Luna SA PKI Bundle

PRODUCT BRIEF

Solution Benefits

Simplicity from Start to Finish

- Easy to use
- Simple to manage
- Integrates with existing technology
- Flexible and scalable
- Offers out-of-the-box best practices policy configurations

Highly Secure

- High Assurance
- Separation of duties
- Online and offline capabilities
- FIPS 140-2 validated cryptographic module
- Common Criteria EAL 4+ certification in process

Cost-effective

- Reduces hardware and software costs
- Saves customers time and money
- Reduces operational and administrative costs

In a PKI environment, it is essential that private keys and certificates are guarded with a reliable key management solution that not only protects against ever-evolving data threats, but mounting compliance mandates as well. Storing cryptographic keys and certificates in hardware on a dedicated, centralized hardware security module (HSM) that is wrapped in multiple levels of security eliminates the risk of loss or theft, and is the only definitive method of ensuring and enforcing trusted, granular security policies.

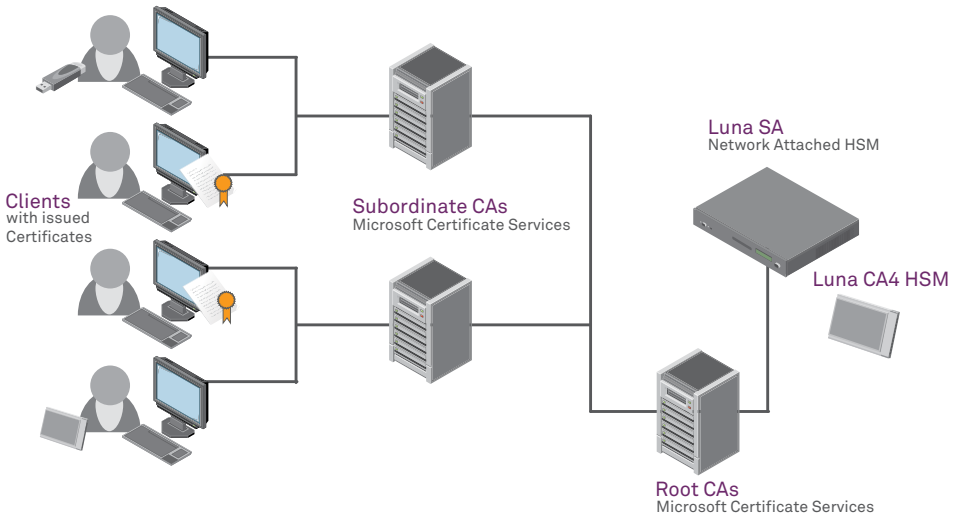
Customers and partners alike have asked for an alternative to the costly and complex solution of multiple hardware devices that require a high level of administration. They desire an approach that allows them to leverage existing technology investments, increase efficiency yet reduce costs, administration, and complexity.

Less Hardware, More Flexibility

With the SafeNet Luna SA PKI Bundle solution, enterprises can realize significant product and maintenance cost savings, as the HSM functionality (key generation/offline root/online root/key export) is made available using one device as opposed to two or three. This approach can enhance any application that involves multiple certification authorities (CAs) with certificates and root keys. It can also be advantageous in managed PKI and key escrow situations.

The PKI Bundle solution allows you to easily and quickly bring your offline CA online, and then remove it when you are done. It also provides the ability to host a dual-purpose key export and key protection HSM, while maintaining FIPS validation on both HSM devices, ensuring that sensitive key material cannot leak to the export token.

PKI Root Key Protection



The PKI Bundle solution is incredibly easy to implement and manage, and provides out-of-the-box best practices policy configurations with an extremely high level of granularity. Features of the PKI Bundle solution include the following:

- Up to 20 partitions for signing and key generation
- Key protection with key generation and export partition
- High performance key generation and export with key protection partition
- Key protection with removable root key partition
- PCMCIA tokens appear as partitions accessible via the same client API as the parent HSM
- Internal Luna SA PCMCIA card reader allows you to host additional HSM tokens
- Key archival supported with segregated Key Management HSMs
- Signing Luna SA with Key Extraction token
- Signing Luna SA with CA4 token
- Export Luna SA with CA4 token

Key Components of the PKI Bundle Solution

The Luna SA provides built-in support for up to two additional, PCMCIA-based HSMs via the SA's integrated card reader, which is accessible through the same client API as the Luna SA. These tokens can be the CA4 and PCM KE (Key Extractions) tokens. Any combination of these two tokens can be used within the internal card reader, providing a flexible deployment option for the customer.

With both online and offline capability for CA key generation and storage, the Luna SA can satisfy the requirement for PKI root key protection. The HSM's support for multiple configuration profiles supports the desire to maintain online and highly available Issuing CAs, while keeping the Root and Policy CAs in offline mode. In just such a scenario, an organization can incorporate the Luna SA network-attached HSM and the Luna CA4 PCMCIA-based HSM for separation of duties and policy, with each component owned and controlled by different individuals and applications, yet all controlled through a single client API.

The Luna SA, and the PCMCIA cards deployed within the SA card reader, can also be configured in High Availability mode to provide reliable and transparent HSM connectivity for any systems leveraging the combined HSM offering.

All HSM components within this product offering—SA, CA4, and KE token—support a redundant, high availability (HA) deployment option, which is inherited as part of the Luna SA client that each HSM leverages. This redundant HA feature allows for automated key-synchronization between duplicated components.

The SafeNet PKI Bundle solution provides significant advantages for PKI management over its competitors. Not only do its multi-faceted features respond directly to consumer demand, but they are wrapped in a solution that saves the customer time, effort, and money. Scalability and cost control are built in as new partitions can be added to existing HSMs instead of having to adding new physical devices. The Luna SA can also be leveraged by other applications (beyond PKI) that require HSM cryptographic services.

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