cpl.thalesgroup.com

THALES

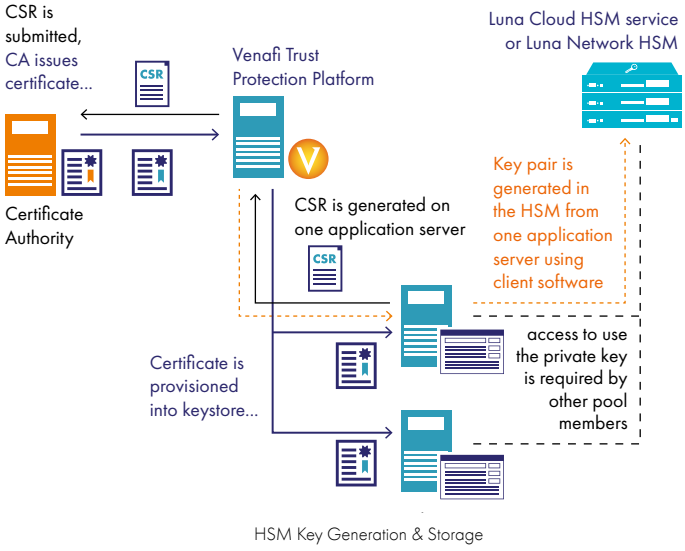
Automated Key and Certificate Life Cycle Management

Secure Web Applications with Venafi Advanced Key Protect and Thales HSMs

Scaling the use of HTTPS has always required trade-offs between security and efficiency. Using machine identities to enable Encryption Everywhere strategies requires that more Secure Sockets Layer/ Transport Layer Security (SSL/TLS) keys and certificates be deployed in more locations. Managing this not only increases resource demands on an organization, it also exponentially increases the risk of exposing keys stored in software.

To help reduce the risk of a data breach, meet compliance requirements, and simplify machine identity protection, Venafi® and Thales have combined the benefits of automated key and certificate life cycle management with Thales' on-premises or cloud-based hardware security module (HSM) key protection with an add-on module to the Venafi Platform called Advanced Key Protect. This out-of-the-box solution delivers full visibility, centralized control and full automation over HTTPS web application keys and certificates. All keys are generated, stored, and used for SSL/TLS within the safe confines of Thales Luna HSMs to reduce the risk of unauthorized data access and loss.

VENAFI®



Enhanced Security Automation

Venafi and Thales deliver a seamless integration that expands an organization's ability to secure HTTPS keys with the power of Thales HSMs to perform cryptographic operations, no matter where deployed or used. Now your organization can automate the full key and certificate life cycle with HSMs for Microsoft,

Apache, and Java applications—from key generation to certificate installation and renewal.

All operations are performed without an administrator executing manual tasks on servers or virtual machines. Advanced Key Protect securely generates key pairs in the HSM where they can be accessed by applications, while ensuring the private keys never leave the hardened, tamper-resistant HSM appliance. Alternatively, Venafi leverages Luna HSMs to generate a key pair, exports it from the HSM, and installs the key and certificate on system that will use the key and certificate. This offers the application a root of trust for your master encryption keys. With either use case, all operations are performed according to the common, centralized policy shared across the Venafi Platform for key and certificate generation, use and renewal.

The integrated solution strengthens your organization's machine identity protection programs by eliminating time-consuming tasks, which can also increase the risk of exposing private keys and introduce errors that threaten application availability. The integration relies on Venafi workflow, policy and auditing capabilities in combination with Luna HSMs, while also supporting the growing number of Certificate Authorities (CAs) in the Venafi Technology Network.

How It Works

Advanced Key Protect automates keys and certificates generated and stored in Luna HSMs for popular application servers. Venafi uses Thales-validated integrations throughout the entire automated life cycle:

1. Venafi Platform requests that web server keys be generated in the Thales Luna HSM, using native commands in Microsoft, Apache, and Java that communicate with Thales libraries.
2. Following key generation, a certificate request is initiated. All Venafi native policy, workflow and CA integrations are supported.
3. Once the certificate is approved and received by the Venafi Platform, it is installed automatically at the application. The process is validated and logged and can be audited at any time.
4. When a certificate is renewed, or a key rolled over, the full process is repeated and automated by the Venafi Platform according to the organization's policy.

Thales HSMs

The security of the SSL/TLS session is dependent on the security of the accompanying web server private keys. Organizations that require a high level of assurance protect their SSL/TLS keys in Luna HSMs. The Thales keys-in-hardware approach ensures your key pairs are securely generated in hardware and that your private key always remains centrally and securely stored, free from rogue administrators and hackers.

Thales offers two solutions that can generate and store the server keys, providing private key protection and strong entropy.

- Data Protection on Demand Luna Cloud HSM service Is a cloud-based HSM that can be deployed within minutes and no need for specialized hardware or associated skills.
- Luna HSMs store, protect and manage sensitive cryptographic keys on-premises in FIPS 140-2 Level 3, tamper-resistant hardware appliances, providing high-assurance key protection within an organization's own IT infrastructure.

In addition, you can extend your HSM investment to address other use cases, including PKI, code and document signing, Transparent Data Encryption, blockchain and migration to the cloud.

Venafi Platform

The Venafi Platform protects machine identities by orchestrating cryptographic keys and digital certificates for SSL/TLS, IoT, mobile, and SSH for the extended enterprise—on-premises, mobile, virtual, cloud, and IoT—at machine speed and scale. Venafi automates the entire key and certificate life cycle as well as remediation to reduce or eliminate security and availability risks connected with weak certificates (such as SHA-1, MD5 or wildcard certificates) or compromised machine identities.

Together, We Can Help

The Venafi Platform and Thales HSMs work together to secure and manage your cryptographic keys:

- Improve your machine identity protection through the fully automated, high-speed key and certificate life cycle operations delivered by the Venafi Platform
- Protect your organization from breach with the Luna HSM hardware root of trust

About Venafi

Venafi is the cybersecurity market leader in machine identity protection, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe encryption, authentication and authorization. Organizations use Venafi key and certificate security to deliver safe machine-to-machine connections and communications—protecting commerce, critical systems and data, and mobile and user access.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us