Ascertia products and Thales Luna HSMs deliver the ultimate high-trust PKI and Digital Signing solutions

How can organisations conduct digital business securely in order to meet internal, compliance and audit requirements?

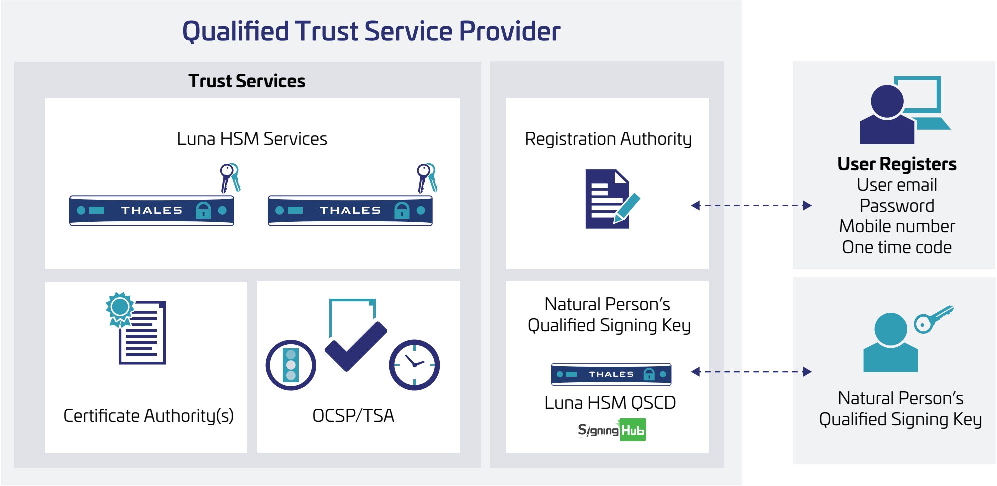
Governments, Enterprises and Trust Service Providers (TSPs) need to ensure document and data integrity with clear authenticity and traceability, in order to conduct secure digital business and meet compliance and audit needs. Public Key Infrastructure (PKI) technology provides the required trust services for protecting businesses with strong identity and authentication. Additionally, PKI also drives efficiencies through the use of digital signatures, removing the need for paper and speeding up the sign-off process. An intuitive user experience, across devices and applications, is critical to give users confidence and trust.

Ascertia's SigningHub provides a powerful e-Signature platform, which utilises the PKI trust services from Ascertia's ADSS Server to provide the ultimate high-trust solution. Designed with flexibility and interoperability in mind, Ascertia products can use existing national and international PKI schemes and other high trust certificates. Customers benefit from a foundation of digital trust through the use of Thales Luna Hardware Security Modules (HSMs), providing the required root of trust security for private signing keys.

SigningHub also supports legally enforceable electronic signatures that comply with key global standards and regulations, such as EU eIDAS, ETSI, SEN, NIS, and Adobe CSC, and provides high levels of interoperability via the Cloud Signature Consortium (CSC) API, which enables high-trust remote signing. Users of SigningHub can also benefit from greater control of the Level of Assurance (LoA) that is required from document signers, be it an EU Qualified Signature or a Basic e-Signature.

Key benefits for Trust Service Providers:

- High-trust and new rule compliant solutions for Advanced and Qualified Remote Electronic Signatures
- Advanced document workflow for facilitating secure digital signature approval
- Global interoperability – easy to use, integrate and configure across a range of business applications
- Authentication, traceability, accountability, data integrity, secure archiving
- Ultimate choice of device agnostic deployment options delivered through our expert partner network – on-premises, public cloud, hybrid or private enterprise cloud



Ascertia SigningHub & ADSS Server

SigningHub is a high-trust e-Signature platform which delivers a complete signing solution, enabling organisations to create seamless workflows for digital signature approval. Whether integrated into core business applications or used as a standalone solution, SigningHub optimises how people review, approve and sign documents on any device, and allows businesses to safely migrate paper-intensive processes to the digital world.

ADSS Server is the cryptographic engine that provides key PKI trust services and powers Ascertia's SigningHub solution. Easy to deploy and offering a full range of PKI services, ADSS Server offers modules for advanced or qualified digital signature creation and verification, together with options for Timestamping (TSA), Certificate Validation (OCSP, SCVP, XKMS), Long-term Archiving (LTANS) as well as Certificate (CA) and Registration (RA) services.

The use of a standards-based approach, high-trust solutions, and a focus on long-term verification, enable these products to deliver the essential trust services required by public and private organisations to conduct electronic business securely and seamlessly.

The world is digitising and as a global leader in high-trust PKI and digital signature products, Ascertia plays a crucial role in delivering this transformation.

Why use Luna HSMs with Ascertia Solutions?

Ascertia provides the broadest range of PKI and digital signature technology in the world, which is used by governments, enterprises and trust service providers to deliver essential digital trust services to facilitate digital business. With the goal of keeping global business flowing, providing assurance, authenticity and protection of business data and documents, Thales is closely aligned with Ascertia and together they already offer high-trust solutions that have been deployed around the world through Ascertia's expert partner network. Encryption or private signing keys handled outside the cryptographic boundary of a certified Luna HSM are significantly more vulnerable to attack, which can lead to compromise and misuse of critical keys. Luna HSMs are the only proven and auditable way to secure valuable cryptographic material. Luna HSMs integrate with Ascertia's products to provide comprehensive logical and physical protection of keys for Certification Authorities, OCSP Validation Servers, Time Stamp Authorities and Digital Signature Services.

In addition, Luna HSMs provide Ascertia's ADSS Server with centralized HSM Services for remote authorised digital signing services (RAS), which removes the requirement for local smartcards and card readers and enables high-trust remote signing, on any device, at any time, from anywhere. Luna HSMs enable Ascertia customers to:

- **Generate secure keys**, which are stored in a tightly controlled, **FIPS 140-2 and CC EAL4+** certified environment that uses robust access control mechanisms, so keys are only used for their authorised purpose
- **Ensure key availability** by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed by the CA, OCSP Validation Service and Digital Signature Services
- **Deliver superior performance** to support demanding applications

Thales Luna HSM – Root of Trust

Luna HSMs provide the foundation of digital trust for your cryptographic system, securing your data, identities and transactions with strong authentication and role separation, and a keys-in-hardware approach. This means you are protected without compromising agility, usability or scalability so that you can meet the high demands of industry regulations and audit requirements, in addition to achieving your business and revenue goals. Luna HSMs are purpose built to address the security and operational needs required to maintain the integrity of PKIs, including:

- **Secure Ascertia ADSS Server private keys** responsible for the SSL/TLS handshake to establish the HTTPS session, and provide secure key storage for ADSS business applications and audit logs, and remote signing
- **True hardware-based key management** - ensure your critical encryption keys and digital identities are always secure and always know their whereabouts by performing all key generation, and key operations including digital signing exclusively within the hardware root of trust by default

- **Store keys off-board without any limit and granular control of key material** by per-key based authorization, for use cases including remote singing and sealing
- Benefit from **end-to-end security and encryption**, and comply with the standards by protecting your private signing keys in **FIPS 140-2 Level 3 certified and Common Criteria EAL4+** (PP 419211-5) validated hardware, securely storing identities used for PKI, digital signing and timestamping
- **Establish trust and integrity** for your data with a **strong security architecture** including side channel attack protection; audit logging; trusted path MofN authentication; multi-factor authentication; crypto agility; and separating your HSM into up to 100 partitions each acting as a unique virtual HSM to secure additional applications and extend your return on investment
- **Secure Backup** - direct hardware-to-hardware backup for disaster recovery
- **Easily install provision and manage Luna HSMs and meet the SLAs** of demanding high transaction volume applications with scalable, high throughput performance, reducing downtime and streamlining operations

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organisations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

About Ascertia

Founded in 2001, Ascertia is a global leader in high-trust PKI and Digital Signature products for digital signature creation, verification, timestamping and secure archiving as well as full PKI solutions to support Qualified Remote Signing, CSC and ePassport use cases. Ascertia's products are easy to integrate, configure and use across a wide range of business scenarios. Public and Private sector organisations use Ascertia technology to deliver the essential trust services that keep citizens secure and business flowing.

For more information please visit www.ascertia.com