ADSS Server™

for PDF, XML & PKCS#7 Signing & Verification

- Apply **corporate** server-based digital signatures
- Enable **end-user** client-side or server-side digital signatures
- Using OASIS DSS signing services
- OASIS DSS-X signature and certificate verification
- Using PEPPOL signature and certificate trust ratings

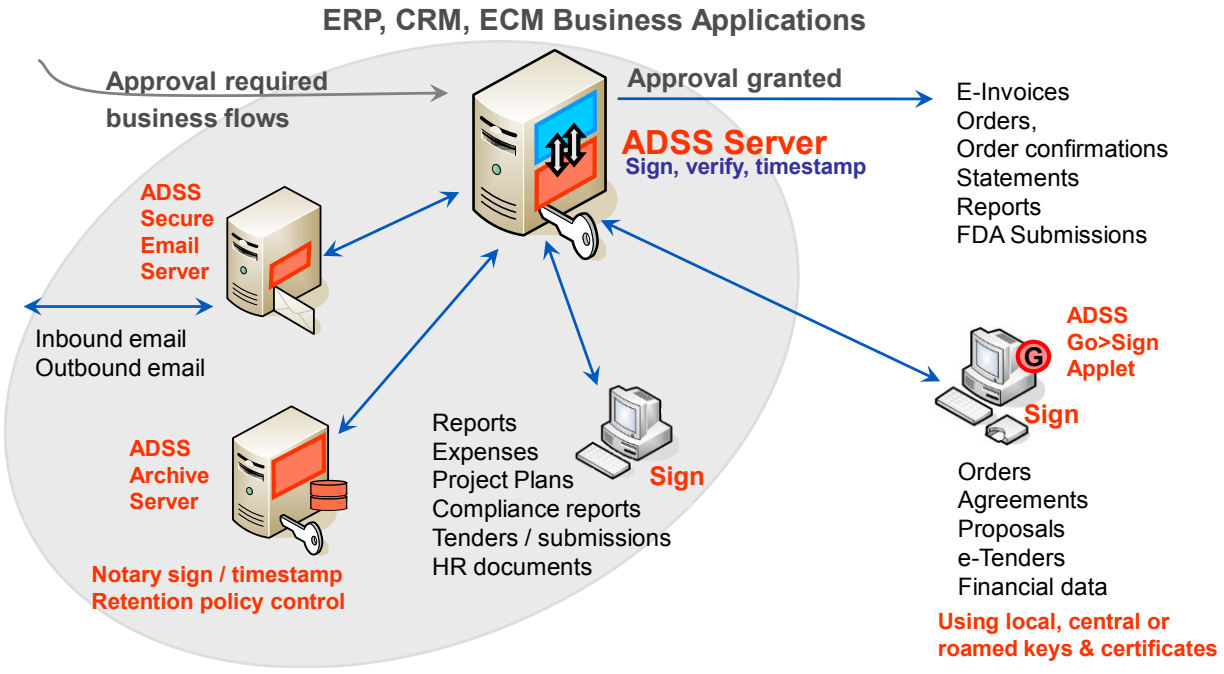
Organisations today are facing a variety of pressures to provide enhanced security of data, better accountability, traceability and audit to aid compliance with local legislation, regional directives and internal needs. From a commercial and efficiency perspective there is also a strong drive to replace paper-based processes with secure, electronic ones. User Identity, system identity and digital signature verification and validation can add significant value to providing trust and traceability within such business processes.

ADSS Server is designed to provide OASIS DSS and DSS-X 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 APIs, Watched Folder or even Email. A minimum of application development or integration 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. Thus small changes do not affect the applications.

The following business workflows benefit from the enhanced traceability of requests and approvals, instant document or data integrity checking, audit and compliance:

- Sending documents with digital signatures to external parties:
  - Receipts, Invoices, Quotations
  - Reports - consultancy and project reports, regulatory data, case notes, next actions etc
  - Approved agreements (Loans, insurance)
  - Government submissions
- Sending documents with digital signatures internally:
  - Personnel documentation
  - Internal policy documents
- Verifying received digital signatures:
  - On quotations and tender documents
  - On Orders, Reports, Regulations etc
  - Invoices, Internal policy documents
  - Authorising/approving expense sheets, time sheets, HR forms, design documents
- Creating a signed notary archive of received documentation

A Business Workflow with accountability, traceability and archive services



Digital signature creation and verification for e-business documents and data

ADSS Server provides high level security services whilst removing all the lower-level complexities from the business environment. ADSS Server administrators define acceptable policies and profiles as well as how they will be applied and how they will be presented. They then permit or deny client applications the right to use these, e.g. the "invoice signing" profile should only be allowed by the specific finance department invoicing application.

The following tables show the multiple different ways in which ADSS Server can be integrated within a business workflow environment to suit existing systems and technologies and the signing and verification options that exist.

ADSS Server Integration Options

	Sign	Verify
ADSS Server Web Services		
- via OASIS DSS XML/SOAP messaging	✓	✓
- via a provided high level .NET API	✓	✓
- via a provided high level Java API	✓	✓
- via a fast HTTP interface	✓	
Using ADSS Go>Sign - Within a web-browser (Go>Sign Applet)	✓	✓
Using ADSS Auto File Processor - For one or more watched folders	✓	✓
Using ADSS Gateway (for data privacy) - to extracts & verifies document signatures	-	✓
Using the Secure Email Server - to handle emails and/or attachments	✓	✓
Used as part of Ascertia Docs	✓	✓

OASIS DSS Signing Capabilities

- ➔ Sign various document / data formats
  - PDF, XML, File, Form (PKCS#7) and S/MIME
- ➔ Sign using various format options
  - Embedded – e.g. PDF, XML DSig
  - Detached – e.g. XML DSig, PKCS#7, CMS
  - Wrapping – e.g. PKCS#7 / CMS / XML DSig
  - Plus timestamps (PAdES-T, XAdES-T, CAdES-T, and -A)
  - Plus validation status (PAdES, XAdES, CAdES)
  - PAdES type 2,3,4 signatures
- ➔ Notary / archive / timestamp / evidence archive
  - LTANS Archiving, plus PAdES-A, XADES-A, CAdES-A
- ➔ For use with any internal or external document
  - Signing using corporate or user, server or client keys/certs
  - Local signing uses ADSS Go>Sign Applet

OASIS DSS-X Verification Capabilities

- ➔ Verify & Trust various document / data formats
  - PDF, XML DSig, PKCS#7, CMS and S/MIME
- ➔ Verify various signature types
  - Embedded – e.g. PDF, XML DSig
  - Wrapping – e.g. PKCS#7 / CMS / XML DSig
  - Detached – e.g. XML DSig, PKCS#7, CMS
- ➔ Special options
  - Add/check timestamp information (XAdES, CAdES, PAdES-T)
  - Add/check validation status information (AdES -X-L -A)
    PAdES type 2,3,4,5 signatures
  - Optional Historic verification of any signature
- ➔ For use with any internal or external document
  - Use with any received signatures at a server
  - Use with any received signature at a desktop

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 is designed to meet CWA 14167-1 requirements for trustworthy systems.

ADSS Server Standards Compliance:

Interface standards:	OASIS DSS and OASIS DSS-X services (including over SSL/TLS), high speed HTTP/S protocols, Auto File Processor (AFP) Watched folders, Secure Email Server for email support, Java and .NET APIs
Signature generation:	PDF, PDF/A, XML DSig, PAdES 2,3,4, XAdES, CAdES (ES, -T, -C, -X, -Long, -EPES, -A), PKCS#7, CMS, S/MIME
Signature verification:	One or multiple PDF, XML DSig, PAdES, XAdES, CAdES, PKCS#7, CMS and S/MIME signatures
Signature enhancement:	Enhances PAdES 3,4,5 XAdES and CAdES signatures to include timestamp and certificate revocation data
Certificate validation:	Uses OCSP, CRLs, Delta CRLs, DPD/DPV or even XKMS and SCVP
Time stamping:	Gets RFC 3161 timestamps using TSP (RFC 3161)
HSM Support:	Any PKCS#11 compliant HSM, smartcard or token, e.g. SafeNet, Thales nShield, Utimaco and others
Operating Systems:	Windows 2003 / 2008 (32/64 bit) Server, Linux (32/64 bit), Solaris 10, 11 others on request
Databases:	SQL Server 2005/ 2008 (including Express), Oracle 10g, 11g, MySQL 5, PostgreSQL 8, 9
Options:	**ADSS CA, TSA and OCSP Servers can also be used to provide advanced trust infrastructure services**

Ascertia Limited
Web: www.ascertia.com
Email: info@ascertia.com
Tel: +44 1256 895416 US: +1 508 283 1890
40 Occam Road, Guildford, Surrey, GU2 7YG, UK

Digitally Signed By: Rod Crook
Reason: I approve this document
09/05/2012 09:23:13 GMT +01:00