Delivering Scalable Private Key Security with Hardware Security Module Leaders

Advanced Key Protect at a Glance
Venafi Advanced Key Protect powers the use of safe cryptographic keys by orchestrating HSM-based generation and storage of cryptographically strong keys across the enterprise.

Prerequisites
• The Venafi Platform
• One of the following
  - Gemalto SafeNet Network HSM
  - Thales nShield Connect

Benefits
• Achieve out-of-the-box compliance with PCI DSS 3.6.1 and 3.6.3
• Minimize risk of compromise through side-channel attacks (like Spectre and Meltdown)
• Leverage your existing HSM investment for strong key generation and storage
• Orchestrate strong keys across your enterprise
• Maintain private keys under enterprise policy control

Until now, enterprises that wanted to use the strong private keys generated from their Hardware Security Modules (HSMs) with the Venafi Platform had to rely on custom development or resource-intensive manual processes. With the introduction of Venafi Advanced Key Protect, organizations can now use the Venafi Platform for the fast, automated orchestration of secure HSM key generation, installation and storage to improve security, increase efficiencies and meet compliance requirements.

As the number of severe vulnerabilities and attacks targeting encryption keys and processes increases, the need for stronger keys throughout the enterprise is becoming more acute. For example, recent side-channel attacks have dramatically increased security risk by making private keys, typically stored in files or memory, more susceptible to compromise.

HSM-generated keys address these risks by producing strong keys with maximum entropy and random number generation. Additionally, HSMs provide secure storage that is accessible at machine speed.

HSM security benefits are so strong that regulations like PCI-DSS mandate that all private cryptographic key material be generated and stored within an HSM to protect in-scope PCI systems. Beyond PCI, organizations can substantially improve their overall security by leveraging HSMs to protect private cryptographic key material across the enterprise.
Traditionally, HSMs have only been deployed for a narrow set of applications. Despite the improved key strength and overall protection that HSMs provide for digital keys, their capabilities have not been utilized broadly to secure a wide range of important enterprise applications. With Venafi Advanced Key Protect, organizations can significantly increase the value they get from their HSMs.

HSM Key Management Challenges

Broad HSM usage without key life cycle orchestration creates new challenges for organizations that want complete visibility into all of their keystores—even for the keys stored in the HSM. Organizations that deploy HSMs widely also lack the ability to centrally manage all their distributed keystores and are unable to consistently apply enterprise policy controls.

Previously, when organizations wanted to use automation to leverage strong HSM keys, manage the entire key life cycle, apply policies or streamline workflows, they had to create custom scripts or run manual processes—both of which require major investments. These largely manual efforts often resulted in high-maintenance, error-prone solutions that did not scale.

The Solution: Venafi Advanced Key Protect

Venafi Advanced Key Protect delivers an out-of-the-box solution that overcomes these challenges. It integrates with industry-leading HSMs, including Thales and Gemalto, to leverage strong HSM keys throughout an enterprise. As an add-on module to the Venafi Platform, Advanced Key Protect applies policy and workflow controls and enables fast, automated orchestration of keys. Together, these capabilities make it possible for enterprises to ensure the consistent use of the strongest cryptographic keys possible.

Supported client versions

- Gemalto/SafeNet (Luna) client version 6.2.2 (plus OpenSSL toolkit 1.0.2 for Apache)
- Thales/nCipher Security World client version 12.40.2

Earliest supported versions of HSM models

- Gemalto SafeNet Network HSM (formerly Luna SA)
  - Models 1700 for Cryptographic Key Export (this is only required for central key generation)
  - Models 7000 running software version 5.4.7-1 and firmware version 6.10.9

How It Works

Venafi Advanced Key Protect improves private key security in two important ways: it allows users to generate strong keys from a central HSM and also provides flexible management of the entire HSM key life cycle for enterprise applications.

Strong central key generation

The Venafi Platform leverages a central HSM—either Gemalto or Thales—to generate key pairs, delivering keys created with strong random number generation.

HSM key life cycle management

Once Venafi Advanced Key Protect triggers the generation of a key pair by the HSM, it then follows one of these two approaches:

1. The Venafi Platform orchestrates the connection to the system that needs the certificate. The key pair is securely maintained on the HSM, delivering HSM-based key protection, and the private key never leaves the HSM. Both Gemalto and Thales HSMs enable this approach and this capability is supported on Apache, Windows IIS and Java.

Private Key Securely Maintained on HSM
When administrators enter application and HSM information into the Venafi Platform, it triggers the following actions by the platform:

• Connects to the managed application and instructs the HSM to generate a key pair
• Retrieves a certificate-signing request (CSR) from the HSM through the managed application
• Uses the CSR for certificate enrollment with a certificate authority (CA)
• Installs the certificate on the managed application (the private key remains on the HSM)

2. For this second option, the Venafi Platform can be used to generate all X.509 and SSH keys in a central HSM, even for applications that do not have the capability to integrate with an HSM. In this approach, instead of keeping the private key in the HSM, the key pair is exported from the HSM and the private key and certificate are installed on the system that will use them. This capability is supported by Gemalto.

Private Key and Certificate Installed on Managed Application

Again, this process begins when an administrator enters application and HSM information into the Venafi Platform, but it triggers these actions by the platform:

• Instructs the HSM to generate a key pair
• Retrieves the private key and a certificate-signing request (CSR) from the HSM
• Uses the CSR for certificate enrollment with a certificate authority (CA)
• Installs the certificate and the private key on the managed application

Next Steps

If you have the Venafi Platform and a Gemalto or Thales HSM, or you’re considering investing in these solutions to deliver strong and secure cryptographic keys, contact us to learn more.

TRUSTED BY THE TOP

5 OF 5 Top U.S. Health Insurers
5 OF 5 Top U.S. Airlines
4 OF 5 Top U.S. Retailers
4 OF 5 Top U.S. Banks
4 OF 5 Top U.K. Banks
4 OF 5 Top S. African Banks
4 OF 5 Top AU Banks

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 machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.

To learn more, visit www.venafi.com