Scaling the use of HTTPS has always required tradeoffs. Using machine identities to enable Encryption Everywhere strategies requires more Secure Sockets Layer (SSL) / Transport Layer Security (TLS) keys and certificates deployed in more locations. This not only increases the management demands on the organization including people and time, but also exponentially increases the risk of keys in software being exposed.

To help you reduce data breach threats, meet compliance requirements, and simplify machine identity protection, we have combined the benefits of Venafi’s automated key and certificate lifecycle management, together with Gemalto’s FIPS 140-2 hardware security module (HSM) key protection. As an organization, you now have full visibility, centralized control, and trust over your webserver keys and certificates, while reducing the risk of unauthorized data access or data loss by ensuring keys are generated and stored within the safe confines of the HSM.

Enhanced Security Automation

Venafi® and Gemalto® deliver a seamless integration that expands an organization’s ability to secure HTTPS keys by leveraging SafeNet Luna Network HSMs to generate cryptographic operations in a centralized model. Automate full key and certificate lifecycles: from key generation to certificate installation and renewal. All operations are performed without an administrator having to execute manual tasks on servers or virtual machines. Key pairs are now securely generated in the HSM where they can be accessed by applications, and the private keys never leave the hardened, tamper-resistant HSM appliance. Furthermore, centralized policy control can be established and enforced to ensure the right key policies and attributes are being implemented. Lastly, this integrated solution eliminates 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’s powerful workflow, policy, and auditing works with the growing number of Certificate Authorities (CAs) in the Venafi Technology Network.

Solution Benefits

- Automated, easy to deploy SSL/TLS key lifecycle management
- Reduce risks with high-assurance, FIPS 140-2 HSM webserver key protection
- Support for Microsoft, Apache, and Java applications
- Simplify compliance auditing and – always know the location of your keys and certs

Organizations leveraging Venafi’s centralized management solution have increased agility to respond to incidents, minimize system and data breaches, and expand their Encryption Everywhere strategies with the security and performance of Gemalto HSMs.
How It Works

The Venafi Platform automates lifecycle management of certificates and keys generated and stored in SafeNet Luna Network HSMs for popular application servers. Venafi uses SafeNet-validated integrations through the entire automated lifecycle:

1. Venafi Trust Protection Platform requests webserver keys be generated in the SafeNet Luna Network HSM, using Microsoft, Apache, and Java-native commands that communicate with the SafeNet 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, the certificate will be transferred and installed automatically at the application and enabled for use. The process is validated and logged, and can be audited at any time with all of Venafi’s powerful reporting and analysis capabilities.
4. When a certificate is to be renewed or key rolled over, the full process is repeated and automated according to an organization’s policy.

High-Assurance Key Protection with SafeNet Luna HSMs

The security of the SSL/TLS session is contingent on the security of the accompanying webserver private keys. Organizations that require a high level of assurance protect their SSL/TLS keys in FIPS 140-2 Level 2 or 3 certified SafeNet Luna Network HSMs - tamper-resistant, network-attached appliances. Gemalto’s keys-in-hardware approach ensures your key pairs are securely generated in hardware, and your private key always remains centrally and securely stored, free from rogue administrators and hackers. Additionally, SafeNet Luna HSM scalability enables you to meet performance and availability requirements, regardless of the size of your SSL/TLS deployment.

In addition to the benefits offered for SSL/TLS, you can then extend your SafeNet Luna Network HSM investment and reduce your total cost of ownership by leveraging your HSM to address other use cases including PKI, code and document signing, TDE, blockchain, and migration to the cloud.

Venafi Platform

Venafi Protection Platform protects machine identities by delivering an enterprise-grade platform designed for security, operational efficiency and organizational compliance. The platform provides visibility of all machine identities across the extended enterprise. With full situational awareness of cryptographic security risk posture at all times, organizations are able to automate the identification of weak certificates, such as SHA-1, MD5 or wildcards while enabling quick response with automated remediation.

Together we can help

Many enterprises today depend on the industry-leading Venafi Protection Platform to address their key and certificate lifecycle management, together with SafeNet Luna Network HSMs to protect cryptographic keys. Contact us to learn how you can improve your machine identity protection through our fully automated, high-speed key and certificate lifecycle operations, and protect yourself against a breach with our HSM hardware root of trust.

About Gemalto’s SafeNet Identity And Data Protection Solutions

Gemalto’s portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions—from the edge to the core. Gemalto’s SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters.

Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

About Venafi

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