1041 Market Street #302

San Diego, CA 92101

(858) 751 - 4865

info@garantir.io

Garantir

Accelerating Cryptographic Operations

With HSM-Secured Keys

Garantir GaraSign Datasheet

GaraSign enables fast and secure remote digital signatures for code signing, SSH, S/MIME, TLS, and more, while the signing keys remain secured in HSMs.

Securing & Managing Access To Private Keys Is Critical

Public key cryptography can be found everywhere in enterprises today. It secures data in transit (TLS), authenticates users to remote servers (SSH & VPN), protects data at rest (TDE), ensures the authenticity of software (code signing), safeguards email (S/MIME and PGP), and more.

Consequently, it's vital to maximize the security of private keys without limiting access to them or inhibiting the performance of business processes.

GaraSign is the solution that provides this balance. It's a platform for cryptographic operations that combines superior security with unparalleled performance.

Maximum Security Without Compromising Performance

Hardware security modules (HSMs) offer excellent security for private keys but they often come with few native client integrations and expose limited interfaces with which to build custom integrations. Poorly-designed integrations often cause performance bottlenecks, making it seem as though speed is being sacrificed for the sake of security.

GaraSign comes with a multitude of native client integrations so it fits directly into any environment. With GaraSign, you get all of the security of your HSMs without limiting the performance of cryptographic operations, like code signing, SSH, TLS, S/MIME, and document signing.

Key Benefits Of GaraSign

• **Strong Security** – private keys never leave the hardware security module (HSM)

• **High Performance** – client-side hashing results in very fast throughput

• **Reporting and audit** features for full visibility on all private key access and usage

• Delivers proven **regulatory compliance**, reliability, and ease of use

• **Highly Scalable** – all nodes are horizontally and vertically scalable

• **Easy to Manage** – keys are centrally managed and the GaraSign administrative interface gives you insight into all activity in the system

• **Easy to Use** – client integrations ensure that you can continue using the same native tools you use today

• **Multiple HSM Support** – GaraSign supports many different HSMs and key managers and can be used with multiple simultaneously

• **Cloud Capable** – GaraSign can be deployed on-premises, in the cloud, or in a hybrid environment

Garantir GaraSign Datasheet
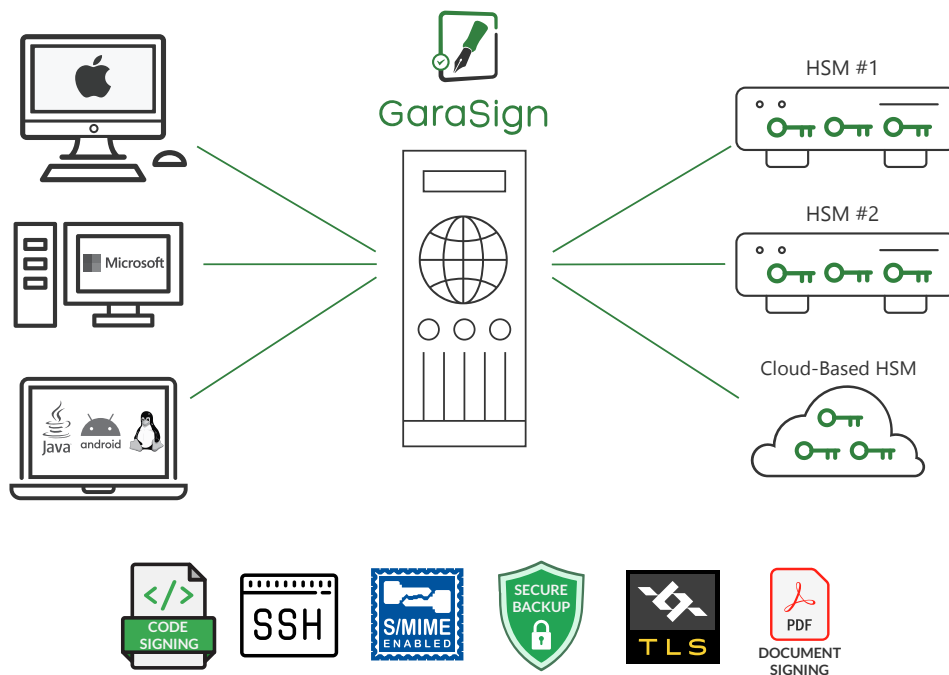
Proxied Private Key Access

GaraSign is deployed on customer-managed infrastructure between your HSMs and the cryptographic clients, restricting those clients to proxied key access. The result is that private keys remain secured in HSMs at all times, while end-users can still gain access to the keys they need to perform cryptographic operations.

Client-Side Hash Signing

GaraSign is built with a client-side hashing architecture. Signing clients hash the data they need to sign before sending it over the network to create the signature. GaraSign receives the hash from the authenticated and authorized client, offloads the signing operation to the HSM, and returns the resulting digital signature to the client. This hash signing architecture limits the amount of data transmitted over the network, so digital signature processes like code signing, SSH, document signing, and more, all remain fast and efficient.

Strong Security Features

Since signing clients are restricted to proxied key access, GaraSign can integrate into existing processes to provide additional advanced security features: multi-factor authentication, device authentication, approval workflows, IP address whitelisting, notifications, and more. Additional security features can be customized for each private key stored in the HSM.
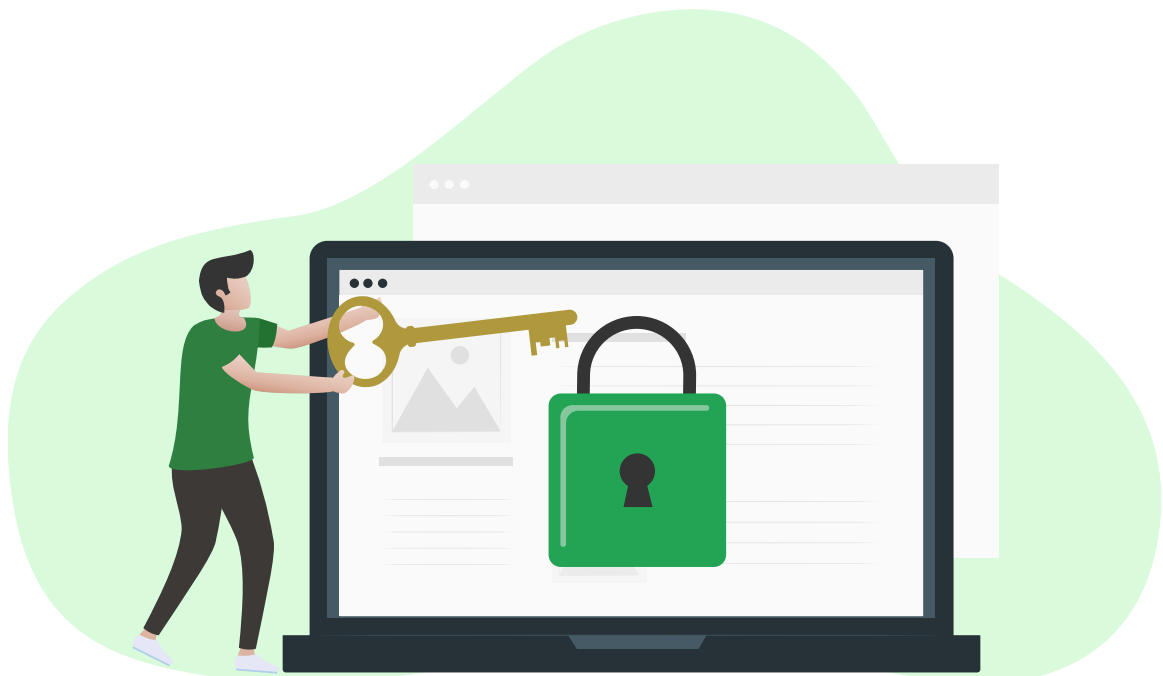
Native Client Integrations

GaraSign comes with a host of integrations:

Garantir

Garantir is a cybersecurity company that provides advanced cryptographic solutions to the enterprise. The Garantir team has worked on the security needs of businesses of all sizes, from startups to Fortune 500 companies. At the core of Garantir's philosophy is the belief that securing business infrastructure and data should not hinder performance or interrupt day-to-day operations. With GaraSign, Garantir's flagship product, private keys remain secured at all times, without limiting the performance of cryptographic operations, including code signing, SSH, S/MIME, document signing, TLS, secure backup, and more.

Garantir