CRYPTOMATHIC
www.cryptomathic.com

Code Signing - Crypto Service Gateway

WHAT IS CODE SIGNING?

To trust the software we are using, we need assurances which attest for the integrity, authenticity and provenance of the underlying code. Companies securely sign code to provide these guarantees. Code signing is important across the technology space, both in software and hardware markets. Whether that be Windows applications, Linux Tarballs, Java JARs or Android and Apple apps in the mobile space. In hardware, manufacturers need to ensure drivers and firmware are securely signed and in the IoT space signing of firmware updates is important for securing the over-the-air (S-OTA) update process.

Securing the code-signing process and more specifically, access to the signing key is vital for providing these authenticity guarantees. If the key can be compromised or misused, then malicious actors could release code under your name/brand - causing reputational damage. The strongest method to ensure the security of key material is to use a Hardware Security Module (HSM). HSMs can, however, be difficult to manage and they expose complicated APIs. Cryptomathic's Crypto Service Gateway (CSG) is designed to simplify the management and use of HSMs and can offer a streamlined and secure code-signing service.

CODE SIGNING AND CSG

CSG is a platform for enabling multiple cryptographic services which require HSM-level security. CSG manages a pool of HSMs to ensure a resilient and available platform; together with exposing a simple to use API for consuming various cryptographic services. CSG's design makes it perfect for solving security sensitive use cases such as code signing.

Benefits of Code-Signing using CSG:

- **Endorsed Signing** – CSG provides enhanced secure workflows for the signing process.
- **Secure key management with HSMs** – Keys are held within FIPS 140-2 level 3 hardware; ensure the strictest security of all key material. Cryptomathic's solution provides a simple and complete approach for securely managing the full key lifecycle.
- **Centralized Policy Control** – CSG's policy enforcement allows security teams to rigorously control who can use keys and the specific parameter choices for all operations from a central service.
- **Logging** – CSG produces extensive tamper-evident logs for auditing purpose. These will record: who, when and what. Who used a key, when they used it and optionally can record the digest of data that was signed.

ENDORSED SIGNING

Accidental or deliberate misuse of a signing key or signing operation can have a large impact and huge reputational cost. CSG delivers a streamlined and strengthened secure system for code signing by enforcing a workflow that requires multi-party approval.

Endorsed signing is a unique CSG feature which is tailored for the code-signing market. When code signing, a vital part of the process is to ensure that that only code that has been properly approved, is signed and released. CSG's endorsed signing feature gives you the secure workflows necessary to control what code may be signed. Endorsed signing requires that a quorum m-of-n authorized 'endorsers' must endorse a code signing request before a secure signing operation is permitted.

SUPPORTED METHODS

CSG supports both RSA and ECDSA signing. Signing services are consumed either directly through the CSG's API (Java, C++, .NET and RESTful) or using a CSG extension. CSG extensions provide additional platform specific encoding and/or integration into 3rd party signtools. Extensions include a CSP for Microsoft Authenticode, JAR/APK signers and more…

Contact Cryptomathic today to let us know your code signing needs and find out how we can help.