ADSS Signing Server

ETSI PAdES, XAdES, CAdES Digital Signatures

ADSS Signing Server is a well-proven, standards-based product that can be deployed on premise for enterprise use or within a managed service as part of a cloud service. It can meet the most demanding needs by providing high throughput and high availability. As a strategic product for Ascertia, it offers support for the latest Windows and Linux operating systems, databases and HSMs.

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.

In the digital world, digital signatures offer far more flexibility and security. Digital signatures are used to secure documents, data, transactions, emails, software applications etc. Signatures can be short lived or last for months, years (or even multiple decades using special archiving approaches).

The most common use cases are (a) document workflow and digital signature approval, and (b) bulk signing of documents such as invoices or reports. In Europe eIDAS defines Qualified eSignatures and Qualified eSeals as the having the highest level of trust and Qualified Trust Service Providers offer Qualified Certificates to natural persons and legal entities to enable them to sign.

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

In the past smartcards have been a dominant form of providing appropriate high-trust security for user and corporate signing keys, HSMs have also been used for bulk signing. eIDAS has now defined a new set of standards to allow centrally managed remote signing and sealing services. Ascertia was the first company in the world to deliver a product (ADSS Server SAM Appliance) that was CC EAL4+ certified as meeting these.

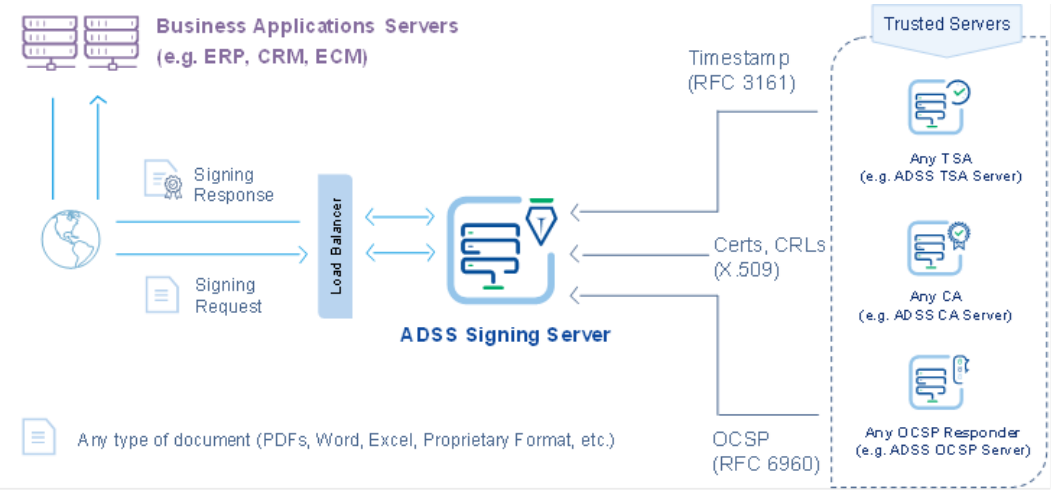
Key Features

- **Standards Supported:**
  IETF, ETSI, ISO, W3C, OASIS, CSC
- **Sign, Verify and Trust data format support:**
  - For PDF & Office documents, XML data, Forms and email
- **Signature format: Sign and verify using all common formats:**
  - PDF: PAdES BES, -T, -LT, -LTA + DT
  - Office: XAdES BES, -T, -XLong, -A,
  - Other: CAdES BES, -T, -XLong, -A PKCS#7, CMS, S/MIME
- **Verification & Enhancement Options:**
  Verify and extend signatures
  - PAdES BES > T > LT > LTA
  - XAdES BES > T > C/X > XL > A
  - CAdES BES > T > C/X > XL > A
  - Supports historic verification
- **Notary / archive / ERS archive:**
  PAdES-A, XADES-A, CAdES-A
  RFC 4998 Evidence Record Syntax (ERS)
- **Enterprise Deployment:**
  ADSS Server can be quickly installed on premise using user or corporate keys/certs to sign document and data.
- **Cloud Service Deployment:**
  ADSS Server can be quickly installed within a trust service provider to handle multi-tenant signing requests.
- **Hybrid Deployment:**
  ADSS Server can hash data locally and send the hash securely to a trust service provider for signing, ensuring confidentiality
- **High-Trust Architectures:**
  ADSS Server can easily be configured to work within multi-tier datacenters and work with multiple CAs, CRLs, OCSP and TSA Servers

ADSS Signing Server Architecture

ADSS Server provides all of the ETSI PAdES, XAdES, CAdES digital signature trust services for a wide range of business documents, data and information workflows. It can be simply and easily integrated with ECM, CRM or ERP business applications via high-speed APIs, OASIS DSS web services or bulk file processing services. Very little application development or integration effort is required since ADSS Server maintains all the management knowledge to understand how to sign, where to sign, with what keys, where these are kept, which CAs to trust, how to validate certificates, etc. Such changes to Security Policies do not affect business applications and they can be securely administered.

ADSS Server provides high-level security services whilst removing all the lower-level complexities from the business environment. ADSS Server administrators map security policies into signature profiles. They then permit or deny client applications the right to use these, e.g. the "invoice signing" profile should only be allowed by the finance department invoicing application. Keys associated with invoice signing are not available to other applications



Common use cases for ADSS Signing Server

- Adding digital signature creation or verification services to web-applications so that users can sign as part of their ERP, CRM, ECM or financial application using API calls to ADSS Server s
- Bulk and signing of PDF, XML and other documents such as, invoices, reports, statements etc.
  - via OASIS DSS XML/Soap Web Services
  - via a fast HTTP/S service interface
  - using ADSS Client SDK and its high-level .NET or Java API
  - using ADSS Auto-File Processor to concurrently process tens or hundreds of documents
  - using one or more corporate (bulk) signing keys/certificates
- Signing keys and certificates can be held
  - locally in USB tokens or smartcards accesses via ADSS Go>Sign Desktop
  - centrally in a qualified trust service provider remote signing service environment
- High availability and throughput
  - ADSS Server supports multi-threaded processing and load balanced across multiple servers to support demanding SLA requirements

Hundreds of server instances have been deployed in all of these modes (and more complex ones too). ADSS Server is used to power SigningHub. SigningHub provides document workflow and digital signature approval processes, allowing end users to review a document, fill-in form fields, add comments and digitally sign documents. It can be used by internal or external users. See how well ADSS Server can power this and similar web-applications at SigningHub.com

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 the Auto File Processor option for ADSS Server.

ADSS Server support services ensure you are in good hands with rapid access to experts should an issue arise. The 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 also available to ensure business deployments are quick, effective and optimally configured.

ADSS Signing Server is a comprehensive solution for creating and verifying advanced digital signatures on 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.

Supported Operating Systems:

Microsoft Server 2022, 2019, 2016
Linux RedHat, SUSE, CentOS, Ubuntu

Supported Databases:

Microsoft SQL Server 2022, 2019, 2017
Oracle 19c, 18c
Azure SQL Database (DB-as-a-service)
PostgreSQL 14, 13, 12, 11
MySQL 8, 5
Percona-XtraDB-Cluster 8, 5

Supported Hardware Security Modules

Thales Luna and ProtectServer
Entrust nShield
Utimaco SS & CS CP5
Microsoft Azure Key Vault
Amazon AWS Cloud HSM (Linux Only)

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