key Security: Keys in Hardware
SafeNet Luna Network HSM is the most trusted general purpose HSM on the market in part because of its unique approach to protecting cryptographic keys. Unlike other methods of key storage which move keys outside of the HSM into a “trusted layer,” the keys-in-hardware approach protects the keys throughout their lifecycle within the FIPS 140-2 validated confines of the SafeNet Luna HSM. This method ensures that your keys always benefit from both physical and logical protections of the network HSM and reduces your audit burden.

The Leading Hardware Security Module for the Cloud
A single SafeNet Luna Network HSM can be separated into 100 cryptographically isolated partitions, with each partition functioning as if it was an independent HSM. This provides a tremendous amount of scalability and flexibility, as a single HSM can protect the cryptographic keys of hundreds of independent applications concurrently.

What’s more, the ability to assign a unique Partition Security Officer to each partition means the configurations of partitions and control over cryptographic keys can be strictly enforced, even in public cloud environments. For service providers, this means partitions can be offered as rentable services and your customers can maintain the trust and confidence that only they have access to their partition and sensitive cryptographic keys.

Flexible Backup and Disaster Recovery Options
SafeNet Luna Network HSM provides secure, auditable and flexible options to simplify backup, duplication, and disaster recovery. Key backups can be performed locally or remotely to a SafeNet Luna Backup HSM, or other SafeNet HSMs.

Secure Audit Logging
SafeNet Luna Network HSM can be configured to selectively log HSM events for security auditing purposes. This allows for separation of duties between an Audit Officer/Team and the people they are auditing – preventing both the administrative and user personnel from tampering with the log files and the auditors from doing anything administrative or accessing keys.

Benefits & Features
Most Secure
- Keys in hardware
- Remote Management
- Secure transport mode for high-assurance delivery
- Multi-level access control
- Multi-part splits for all access control keys
- Intrusion-resistant, tamper-evident hardware
- Suite B algorithm support
- Secure decommission
- Secure Audit Logging
- Strongest cryptographic algorithms

Sample Applications
- PKI key generation and key storage (online and offline CA keys)
- HSM-as-a-Service for private and public cloud environments
- Certificate validation and signing
- Code signing
- Document signing including remote signing use cases
- Transaction processing
- Database encryption
- Smart card issuance
- Hardware root of trust for the IoT
Operational Enhancements

The enhanced SNMP trap functionality of SafeNet Luna Network HSM provides operations teams with real-time visibility into important events related to their HSM infrastructure. Support for the leading Security Information and Event Management (SIEM) platforms enables deeper analysis and streamlined reporting of HSM events.

Common Architecture

All SafeNet general purpose HSMs benefit from a common architecture where the supported client, APIs, algorithms, and authentication methods are consistent across the entire general purpose product line. This eliminates the need to design applications around a specific HSM, and provides the flexibility to move keys from form factor to form factor.

Available in Two Performance Models

SafeNet Luna Network HSM is available in two performance models: SafeNet Luna Network HSM 7000 is a high performance HSM capable of best-in-class performance across a breadth of algorithms including ECC, RSA, and symmetric transactions. SafeNet Luna Network HSM 7000 also features dual, hot-swappable power supplies that ensure consistent performance and no down-time. The standard performance variant, SafeNet Luna Network HSM 1700, includes a single power supply, and is capable of 1700 RSA 1024-bit transactions per second (tps).

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>SafeNet Luna Network HSM 1700</th>
<th>SafeNet Luna Network HSM 7000</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-1024</td>
<td>1,700 tps</td>
<td>7,000 tps</td>
</tr>
<tr>
<td>RSA-2048</td>
<td>350 tps</td>
<td>1,200 tps</td>
</tr>
<tr>
<td>ECC P256</td>
<td>570 tps</td>
<td>2,000 tps</td>
</tr>
<tr>
<td>ECIES</td>
<td>200 tps</td>
<td>300 tps</td>
</tr>
<tr>
<td>AES-GCM</td>
<td>3,700 tps</td>
<td>3,700 tps</td>
</tr>
</tbody>
</table>

Contact Us: For all office locations and contact information, please visit www.safenet.gemalto.com/contact-us/
Follow Us: blog.gemalto.com/security/