cpl.thalesgroup.com

THALES
Building a future we can all trust

Securing the Code Signing Process

Venafi Next-Gen Code Signing and Thales Luna HSMs

With the development of software for internal and external distribution, most are now software businesses. Code signing is a critical security control that helps businesses and their customers know software can be trusted. Even though code signing has protected businesses and consumers for decades, there has been an increase in cybercriminals stealing, forging, or leveraging vulnerabilities in the code signing process. This increases the risk that critical internal software infrastructure is compromised by hackers or the reputation of a business is damaged when malware is inserted by a third party into their software products.

The first step in protecting code signing is to store private keys in a hardware security module (HSM), such as on-premises Luna HSM or cloud-based Data Protection on Demand (DPoD) Luna Cloud HSM service. These secure, FIPS 140-2 Level 3 compliant solutions maintain Root-of-Trust private key protection. However, cybercriminals have learned to exploit the code signing process making it critical to secure.

Secured Key Storage. Secured code signing process.

Venafi Next-Gen Code Signing and Thales HSMs (DPoD and Luna) in the cloud, on-premises or as a hybrid solution deliver a seamless integration that not only secures private code signing keys but also secures the process by enforcing industry-accepted best practices. Together, these solutions secure the storage of private code signing keys, automate code signing policy enforcement, manage the full lifecycle of code signing certificates, separate code signing roles and responsibilities, and provide a full audit trail of code signing activities.

Venafi

Focusing on the Needs of Software Development Teams

Software development teams often do not have PKI expertise, even though they are often the ones responsible for code signing. This can create a vulnerability if they make wrong choices around their code signing process.

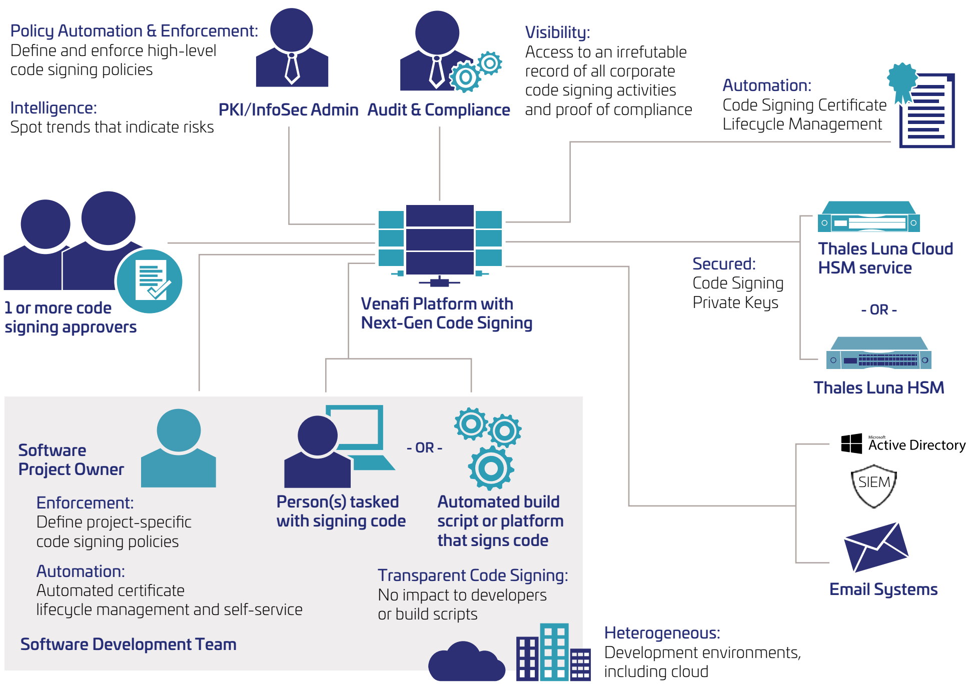
Even if their company's security team provides centralized code signing services, development teams may circumvent this because they are cumbersome to use, can't be automated, or simply take too long to perform.

To address this, it is important for InfoSec teams to provide a code signing service that focuses on the needs of their software development teams:

- Can be easily scripted and doesn't require developers to change their build process at all
- Seamlessly integrates with their existing tools and software processes, including DevOps, Continuous Integration, and Continuous Delivery
- Does not slow down software builds

How It Works

Venafi Next-Gen Code Signing automates the full certificate lifecycle in addition to enforcing and automating a secure code signing process. Software developers continue to use the code signing tools that they have always used. Private code signing keys always remain protected within the Thales DPoD and Luna HSMs. Access to these keys is controlled by the code signing process enforcement policies that have been defined in the Venafi platform.



Policy Automation & Enforcement:
Define and enforce high-level code signing policies
Intelligence:
Spot trends that indicate risks
PKI/InfoSec Admin
Audit & Compliance
Visibility:
Access to an irrefutable record of all corporate code signing activities and proof of compliance
Automation:
Code Signing Certificate Lifecycle Management
1 or more code signing approvers
Venafi Platform with Next-Gen Code Signing
Secured:
Code Signing Private Keys
Thales Luna Cloud HSM service
- OR -
Thales Luna HSM
Active Directory
SIEM
Email Systems
Software Project Owner
Enforcement:
Define project-specific code signing policies
Automation:
Automated certificate lifecycle management and self-service
Person(s) tasked with signing code
- OR -
Automated build script or platform that signs code
Transparent Code Signing:
No impact to developers or build scripts
Software Development Team
Heterogeneous:
Development environments, including cloud

Venafi Next-Gen Code Signing

Venafi Next-Gen Code Signing is built on top of the Venafi Platform which protects machine identities by orchestrating cryptographic keys and digital certificates for SSL/TLS, IoT, mobile, code signing, 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.

Thales Luna HSM Solutions

Thales offers two solutions that maintain Root of Trust private key protection for the Venafi Platform with Next-Gen Code Signing: On-premises Luna HSM, or cloud-based Data Protection on Demand Luna Cloud HSM service, provide flexibility for cloud-based, hybrid/multi-cloud or on-premises private key generation, storage and protection. This flexibility makes it easier to deploy a solution to address ever-changing compliance mandates and budgetary requirements.

- Data Protection on Demand (DPoD) Luna Cloud HSM service offers key management capabilities that can be deployed within minutes with no need for specialized hardware or associated skills.
- Luna HSMs store, protect, and manage sensitive cryptographic keys in a tamper-resistant on-premises HSM, providing high-assurance key protection within an organization's own IT infrastructure.

In addition, you can extend your investment by leveraging your Thales HSMs to address other use cases, including PKI, TLS/SSL, document signing, Transparent Data Encryption, Blockchain, and migration to the cloud and support for hybrid environments.

Together We Can Help

The Venafi Next-Gen Code Signing solution and DPoD or Luna HSMs work together to secure the storage of your code signing keys and secure your code signing process:

- Automate the code signing certificate life cycle and eliminate the need for software teams to manage this themselves
- Secure code signing activities through policy and workflow enforcement
- Provide an audit trail of all code signing activities
- Protect your private keys and certificates with Thales HSM root of trust
- Provide a code signing-as-a-service solution that software developers will want to use

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 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 amount 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.