ADSS Server SAM Appliance

EN 419 241 Compliant Remote Authorised Signatures

ADSS Server SAM Appliance is a high performance 1U hardware appliance that meets FIPS 140-2 Level 3 and is Common Criteria EAL4+ Certified against the eIDAS standard EN 419 241-2 Protection Profile with high-trust Sole Control Assurance Level 2 (SCAL2). It can meet the most demanding needs by providing high throughput and high availability for delivering remote authorised natural person Qualified eSignatures or corporate Qualified eSeals.

Digital Signatures Overview

Signatures are typically used to provide a means for individuals to agree contracts and authorise transactions. Digital Signatures identify the person who signed and are legally enforceable in courts of law in various jurisdictions. In the paper world there are problems with document security and traditional ink signatures, (a) signatures can be forged and (b) the contents of a document can be altered after the signature has been applied. As a result, a signer can also falsely deny having signed a document.

In the digital world, digital signatures offer far more security by proving who signed, when the signature took place and that the document has not changed by a single bit. Digital signatures are used to secure documents, transactions, emails, software applications etc. Signatures can be short lived or last for months, years (or even multiple decades using special archiving approaches).

In Europe, eIDAS defines Qualified eSignatures and Qualified eSeals as having the highest level of trust to enable natural persons and legal entities to sign or seal to ensure authenticity, data integrity and non-repudiation.

EU eIDAS leads the world in how high-trust signatures services must be offered from a technical, physical, logical and procedural perspective. Standards from ETSI, CEN, IETF and ISO define how digital signatures must be created to ensure security, interoperability and longevity.

In the past smartcards have been a dominant form of providing appropriate high-trust security for user and corporate signing keys. eIDAS has defined a new set of standards to allow centrally managed remote signing and sealing services which offer far better user experience with the ability to sign from any device and location and whilst maintaining the highest levels of trust. Ascertia was the first company in the world to deliver a CC EAL4+ certified EN 419 241-2 product with ADSS Server SAM Appliance v6.0 and has now released its next generation appliance.

Key Features

- **Certifications:**
  - Common Criteria EAL4+ EN 419 241-2
- **Standards Compliance:**
  Meets the requirements for:
  - FIPS 140-2 Level 3 Compliant Appliance
  - EN 419 241-1 & 2
  - EN 419 221-5
  - TS 119 431-1
  - TS 119 431-2
  - TS 119 432
  - Cloud Signature Consortium (CSC)
- **Cryptography Support**: Supports strong signing & hash algorithms:
  - RSA 2048, 3072, 4096, 8192
  - ECDSA 256, 384, 521
  - SHA-256, SHA-384, SHA-512 & others
- **Supports Sole Control Assurance**
  - Level 1 & 2
- **Remote Authorisation Support**
  - Touch ID
  - Face ID
  - Passcode
  - SAML Identity Providers
  - OIDC Identity Providers
- **High-Availability**: ADSS Server SAM Appliance is well proven at offering high throughput, high availability and scales to meet demanding business needs.

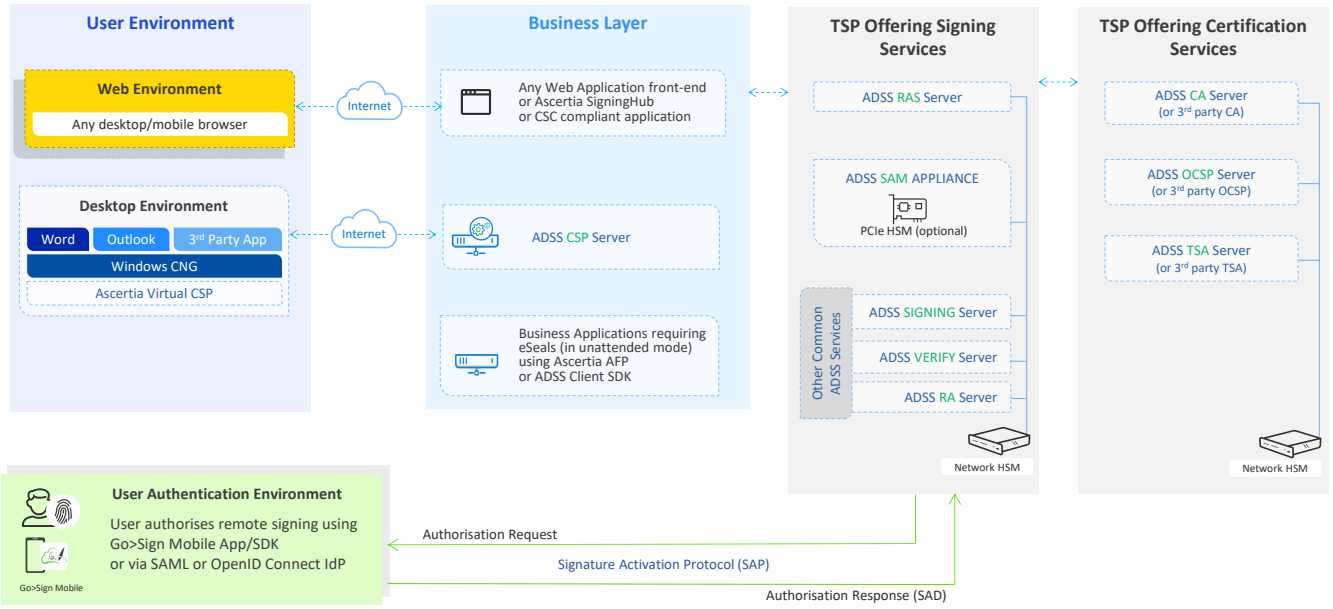
ADSS Server SAM Appliance Remote Authorised Signature Architecture

Qualified Remote signing is where a natural person signs a document by using the online services of a Qualified Trust Service Provider (QTSP) who is responsible for managing the signing key on behalf of the owner. The QTSP's responsibilities include ensuring that signing keys remain under the sole control of the owner with a high degree of confidence. Remote signing is sometimes referred to as server-side signing or more generally as cloud signing.

A similar signing approach can also be employed for legal entity signing, referred to in eIDAS as eSeals. Remote eSeals are where the QTSP remotely manages the e-seal keys on behalf a legal entity. These eSeals can also be at two levels of assurance i.e. Sole Control Assurance Level (SCAL) 1 and 2. Qualified eSeals require the solution to use SCAL2.

Designed to meet the needs of Qualified Trust Service Providers (QTSPs), Ascertia ADSS Server SAM Appliance meets the EU eIDAS requirements for remote signatures as defined in EN 419 241 Part 1 and Part 2. Together with Ascertia's SigningHub and ADSS Server products, QTSPs are able to provide fully hosted remote signing services or hybrid solutions. ADSS Server SAM Appliance is delivered within a FIPS 140-2 Level 3 compliant 1U chassis to ensure that high-trust security is maintained for all system events, transactions and operational activities. Ascertia's approach is unique in delivering a complete SAM solution within a high trust environment.

ADSS Server provides instant interoperability for signing applications by exposing a cloud signature consortium (CSC) compliant interface as well as providing broad support for secure signature authorisation via enterprise or national SAML, OAuth and OpenID Connect providers.



Benefits of Remote Signing

- No local hardware – there is no need to distribute smartcards / tokens to users that hold their signing keys since these are all securely managed centrally. This reduces costs substantially and improves the user experience
- Sign anywhere – any business application finds it easy to sign using whatever interface is presented to the user, typically on a desktop or mobile browser or within a mobile app. Various authentication / authorisation options are available from Ascertia or using third party Identity Providers (SAML / OpenID Connect / OAuth)
- Simplified key management – all cryptographic key management is securely managed centrally without user involvement, ensuring certificate issuance, certificate revocation, and certificate renewal is easy and fast
- Centralised policy control – all the signature policy settings relating to signature creation and verification are controlled centrally by the TSP, ensuring strong security and simplicity for users
- Centralised audit trail – all signing actions performed by a user are recorded by the TSP together with process-related meta information to provide supplementary evidence of the user's involvement beyond the signed document itself.
- Simplified signing – traditionally the use of high trust Qualified or AATL Advanced signatures has been associated with an awkward user experience. Remote signing services removed these obstacles and enables greater user acceptance using long-term signing keys or one time signing keys as required.

With so many options, Ascertia and its delivery partners can help you to define the best options to meet the various business, legislative and regulatory needs and reduce the risks and costs involved in creating, sending, receiving and storing unprotected business documents. The multiple capabilities of ADSS Server can be used to solve today's needs and also offer tremendous investment protection to meet the changing needs of tomorrow.

ADSS Server has been designed to meet the needs of SMEs, large multi-national organisations, managed service providers and regional trust schemes. It does this by providing flexibility, resilience, scalability, combined with well-designed internal security, management, audit logging and reporting that meets ETSI / CEN requirements for trustworthy systems.

For bulk file or document signing review Ascertia's ADSS Auto File Processor product.

Ascertia's Support Services ensure you are in good hands with rapid access to experts should an issue arise. The support service also provides regular access to the latest versions of your licensed software.

Before each release Ascertia runs thousands of functional and security tests. Sophisticated pen-tests are carried out to ensure that ADSS Server is resistant to all known security attack scenarios.

Training services and Premier Success services are available to ensure business deployments are quick, effective and optimally configured.

ADSS Server SAM Appliance is a Common Criteria Certified Remote Qualified Signature Creation Device (RQSCD), that enables QTSP's to deliver qualified digital signature services for natural persons, legal representatives, timestamps, and eSeals for any type of document, web form or transaction.

Secure web-based management is provided as standard together with advanced management configuration options and detailed reporting.

- **Embedded Operating Systems:**
  Red Hat Enterprise Linux
- **Hardware Specification**
  Intel XEON CPU
  32 GB DDR4 RAM
  1 TB SSD HDD
- **Embedded Databases:**
  Percona-XtraDB-Cluster
- **Hardware Security Module support (all must be EN 419 221-5 certified)**
  Thales Luna K7
  Entrust nShield Solo XC
  Utimaco CS CP5

Mike Hathaway | Chief Product Officer

About Ascertia

Ascertia provides digital trust for people, devices, data and documents for everybody from individuals to Enterprises and Governments. Ascertia's PKI and digital signature technologies serve a global customer base and partner network via direct and indirect sales channels.

For more info
info@ascertia.com
www.ascertia.com