GaraSign for Code Signing

Providing a highly secure, performant, and standardized means for companies to sign their code and data.

Garantir's remote code signing solution, GaraSign, provides the security of your data center while removing the performance bottlenecks of traditional code signing. By keeping your private key inside a centrally managed HSM and only sending the hash of the data to be signed, the optimum balance of security and performance is achieved

GaraSign code signing allows your remote and distributed teams to sign code securely and efficiently, allowing you to scale out development without sacrificing security. By reducing the bottleneck associated with traditional code signing, our solution allows you to build and deliver higher quality software more frequently to help increase your bottom line.

KEY BENEFITS

- Remote signing without direct access to signing keys
- Highly scalable
- Multiple HSN and Manager support
- Approval workflow support for high-security keys
- Centralized auditing

THE SOLUTION

GaraSign code signing realigns code signing with the needs of today. By allowing remote developers and build servers to securely and efficiently sign their code without access to the HSMs that house the private key material, this solution allows companies to scale our their distributed and/or outsourced development efforts without sacrificing security

HOW IT WORKS

A hardened web service sits in front of the hardware security modules (HSMs) that store your private keys. The authenticated remote signing clients (i.e., your remote developers and build servers) then send the hash of the data they need to sign to the web service which, in turn, signs the data and returns the signature back to the remote client if all security checks pass. This solution is designed to be transparent to today's current signing technologies to integrate directly with your current environment.

SOLUTION INTEGRATIONS

- Developed on an open REST API, allowing for custom integrations and requirement
- Integrates with existing code signing tools and standards
- Backend infrastructure integrates with HSMs, key managers, and software-based key stores simultaneously

Current Integrations and signature formats include:

- macOS (codesign, productsign, etc.)
- Windows (signtool, strong name, etc.)
- GPG/PGP
- Java (jarsigner, apksigner)
- Repository packages (RPM, NPM, Debian)
- Documents (PDF, Microsoft Office)
- PKCS#7 (Cryptographic Message Syntax)
- PKCS#11

Upcoming Integrations:

- Docker Images