Solution Brief

Fast, Secure, and Scalable Digital Signatures with Garantir and Thales

HSM-Backed Digital Signatures for Code Signing, SSH, S/MIME, and more...

cpl.thalesgroup.com

THALES
Building a future we can all trust

Garantir

THALES
Building a future we can all trust

Garantir

Balancing Security and Performance

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 – storing the keys in an HSM - and performance – distributing the keys out to end users. It is common for enterprises to distribute SSH and S/MIME keys to the various computers in their network, leaving those keys exposed and tough to manage. Those same companies often require their developers and build teams to upload their code and binaries to a central server that has access to the corporate HSM for code signing, leading to a performance bottleneck for CI/CD servers. What companies need is a way to achieve the performance of local keys with the security and scalability of centralized key management backed by a hardware security modules (HSMs).

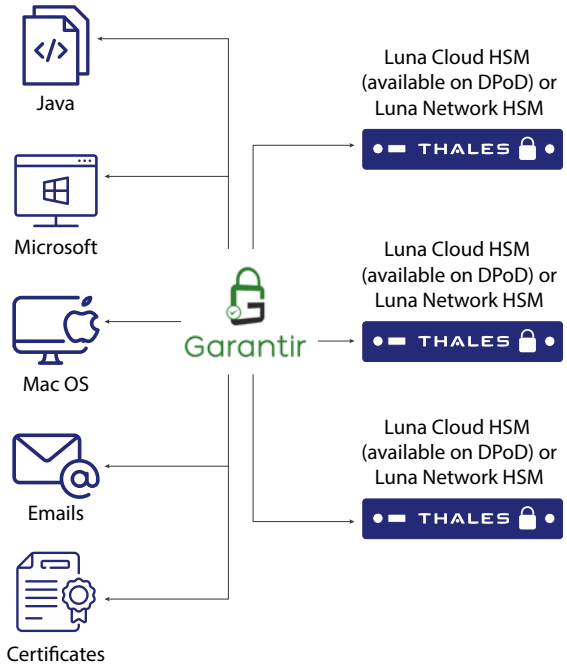
Fast, Secure, and Scalable Digital Signatures with Garantir and Thales

Garantir's cryptographic services platform addresses these issues by allowing clients to hash the data client-side before sending the data over the network to be signed by the keys in the HSM. Using this approach, the data sent over the network is minimal which allows for sub-second signatures without exposing the sensitive private key material.

Benefits of Garantir with Luna HSMs

- **Strong security** – keys never leave the HSM
- **Reporting and audit** features for easier adherence to compliance regulations
- Delivers proven **compliance**, reliability and ease of use
- **High performance** – client-side hashing results in very fast throughput
- **Scalable** – all nodes are horizontally and vertically scalable
- **Easy to manage** – keys are centrally managed and the Garantir administrative interface gives you insight into all activity in the system
- **Easy to use** – a multitude of client integrations ensures that you can continue using the same tools, platforms, and operating systems you use today
- **Cloud capable** – Garantir and Luna HSMs can be deployed on-premises, in the cloud, or in a hybrid environment
- **Enterprise ready** – Garantir integrates with all your enterprise features including Active Directory, log management platforms, notification systems, and more

- **Quantum-Safe** - Luna HSMs native support for PQC algorithms ensures long-term protection against emerging quantum threats, including Harvest-Now, Decrypt-Later (HNDL) attacks



- **Largest set of client integrations –** Garantir comes with the largest set of client integrations including, but not limited to:
  - Windows
  - Java/Android
  - macOS
  - RPM
  - GPG
  - Debian
  - OpenSSL
  - PKCS#11
  - NPM
  - ... and more

Garantir & Thales Luna HSMs

Combining Garantir's platform with the industry's most trusted brand of HSM is a natural integration. When backed with a Thales Luna HSMs or Data Protection on Demand (DPoD) Luna Cloud HSM services, Garantir provides unrivaled key protection, performance, and scalability. Garantir also enables customers to transparently deploy advanced security features, such as multi-factor authentication, device authentication, approval workflows, IP address whitelisting, notifications, and more.

Thales offers two solutions that maintain Root of Trust private key protection for Garantir's platform. Luna HSMs provide companies 140-3 Level 3 and FIPS 140-2 Level 3 compliance with the option of maintaining root of trust protection and management of encryption keys across cloud-based, hybrid/multi-cloud, on-premises, or a mixture of deployments. This flexibility makes it easier to deploy a solution to address ever-changing compliance mandates and budgetary requirements.

- **Luna Cloud HSMs** (available as a service on Thales Data Protection on Demand), provides a cloud-based HSM service that offers key management capabilities that can be deployed within minutes with no need for specialized hardware or associated skills.
- **Luna HSMs** store, protect, and manage sensitive cryptographic keys in a tamper resistant on-premises Luna HSM, providing high-assurance hardware key protection and key ownership within an organization's own IT infrastructure. Luna HSMs are FIPS 140-3 Level 3 validated and Common Criteria EAL 4+ certified to meet the strict compliance and regulation requirements such as GDPR and eIDAS.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted organizations protect critical applications, data, identities, and software anywhere, at scale. Through Thales' integrated platforms, customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

About 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 Garantir's platform, 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.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us