

SURFnet Selects Thales Luna HSMs to Secure DNSSEC Material

Thales Luna HSMs Safeguard Thousands of DNS Zones for National Computer Network in the Netherlands

SURFnet enables groundbreaking education and research—designing and operating the hybrid SURFnet network, as well as providing innovative services in the field of trusted identities and electronic collaboration.

The SURFnet network is the national computer network for higher education and research in the Netherlands. Connecting to the SURFnet network is restricted to the following organizations:

- Universities
- Academic hospitals and teaching hospitals
- Institutes for higher professional education
- Research institutes
- Corporate R & D departments
- Libraries
- Other organizations funded by the Ministry of Education, Culture and Sciences

Business Challenge

Because SURFnet is a provider of network support for a large constituency of organizations, including universities, hospitals, research institutes, corporate research bodies, and scientific libraries, they needed to safeguard private key material used in DNS Security Extensions (DNSSEC).

With such large amounts of information in play for SURFnet's network and its large constituency, its network has opened itself up to standard DNS security flaws, where unsecured and vulnerable caching name servers are easy targets for hackers to hijack Web traffic containing sensitive data. SURFnet recognized the need to add DNSSEC to its repertoire to protect their network from many vulnerabilities, including cache poisoning, man-in-the-middle attacks, rerouting of e-mails, and denial-of-service attacks.

As a provider of a massive network of respected bodies and institutions in the Netherlands, SURFnet needed a DNS security solution that was:

- Compatible with OpenDNSSEC, an Open Source software that manages security for DNS.
- Compliant with the PKCS#11 standard, which calls for a platform-independent API to the HSM.
- Supported by world-class customer support.
- Provided by a reliable and reputable security provider.



“Thales met the requirements for robust security and the availability needed to ensure integrity of the domain name space and matched our performance needs, which are based on our large number of supported network organizations across the Netherlands. Luna HSMs gave us the much-needed ability to back up data securely and quickly, as well as managing security keys to maintain the integrity of those keys.”

– Roland van Rijswijk SURFnet

Solution

SURFnet evaluated a number of security vendors' solutions for DNSSEC and chose Luna HSMs for its standards-based DNSSEC solution backed by superior customer support.

After testing their DNSSEC options, SURFnet found Luna HSMs to:

- Secure digital signatures in order to ensure the validity of response to queries through every zone in the DNS hierarchy, and establish the chain of trust.
- Control access so only authorized customers and internal staff can access sensitive applications and data.
- Scale to accommodate high-volume processing.
- Have secure backup features.
- Store all key material in hardware ensuring integrity and protection of all hardware keys.
- Provide standardized PKCS#11 support for application integration to the Luna HSMs.

SURFnet will initially deploy DNSSEC for its own domain to pioneer the technology on its network. It will then deploy the technology for its large constituency, leveraging the scalability offered by Luna HSMs. SURFnet will operate the Luna HSMs in high-availability mode to ensure maximum redundancy for this critical infrastructure.

"Thales has proven to be an elite security vendor for our DNSSEC rollout. The Luna HSMs were scalable, easy to deploy, and let us install security through a phased approach, thus allowing for maintenance of ongoing network viability," said Roland van Rijswijk for SURFnet. "The compliance to PKCS standards, as well as its FIPS 140-2 Level 3 and Common Criteria EAL 4+ certifications, combined with its compatibility to OpenDNSSEC has shown our constituents that we are serious protecting the vulnerabilities in DNS technology."

Benefits

Since deploying Luna HSMs, SURFnet has revamped its key management capabilities through key generation, distribution, rotation, storage, termination, and archival—keeping the private DNSSEC signing key and DNS server secure at all time. Luna HSMs also boosted SURFnet's cryptographic processing capabilities, by offloading it from application servers and storing cryptographic keys in a centralized, hardened device; thereby eliminating the risks associated with having these assets housed on poorly secured platforms. Using Luna HSMs has also allowed SURFnet to significantly streamline security administration.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.