SECTIGO

Code Signing

Overview

Every internet transaction provides an opportunity for malicious hackers to intercept and corrupt the information passing between the two unsuspecting parties. One such attack vector is through code that is downloaded or automatically updated online. **Sectigo Code Signing** enables developers to add a layer of assurance, informing users the software they're receiving can be trusted. Utilizing certificates that allow developers to digitally sign software before distribution, Code Signing lets end users downloading digitally signed 32-bit or 64-bit programs know the code actually comes from the developer and has not been modified by a third party since it was signed.

SECTIGO

SOFTWARE LIFECYCLE

Managing Approval

Signing Operations

Maintenance

From drivers and firmware to scripts and applications, there are many file types that need code signing to show they're free of malevolent alteration. By digitally signing the executable software with a publicly trusted X.509 certificate, code developers can increase confidence in their software. If hackers do inject malicious code into a piece of software, Sectigo Code Signing will catch the infestation and alert the user prior to software installation, preventing any damage.

Not only does Sectigo Code Signing build trust with the end user, it also enables file reputation in Microsoft's SmartScreen Application Reputation filter.

Code Signing Variations

Unlike code signing products from many other vendors, Sectigo Code Signing assists you with the entire software lifecycle — from managing approval to signing operations to subsequent maintenance — delivering everything you need in one integrated solution.

Sectigo Code Signing also offers On-Demand service in two variations. With the **In-House Hosted Mode**, Sectigo runs the back end on the cloud, while the developer utilizes its in-house team to run the rest of the lifecycle. This solution is ideal for companies that are more comfortable holding and protecting their own private keys than they are using a third party.

Companies can also select the **Cloud Service Mode**, in which Sectigo runs everything at the back end, so developers can spend minimum time and attention managing their certificates.

Sectigo Code Signing is available in both **Organization Validated** — commonly referred to as "Standard Code Signing certificates" — and **Extended Validated (EV) Code Signing certificates**.

EV Code Signing certificates give developers and end users all the benefits of Standard Code Signing certificates and are additionally compatible with higher security operating system features, including Microsoft SmartScreen and Windows kernel mode.

Additionally, the EV certificate reduces the possibility that the certificate could be exported and used by an unauthorized entity by using two-factor authentication and requiring that private keys be stored on an external hardware token needed for code signing.

The Sectigo Difference

Verifying your software with Sectigo Code Signing not only builds trust in your product, but it also delivers value-added capabilities for implementing and managing your certificates. Code Signing allows you to designate and authorize which users can sign the code on behalf of your organization and to approve a second authorized entity, if required by company policy.

Additionally, in lieu of sending the entire executable file, your company can send a hash of the file to the Sectigo Cloud for signing — all that's needed is for the developer to embed the signed hash within the file. Not only does Sectigo allow for your company to generate and store the private key in an HSM for added security, you can even host the non-CA components at your premise, including local key generation.

By implementing Sectigo Code Signing, you'll increase the security of your software and build trust with your customers — all while partnering with a company that's synonymous with reliability and security.

Note: Microsoft Internet Explorer 11 or Mozilla Firefox are required to collect the certificate. Code Signing certificates cannot be generated using Apple Safari, Google Chrome, or Microsoft Edge.

About Sectigo
Trusted by enterprises globally for more than 20 years, Sectigo (formerly Comodo CA) provides web security products that help customers protect, monitor, recover, and manage their web presence and connected devices. As the largest commercial Certificate Authority, with more than 100 million SSL certificates issued across 150 countries, Sectigo has the proven performance and experience to meet the growing needs of securing today's digital landscape.