Solution Brief

Ascertia and Thales offer the Ultimate High-Trust PKI and Digital Signature Solutions

Helping organisations conduct digital business securely to meet internal, compliance and audit requirements

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Key Benefits

- Compliant with eIDAS regulations and Cloud Signature Consortium (CSC), which is a global association committed to driving standardization and interoperability of highly secure, compliant cloud-based signature
- Highly certified - FIPS 140-3 Level 3 validated and Common Criteria EAL 4+ Certified
- Advanced document workflow for facilitating secure digital signature approval
- Strong non-repudiation - including traceability and audit trails
- Global interoperability makes it easy to use, integrate and configure across a range of business applications
- Ultimate choice of device agnostic deployment options delivered through our expert partner network - on-premises, public cloud, hybrid or private enterprise cloud

The Challenge

As organisations continue to transform digitally, they are moving away from traditional signing methods. Digital signatures confirm the authenticity and integrity of digital documents, serving as the equivalent of a handwritten signature or stamped seal. This shift accelerates business processes, reduces operational costs, and ensures compliance with regulations, but also presents certain challenges.

With this move towards digital signing comes the importance of protecting digital signatures from compromise. Secure storage and protection of private keys is integral to the security of the Asymmetric Key Cryptography used in Public Key Infrastructures (PKIs). This requires mechanisms to secure the cryptographic keys at the heart of the digital signature itself. PKIs are relied upon to secure digital applications, but organisations can't rely on PKIs alone to safeguard digital applications.

Digital signatures get their official status through signing certificates, which authenticate digital documents, content, and owners. A

Certificate Authority (CA) is the core component of a PKI and establishes a hierarchical chain of trust, verifying organizations' compliance with standards. If a CA's root key is compromised, the credibility of financial transactions, business processes, and intricate access control systems is adversely affected.

Together, Thales and Ascertia enhance signer authenticity and ensure data integrity in digital signing, promoting accelerated digital transformation, compliance with regulatory requirements and increased security.

Ascertia Digital Trust Products

Ascertia offers robust cryptographic algorithms and secure key management to ensure the integrity and authenticity of electronic signatures. PKI technology provides the required trust services for protecting businesses with strong identity and authentication. PKIs also drive efficiencies through digital signatures, removing the need for paper and speeding up the sign-off process.

Ascertia's digital trust products and services focus on delivering complete electronic signature solutions, PKI trust services and digital identity registration management. Ascertia's core products, SigningHub, ADSS PKI Server and ADSS SAM Appliance, are used by governments, enterprises, and trust service providers (TSP) to provide essential digital trust services to conduct global business securely and seamlessly.

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 optimizes how people review, approve and sign documents on any device, and allows businesses to safely migrate paper-intensive processes to the digital world.

ADSS PKI Server is the cryptographic engine that provides key PKI trust services. Certificates issued by ADSS Server based Certification Authorities enable users to sign documents digitally using in Ascertia's SigningHub solution. Easy to deploy and 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.

ADSS SAM Appliance is a Common Criteria Certified Remote Qualified Signature Creation Device (RQSCD) that enables TSP to deliver qualified digital signature services for natural persons, legal representatives, timestamps, and eSeals for any document, web form, or transactions. The SAM Appliance can be shipped with an internal EN419221-5 certified Hardware Security Module (HSM) OR used with a suitable external network connected HSM like the Thales Luna Network Hardware Security Model (HSM) to authorize the signing or sealing keys securely.

The use of a standards-based approach, high-trust solutions, and a focus on long-term verification enables these products to deliver the essential trust services required by public and private organizations to conduct electronic business securely and seamlessly. The world is digitizing, and as a global leader in high-trust PKI and digital signature products, Ascertia plays a crucial role in delivering this transformation.

Root of Trust Thales Luna HSMs

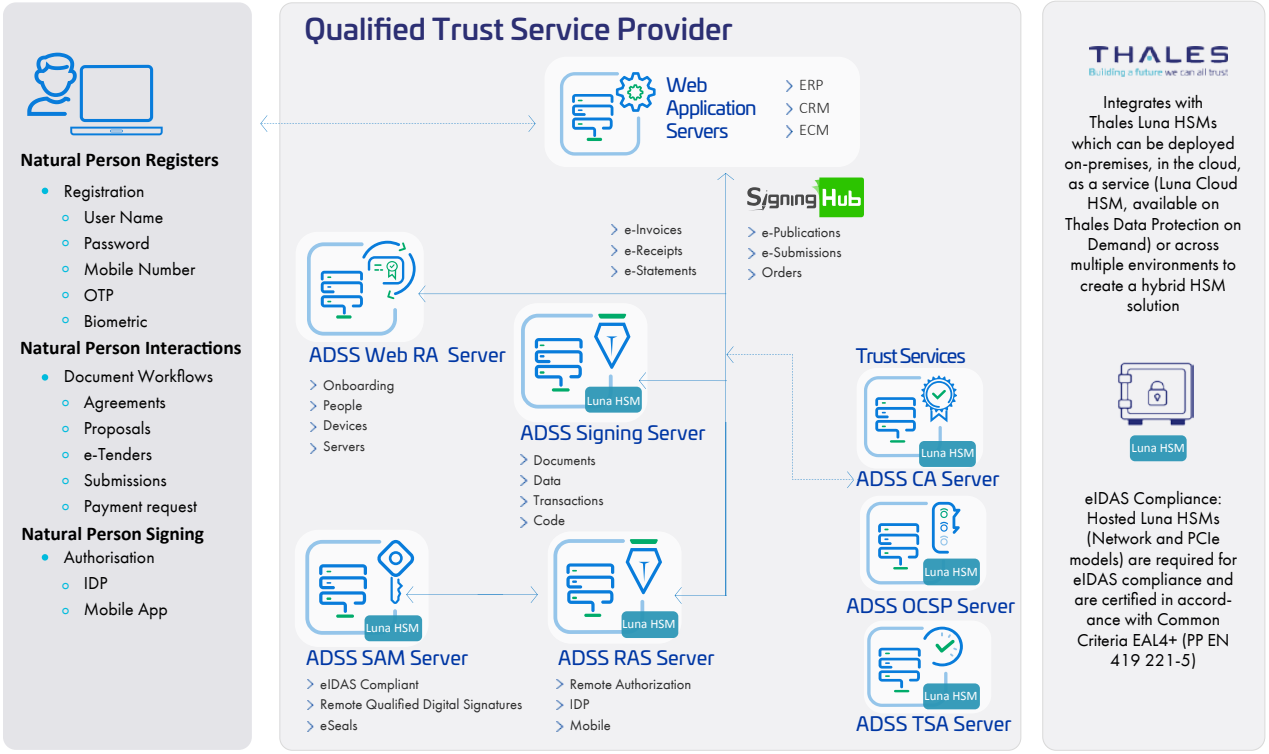
Thales Luna HSMs provide the foundation of digital trust for cryptographic systems, securing data, identities, and transactions with strong authentication, role separation, and a keys-in-hardware approach. Organizations are protected without compromising agility, usability, or scalability to meet the high demands of industry regulations and audit requirements, in addition to achieving business and revenue goals.

Thales is closely aligned with Ascertia, offering high-trust security solutions deployed worldwide through Ascertia's expert partner network. Ascertia SigningHub provides a powerful e-signature platform that utilises PKI trust services from Ascertia's ADSS PKI Server, which provides the ultimate high-trust solution. Customers benefit from a foundation of digital trust through Thales Luna HSMs, providing the required root of trust security for private signing keys. Encryption or private signing keys handled outside the cryptographic boundary of HSMs are significantly more vulnerable to attack, which can lead to compromise and misuse of critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic material. In addition, Luna HSMs provide Ascertia's ADSS PKI 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.

Thales Luna HSMs are purpose-built to address the security and operational needs required to maintain the integrity and protection of private keys associated with PKI digital signatures, including:

- Securing 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
- Ensuring critical encryption keys and digital identities are always secure and always know their whereabouts by performing all key generation and operations, including digital signing exclusively within the hardware root of trust
- Storing 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
- End-to-end security, encryption, and compliance with the standards by protecting private signing keys in FIPS 140-3 Level 3 certified, Common Criteria EAL4+ (PP 419211-5) validated hardware, and eIDAS certified as both a Qualified Signature and Qualified eSeal Creation Device (QSCD)
- Establishing trust and integrity for data with strong security architecture, including side-channel attack protection, audit logging, trusted path MofN authentication, multi-factor authentication, crypto agility, and separating HSM into up to 100 partitions
- Easy installation, provisioning, and managing of the HSM to run workloads with flexibility and at scale

Ascertia Digital Trust Products + Thales Luna HSM



In Conclusion

Thales and Ascertia work together to guarantee essential digital trust products and services that deliver complete digital signature solutions. Ascertia's core products, SigningHub, ADSS PKI Server and ADSS SAM Appliance, in combination with Thales Luna HSMs, enable the strongest utilisation of digital signatures and deliver the essential trust services and certifications required by public and private organisations to conduct global business.

About Ascertia

Ascertia delivers digital trust products and services globally for Enterprises, Governments and Trust Service Providers. Ascertia solutions enable digital business processes which are fundamentally underpinned by digital trust to ensure that digital identities are proven, and business transactions are trustworthy. Ascertia's digital signature platform and PKI products deliver digital trust across people, devices, data, and documents. At the heart of Ascertia's digital trust ecosystem is a wide-reaching customer base, 100+ expert partners and integrators which have been delivering Ascertia products, cloud services and apps since 2001.

Ascertia became part of the InfoCert – Tinexta Group in 2023. InfoCert is the largest Qualified Trust Service Provider in Europe. They build sustainable and innovative digitisation solutions tailored to meet the unique needs of clients from different industries. InfoCert's commitment extends to upholding the highest standards of security and compliance, delivering a user-friendly experience, and ensuring complete legal validity.

For more information please visit www.ascertia.com.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

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