CRYPTOMATHIC

Solution Brief

Enterprise-Grade Code Signing Platform

Powered by Cryptomathic Crypto Service Gateway (CSG)

Secure Code Signing

Code signing is important across the technology space, both in software and hardware markets. This ensures authenticity and integrity, 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 over-the-air ('FOTA') update processes.

Securing the code-signing process and, more specifically, controlling access to the signing keys is critical in providing these authenticity guarantees. If a key can be compromised or misused, then bad actors can release malicious code into your ecosystem - causing massive reputational damage. The strongest method to ensure the protection of key material is to use a Hardware Security Module (HSM). HSMs can, however, be difficult to manage, can expose complicated APIs and, by themselves, do not address all the challenges of the code signing use case.

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

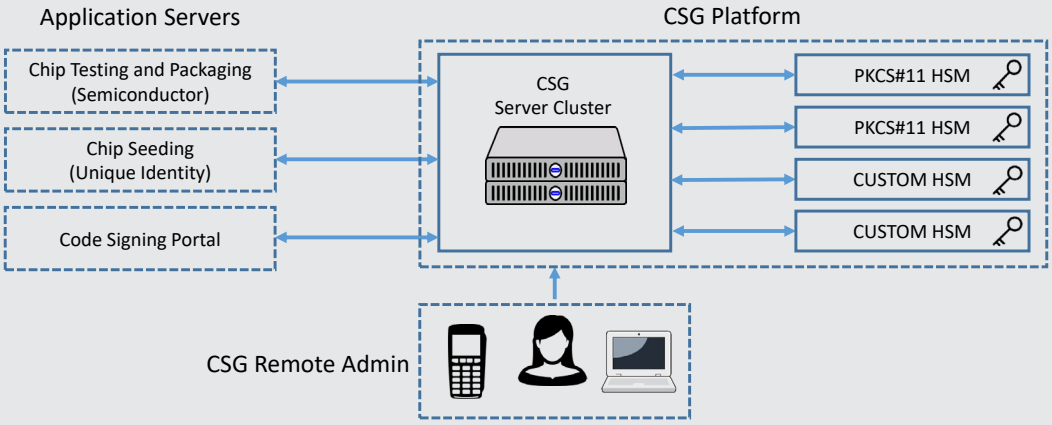
CSG is a platform for enhancing the raw cryptographic services available from HSMs. CSG creates a resilient and available service from a pool of HSMs by exposing a simple-to-use API for integrating with applications. CSG's design makes it perfect for solving security-sensitive use cases such as code signing. With CSG, a business can provide fine-grained control over its code signing operations: ensuring that critical keys are only allowed to sign code once a quorum of trusted staff have approved the process. A single CSG system can support multiple use-cases simultaneously, further increasing efficiency, cost savings and allowing confident compliance

Solution Benefits

- ✓ **Endorsed Code Signing** – CSG enables secure workflows for the signing process, involving several users for necessary approvals. Additionally, groups can be established, each with a flexible quorum of parties required to approve (Endorse) a signature request.
- ✓ **Scalable shared infrastructure** – Multiple applications can use the same platform for improved efficiency and cost savings
- ✓ **Secure key management with HSMs** – Keys are held within FIPS 140-2 level 3 hardware, ensuring the strictest security of all key material.
- ✓ **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 purposes. These record who used a key, when they used it and can record the digest of data that was signed. The parties approving the signing (endorsing the request) are also logged.

High Level Architecture

The CSG platform comprises of a CSG server cluster and shared HSMs. The CSG server cluster provides an easy-to-use code signing service for the applications and distributes load to the appropriate HSMs as well as enforces crypto policy and centralized key management. Application-specific crypto parameters are all managed centrally through an easy-to-read policy language. The policy simplifies internal and external compliance audits and empowers your security team with true crypto agility and centralized code signing capabilities.



Endorsed Code Signing with CSG

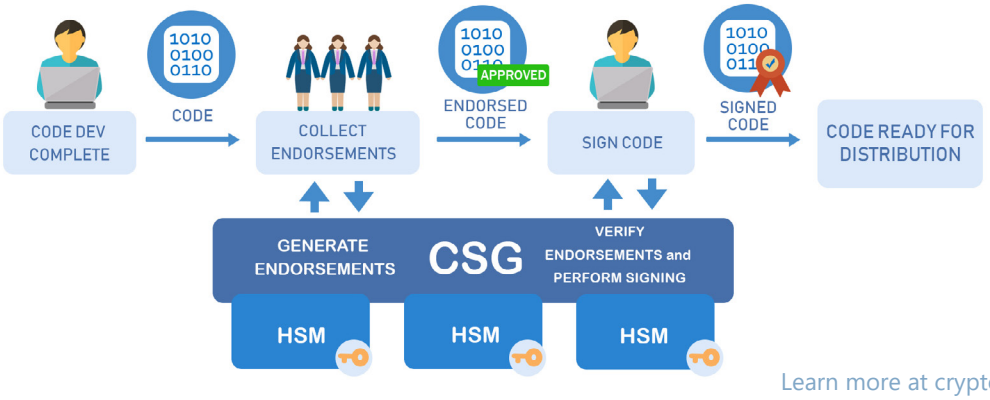
Accidental or deliberate misuse of a signing key or signing operation can have a large impact and huge reputational cost. CSG delivers a streamlined and strengthened secure system for code signing by enforcing a workflow that requires multi-party approval. Endorsed Code Signing is a unique CSG feature which is designed specifically for the challenges of code signing. A vital part of the process is to ensure that only code that has been properly approved, is signed and released. CSG's gives you the secure workflows necessary to control which code is signed. Endorsed Code Signing requires that a quorum m-of-n authorized 'endorsers' - distributed across multiple groups - must approve a code signing request before it is executed.

Endorsed Code Signing workflow

The diagram below illustrates the secure Endorsed Code Signing process.

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 and JAR/APK signers.



Learn more at cryptomathic.com/CSG

About Cryptomathic

Contact us: Sales_enquiry@Cryptomathic.com

Cryptomathic is a global provider of secure server solutions to businesses across a wide range of industry sectors, including banking, government, technology manufacturing, cloud and mobile. With over 30 years' experience, we provide systems for Authentication & Signing, EMV and Crypto & Key Management through best-of-breed security solutions and services.

We pride ourselves on strong technical expertise and unique market knowledge, with 2/3 of employees working in R&D, including an international team of security experts and a number of world-renowned cryptographers. At the leading edge of security provision within its key markets, Cryptomathic closely supports its global customer base with many multinationals as longstanding clients.

v1.0