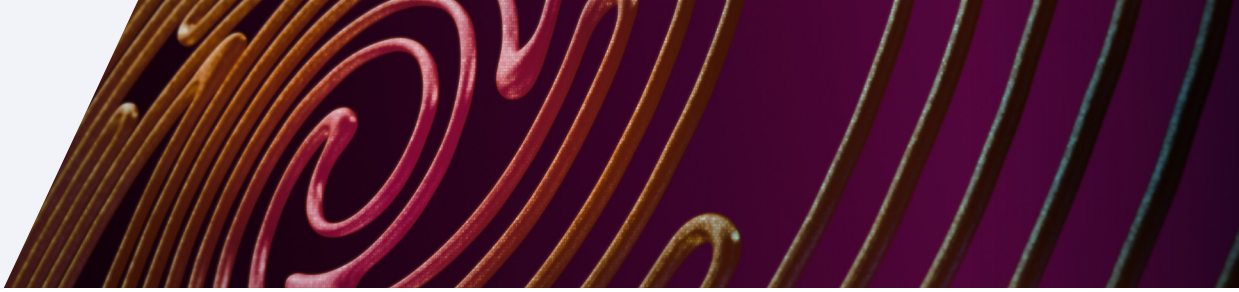
Venafi



TECH BRIEF

Adding CodeSign Protect Capabilities to the Venafi Platform

Comparing basic code signing certificate management provided by Venafi TLS Protect with additional features offered by Venafi CodeSign Protect

Venafi CodeSign Protect Technical Brief

Purpose: This technical brief compares the advanced code signing process capabilities provided by Venafi CodeSign Protect with the basic code signing certificate management capabilities available in Venafi TLS Protect.

Why This Information Is Important: While TLS Protect was designed to manage and secure all x.509 certificates, CodeSign Protect adds value for securing and automating the end-to-end code signing process.

What CodeSign Protect Adds:

- Secures code signing private keys
- Integrates with popular code signing tools
- Automates code signing workflows:
  - Which code signing certificates can be used and who can use them
  - Which code signing tools can be used
  - Who must approve code signing requests
- Enables policy control on a project-by-project basis
- Includes project-based workflows and approvals

The Venafi Trust Protection Platform, which is the foundation for most Venafi products, is designed to protect x.509 certificates like code signing certificates. Venafi TLS Protect, the flagship product on the platform, provides visibility, intelligence and automation for certificate management and security. However, it does not provide specialized protection for code signing.

With code signing, specialized protection is needed for code signing infrastructure, workflows and policy enforcement. Venafi CodeSign Protect delivers these additional capabilities to the largest, most distributed, global enterprises.

So, why is CodeSign Protect needed? TLS Protect is not optimized to manage the workflows needed to secure the end-to-end code signing process and is not integrated with common code signing tools that many developers use.

To highlight the additional value provided by CodeSign Protect, this document summarizes key differences between the certificate management capabilities provided by Venafi TLS Protect and the Venafi CodeSign Protect solution.

	Basic Management of Code Signing Certificates	Secured Code Signing Process
Capability	**TLS Protect**	**Venafi CodeSign Protect**
Private key protection	**Not included** Developers decide where to store private keys, secured or not. They must have ongoing access to private keys for all code signing activities.	**Included** Developers do not directly access private code signing keys when performing code signing operations. The keys are securely managed in either: • The Venafi Platform encrypted secret store • A connected HSM Private keys never leave Venafi CodeSign Protect, remaining securely protected.
Protection of code signing private keys while being used to sign code	**Not included** Developers must possess code signing private keys to sign code. This creates security risks and can cause key sprawl.	**Included** Code signing private keys always remain in the Venafi Platform or a connected HSM. An integration with the developer's code signing tool sends the hash of the code to the Venafi Platform, which encrypts the hash with the private key, and then returns the encrypted signature back to the developer's code signing tool—all without the developer having to perform additional steps.
Protection of private keys during certificate enrollment	**Included** Protects private keys by securely generating the key pairs required to create CSRs.	**Included**
Policy enforcement during certificate enrollment	**Included** Allows for policy enforcement of certificate attributes such as key length, algorithm, subject DN, CA template and domains.	**Included**
Policy enforcement specifying which applications can be used to sign certificates	**Not included**	**Included** Development team owners are able to specify code signing policies for their projects. This includes being able to specify which code signing certificates are available for use in a particular application.

	Basic Management of Code Signing Certificates	Secured Code Signing Process
Capability	**Core Functionality Provided by Venafi TLS Protect**	**Additional Code Signing Capability Provided by Venafi CodeSign Protect**
Policy control over which users can perform signing operations with a particular code signing certificate	**Not included**	**Included** Project-specific policies can enforce which users have access to code signing certificates, which certificates are available and who needs to approve usage.
Workflow for certificate usage	**Not included**	**Included** Specific project-based workflows and approvals are provided.
Compliance auditing of certificates in inventory	**Included** A dashboard with reporting capabilities provides visibility into all certificates in inventory. This includes critical values such as validity dates, unapproved issuers, algorithms used and key lengths.	**Included**
Discovery and identification of devices and applications with which certificates are associated	**Included** Utilizing agent and agentless discovery methods, certificates are discovered and added to inventory.	**Additional value in future release** In a future release, CodeSign Protect will support code signing certificate discovery.
Certificate actions	**Included** Certificates can be created, renewed, reissued, revoked and deleted.	**Included**
Integrations with software development code signing tools	**Not included**	**Included** Venafi CodeSign Protect integrates with the native code signing tools provided by many software development environments without requiring any additional effort from developers.

	Basic Management of Code Signing Certificates	Secured Code Signing Process
Capability	**Core Functionality Provided by Venafi TLS Protect**	**Additional Code Signing Capability Provided by Venafi CodeSign Protect**
Notifications	**Included** Comprehensive notifications are available based on logged events, including expiration notifications, validations, approvals, revocations and workflow operations.	**Included**
Reporting	**Partial support** Reports on certificates in inventory generated and filtered based on certificate attributes.	**Additional value in future release** Access to audit data and reports such as code signing activity, who signed code, which tools were used to sign code, who approved a signing operation, etc.

Contact Venafi to learn how Venafi CodeSign Protect can complement your Venafi TLS Protect deployment to better protect code signing across your organization.

Visit: **venafi.com/contact**

Trusted by

5 OF THE 5 Top U.S. Health Insurers
5 OF THE 5 Top U.S. Airlines
3 OF THE 5 Top U.S. Retailers
3 OF THE 5 Top Accounting/Consulting Firms
4 OF THE 5 Top Payment Card Issuers
4 OF THE 5 Top U.S. Banks
4 OF THE 5 Top U.K. Banks
4 OF THE 5 Top S. African Banks
4 OF THE 5 Top AU Banks

Venafi is the cybersecurity market leader in machine identity management, 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 venafi.com**