THALES

Secure Code Signing at the Speed of DevOps

With Keyfactor Code Assure and Thales HSMs

Software developers and IoT manufacturers rely on code signing to protect end users and their company's reputation. But the integrity of code signing hinges entirely on the security of your private keys. As attackers become more adept at compromising these keys to spread malware, failure to implement secure code signing practices can expose your organization to costly and often irreparable attacks.

The Challenge

Most organizations recognize the importance of code signing as a security control, but often overlook the critical aspects of protecting code signing keys and ensuring that only the right code is signed with the right certificate. As the need for code signing increases with the proliferation of software applications and IoT devices, so too does its complexity.

The burden to sign code often falls to software developers—people who specialize in code, not security. With this lack of expertise in security best practices, keys can wind up in vulnerable network locations from workstations to build servers, and who knows where else.
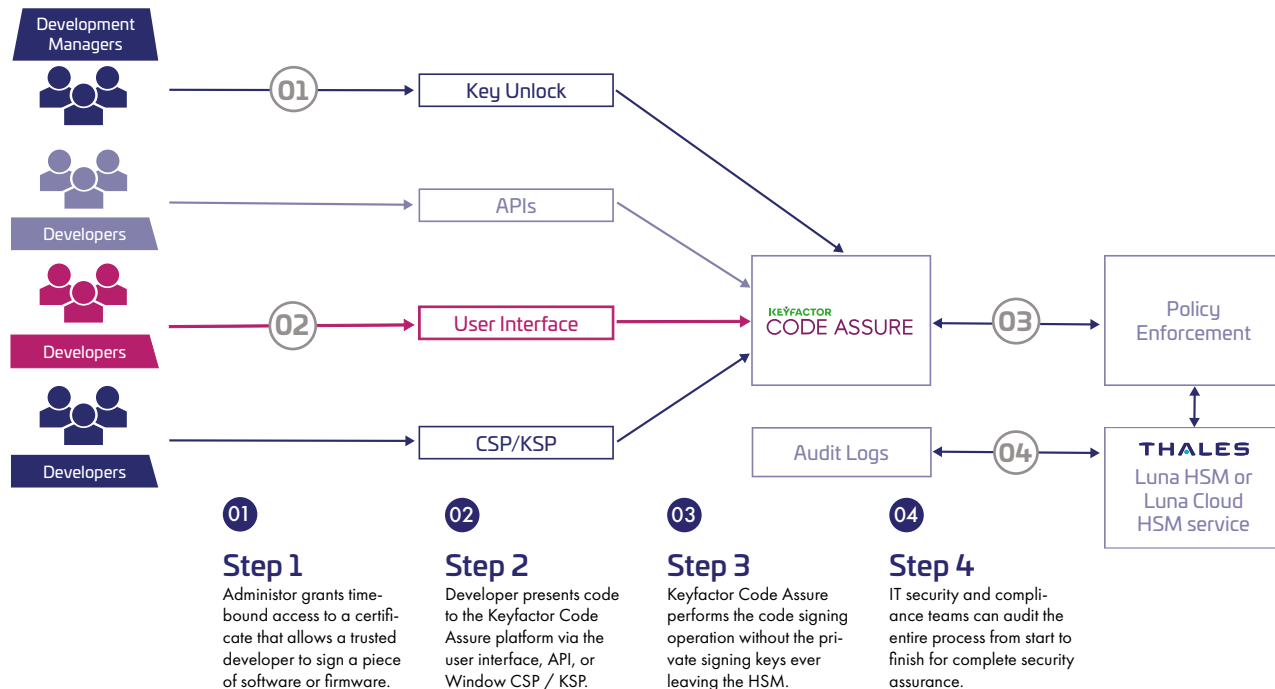
Code signing is critical, but it isn't enough on its own. Businesses must protect their keys and certificates and implement robust code signing practices. The price for falling short is a bad experience for your users and an even worse experience for your business.

The Solution

Keyfactor and Thales deliver a seamless integration that enables organizations to defend against emerging code signing threats with the combined high-level assurance of Thales hardware security modules (HSMs) and an intuitive code signing platform—Keyfactor Code Assure.

Keyfactor Code Assure is a single, centralized solution that enables developers to securely sign any code, from anywhere, while providing complete visibility and protection of all code signing activities. Private keys are stored in a centralized and secure HSM. Once inside, the keys never leave the HSM.

Thales offers two solutions that maintain Root of Trust private key protection for the Keyfactor Code Assure platform: 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.

KEYFACTOR

Step 1

Administor grants time-bound access to a certificate that allows a trusted developer to sign a piece of software or firmware.

Step 2

Developer presents code to the Keyfactor Code Assure platform via the user interface, API, or Window CSP / KSP.

Step 3

Keyfactor Code Assure performs the code signing operation without the private signing keys ever leaving the HSM.

Step 4

IT security and compliance teams can audit the entire process from start to finish for complete security assurance.

Key Features

- Keyfactor Code Assure offers workflow automation and policy enforcement to ensure that only the right code is signed by the right developer with the right key—and at the right time
- Luna Cloud HSM service is a cloud-based HSM as a service that can be deployed within minutes with no need for specialized hardware or associated skills
- Luna HSMs store and protect sensitive cryptographic keys on-premises in FIPS 140-2 Level 3, tamper-resistant hardware appliances, providing high-assurance key protection within an organization's own IT infrastructure

Solution Benefits

- Enhanced protection of code signing private keys eliminates the risk of theft or misuse
- Centralized policy enforcement to ensure that only your code is signed with your certificates
- Workflows enable dispersed DevOps teams to automate code signing requests and approvals
- Complete visibility of all code signing activities for compliance and auditability
- Robust APIs allow developers to sign code remotely without requiring access to keys
- Designed as a cloud-first solution, including out of the box integration of Keyfactor Code Assure with Data Protection on Demand

About Keyfactor

Keyfactor, formerly Certified Security Solutions (CSS), is a leading provider of secure digital identity management solutions that enable organizations to confirm authenticity, and ensure the right things are interacting in the right ways in our connected world.

From an enterprise managing millions of devices and applications that affect people's lives every day, to a manufacturer aiming to ensure its product will function safely throughout its lifecycle. Keyfactor empowers global enterprises with the freedom to master every digital identity. Its clients are the most innovative brands in the industries where trust and reliability matter most.

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 number 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.