Automated Key and Certificate Life Cycle Management

Secure web applications with the Venafi Platform and the Gemalto SafeNet 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 data breach, meet compliance requirements and simplify machine identity protection, Venafi® and Gemalto® have combined the benefits of automated key and certificate life cycle management with FIPS 140-2 hardware security module (HSM) key protection. This combination 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 SafeNet HSMs to reduce the risk of unauthorized data access and loss.

Enhanced Security Automation

Venafi and Gemalto deliver a seamless integration that expands an organization’s ability to secure HTTPS keys with the power of SafeNet Network HSMs to perform cryptographic operations no matter where deployed or used. Now your organization can automate the full key and certificate life cycle with SafeNet 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. Key pairs are securely generated in the HSM where they can be accessed by applications, and the private keys never leave the hardened, tamper-resistant HSM appliance. 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 SafeNet HSMs, while also supporting the growing number of Certificate Authorities (CAs) in the Venafi Technology Network.

Solution Benefits

- Get automated, easy-to-deploy SSL/TLS key life cycle management.
- Reduce risks with high-assurance, FIPS 140-2 HSM web server key protection.
- Leverage support for Microsoft, Apache and Java applications.
- Simplify compliance auditing—always know the location of your keys and certificates.
How It Works
The Venafi Platform automates keys and certificates generated and stored in SafeNet HSMs for popular application servers. Venafi uses Gemalto-validated integrations throughout the entire automated life cycle:
1. Venafi Platform requests that web server keys be generated in the SafeNet Network HSM, using native commands in Microsoft, Apache and Java that communicate with 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, 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.

Gemalto SafeNet 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 FIPS 140-2 Level 2 or 3 certified SafeNet Network HSMs. The Gemalto 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. Additionally, Gemalto HSM scalability enables you to meet performance and availability requirements, regardless of the size of your SSL/TLS deployment.

In addition, you can extend your SafeNet Network HSM investment by leveraging your HSM to address other use cases, including PKI, code and document signing, TDE, 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 SafeNet 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 Gemalto 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.

ABOUT GEMALTO’S SAFENET IDENTITY AND DATA PROTECTION SOLUTIONS
Gemalto 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.