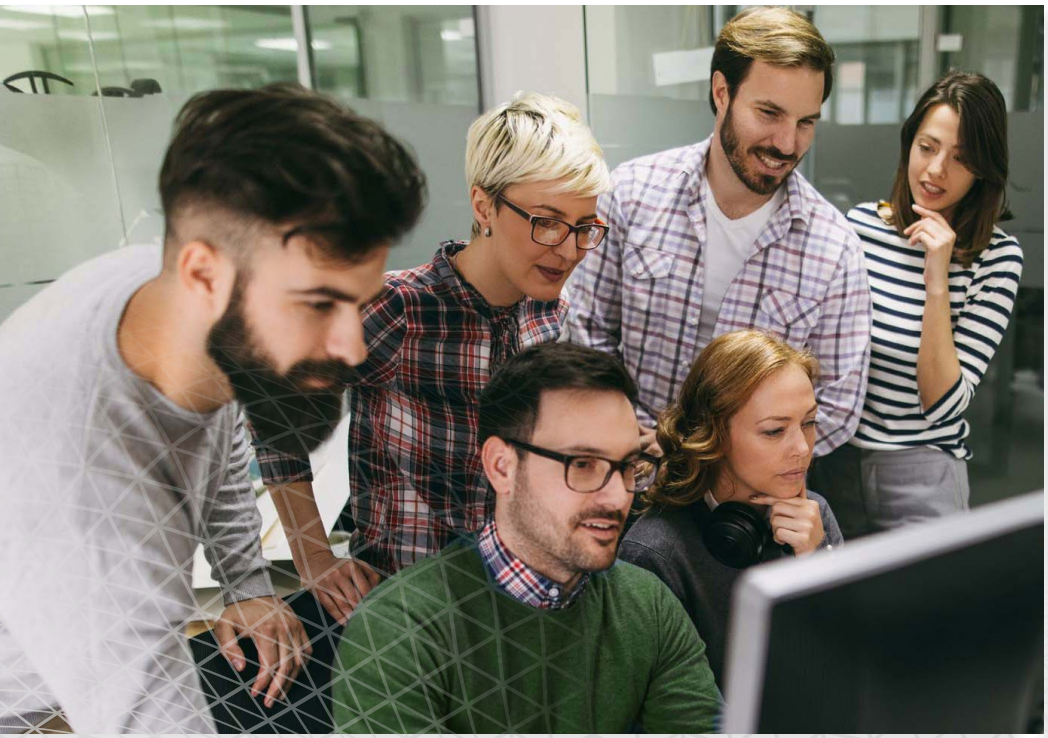
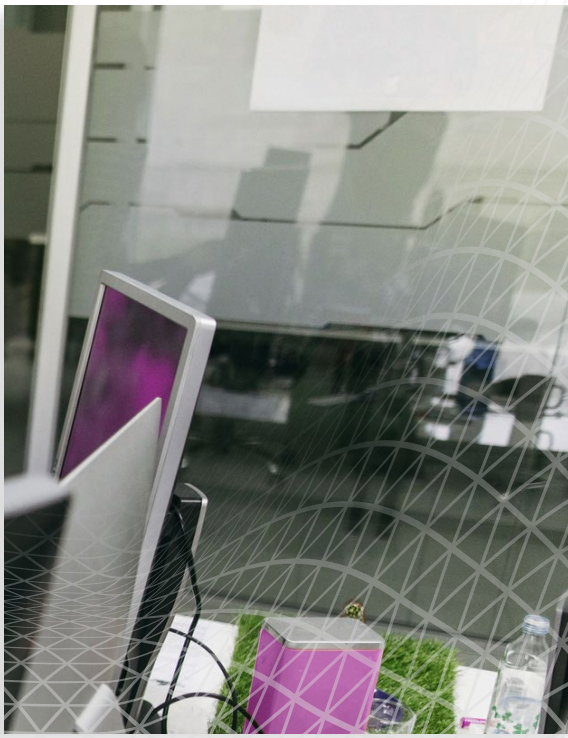
KEYFACTOR

CODE ASSURE

SECURE CODE SIGNING AT THE SPEED OF DEVOPS

- GET COMPLETE VISIBILITY & CONTROL OF CODE SIGNING OPERATIONS
- STORE ALL CODE SIGNING CERTIFICATES IN A SECURE HSM
- INTEGRATE SEAMLESSLY WITH BUILD & RELEASE WORKFLOWS





KEYFACTOR

CODE ASSURE

Overview

The demand for trust in today's uber connected digital world is unprecedented. Consumers need proof that the apps, software, and firmware they download are legitimate. This is where code signing comes in. Code signing certificates are used by developers to digitally sign software, allowing consumers to verify that your code is legitimate and can be trusted. It also means that users won't receive a warning message that could lead them to abandon installation altogether.

Most software developers and hardware manufacturers recognize the need for code signing, but the biggest challenge is how to implement it securely. The burden to protect code signing certificates is often left to developers that specialize in code, not security. Certificates and the private signing keys associated with them wind up in unsecured locations – from developer workstations to build servers, and who knows where else.

IT Security Challenges

Attackers are always changing the game and your software is their next target. IT security teams must take control and protect code signing operations to defend against these sophisticated threats.

SOFTWARE INTERCEPTION

Attackers can intercept a copy of your software and re-distribute it with malware bundled inside – turning your code into a "Trojan Horse" designed to spread malicious code without any warning signs.

KEY COMPROMISE

If the private key linked to a code signing certificate is compromised, it's game over. Stolen code signing keys are frequently sold or used to create signed malware that appears to be published by your company.

SIGNING BREACH

Hackers don't even have to steal your keys either. If build servers or developer workstations are breached, an attacker can easily submit malware to be signed as a "trusted user", often times without detection.

Dev Team Challenges

Building security into the development process often adds time and effort to release cycles, leading to tradeoffs between speed and security. Code signing and any security built around it must be fast and efficient – without disruption to the DevOps pipeline.

SPEED VS SECURITY

Balancing agile, rapid development with the demand for robust security is seriously challenging. Faster release cycles and more frequent changes to code leave no room for additional workload.

DISPERSED TEAMS

Geographically dispersed and outsourced development teams need access to signing certificates to ensure integrity in the software supply chain, but keys are often stored in vulnerable network locations.

SDLC CHANGES

Changes to the Software Development Lifecycle (SDLC) or Continuous Integration (CI) process can create more risk than they prevent. Security must adapt and integrate with fast-paced DevOps environments.

Keyfactor™ Code Assure

SECURE CODE SIGNING AT THE SPEED OF DEVOPS

Our Solution

Keyfactor Code Assure is the only platform that gives you complete visibility, control, and protection of code signing operations – without disruption to existing build and release workflows. Code signing certificates and keys are stored centrally in a tamper-resistant certified HSM. Once inside, private keys never leave the HSM. Robust APIs enable developers anywhere with quick and controlled access to code signing, while the security team retains a full audit trail of code signing activities.

FOR DEVELOPERS

Focus on writing code, not securing keys.

As a developer, you own what you build. Keyfactor Code Assure enables you to digitally sign any code, from anywhere – without the hassle of storing and securing code signing keys on your machine or re-engineering your build, test, and release workflows.

FOR SECURITY

Get complete visibility and control.

Counterfeit signed code is on the rise and your keys are the target. Keyfactor Code Assure gives you the power to secure code signing operations with end-to-end auditable controls and assured protection of private signing keys from outsider and insider attacks.

FOR EXECUTIVES

Stay out of headlines and ahead of the curve.

Recent code signing attacks underscore the importance of managing reputational risk. Whether enterprises consume software or sell it, all business leaders need to invest in the trust that is associated with their digital brand – and expect the same of their vendors.

Key Benefits

PROTECT YOUR KEYS

Store code signing keys and certificates in a centralized and secure hardware security module (HSM). Once inside the keys will remain unusable until they are unlocked for use by a designated owner.

CONTROL ACCESS

Enable developers with quick and controlled access to certificates for signing. Restrictions can be enforced to unlock certificates for a time duration, number of signatures, who can sign, and more.

ANY TEAM, ANYWHERE

Allow developers to sign code from anywhere with a unique technology that enables distributed teams to sign code remotely while keys and certificates never leave the secure confines of your HSM.

NO DISRUPTION

Secure code signing operations from end to end without making any changes to your existing SDLC or CI/CD pipeline.

END-TO-END VISIBILITY

Get a complete and actionable audit trail of who used code signing certificates, when, and who authorized the action – all from a single console.

DEPLOY ANYWHERE

Available on premise or in the cloud with the power of Thales Cloud HSM On-Demand built right into the platform. No re-engineering, no hardware – no problem.

KEYFACTOR

How It Works

Keyfactor Code Assure stores all code signing certificates from disparate network locations (i.e. developer workstations, build servers, and thumb drives) in a centralized and secure HSM. Once inside, the certificates never leave the vault. Only developers with the right access can request code to be signed, where it is then signed and returned to the user. Access controls ensure that only developers with the right privileges can sign your software and firmware.

> "The use of PKI to sign code is an increasingly important use case."[1]

FIGURE 1. KEYFACTOR CODE ASSURE | WORKFLOW

01

STEP 1

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

02

STEP 2

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

03

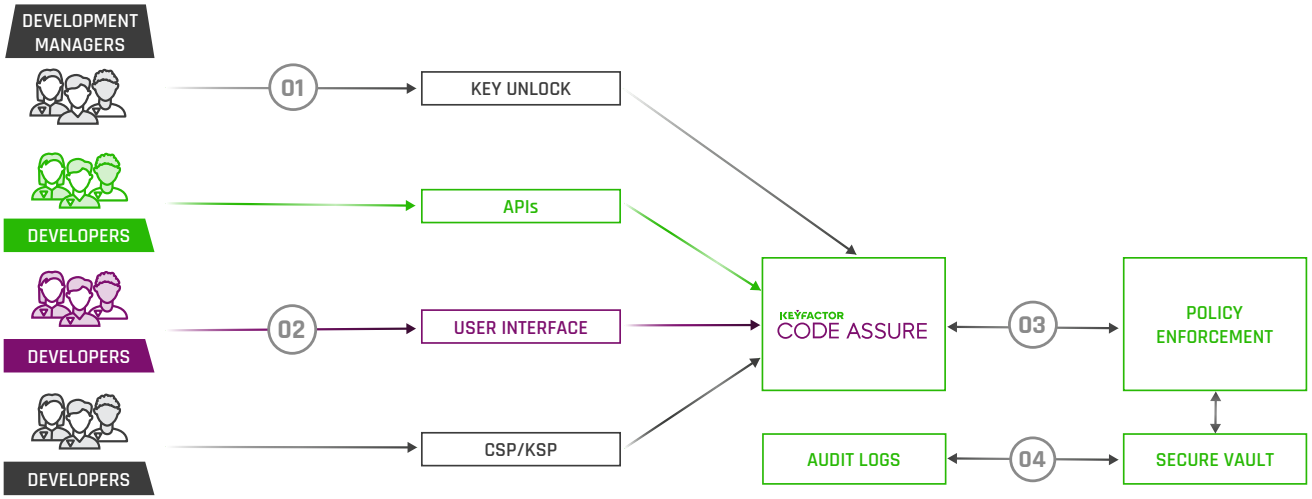
STEP 3

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

04

STEP 4

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



READY TO GET STARTED? VISIT WWW.KEYFACTOR.COM AND CONNECT WITH ONE OF OUR SECURITY SPECIALISTS. ALREADY A KEYFACTOR CLIENT? KEYFACTOR CODE ASSURE IS AVAILABLE AS A STANDALONE PLATFORM OR AS AN ADDITIONAL MODULE FOR KEYFACTOR COMMAND AND KEYFACTOR CONTROL.

Sources: 1. Solution Comparison for PKI (2019), Gartner

ABOUT

KEYFACTOR

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

CONTACT US

- www.keyfactor.com
- 216.785.2990