Garantir and Entrust deliver secure digital signature solution for the enterprise

GaraSign enables customers to stand-up scalable signing systems with an nShield HSM root of trust

HIGHLIGHTS

- Protect sensitive cryptographic keys throughout entire lifecycle

- Integrate nShield® hardware security module (HSM) root of trust

- Allow clients to hash their data prior to sending it over network

- Deliver high speed required for performance-sensitive systems

- Integrate with Active Directory, log management and notification systems

- Support wide set of clients for quick integration into workflows

Balancing security and performance for an enterprise-wide digital signature platform is hard

Now more than ever, companies are making heavy use of public key cryptography to meet the growing demands of the tech industry. Unfortunately, the tools provided by the industry haven't scaled well and companies have had to choose between security and performance. What companies need is a way to achieve the performance delivered by local keys with the security and scalability of centralized key management, backed by an HSM root of trust.
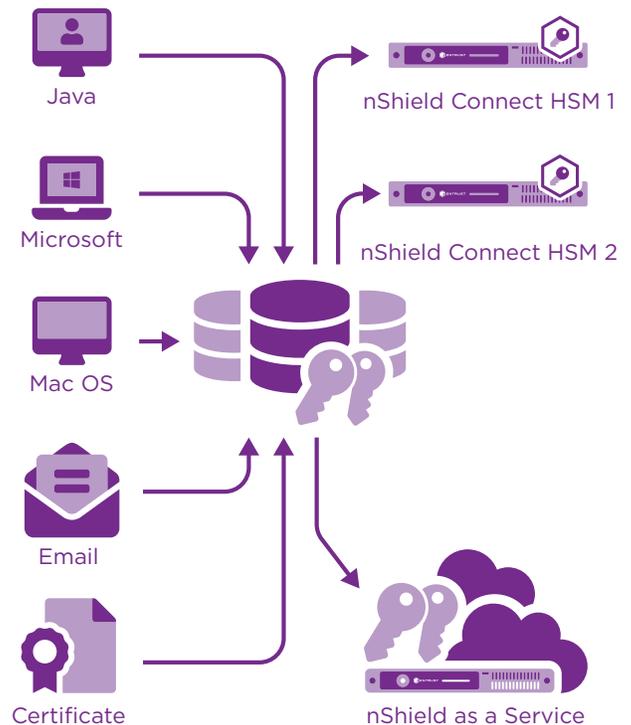
nShield HSMs, on-premises or as a service (nSaaS), protect the cryptographic keys used by GaraSign enterprise signing system to deliver digital signatures.

LEARN MORE AT ENTRUST.COM/HSM

Garantir and Entrust deliver secure digital signature solution for the enterprise

Fast, secure and scalable digital signatures with garasign

GaraSign, Garantir's digital signature platform, balances the security and performance of digital signatures across the enterprise. The solution allows clients to hash data client-side, before sending over the network for signing. Using this approach, the data sent over the network is minimal which allows for sub-second signatures without exposing sensitive private keys.

Developed on an open REST API, GaraSign allows for custom integrations. On the client side, GaraSign integrates with existing signing tools and email clients while supporting HSMs, key managers, and software-based key stores simultaneously on the backend.

GaraSign integrates with Entrust nShield Connect HSMs and nSaaS to protect and manage the private signing keys used to sign their hashed data.

Why use Entrust nShield HSMs with GaraSign?

Encryption and signing keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise of critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic key material. nShield Connect HSMs and nSaaS integrate with GaraSign to provide comprehensive logical and physical protection of the private keys used for enterprise-wide code signing, SSH, S/MIME, and TLS deployments.

nShield HSMs enable GaraSign customers to:

- Secure keys within carefully designed cryptographic boundaries that use robust access control mechanisms, so keys are only used for their authorized purpose

- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed by GaraSign's signing and administration servers

- Deliver superior performance to support time-sensitive signing applications

Garantir

Garantir is a leading provider of high performing and secure enterprise digital signature platforms - GaraSign. By seamlessly integrating into customers' existing environments, GaraSign enables easily signing of code, emails, documents, and data - while keeping the signing keys securely locked away in an nShield HSM root of trust.

www.garantir.io

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations.

Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com