

## ADSS Server™

- Apply **corporate** digital signatures
- Enable **end-user** client-side or **server-side** digital signatures
- Provide centralised signature verification
- Provide centralised certificate validation



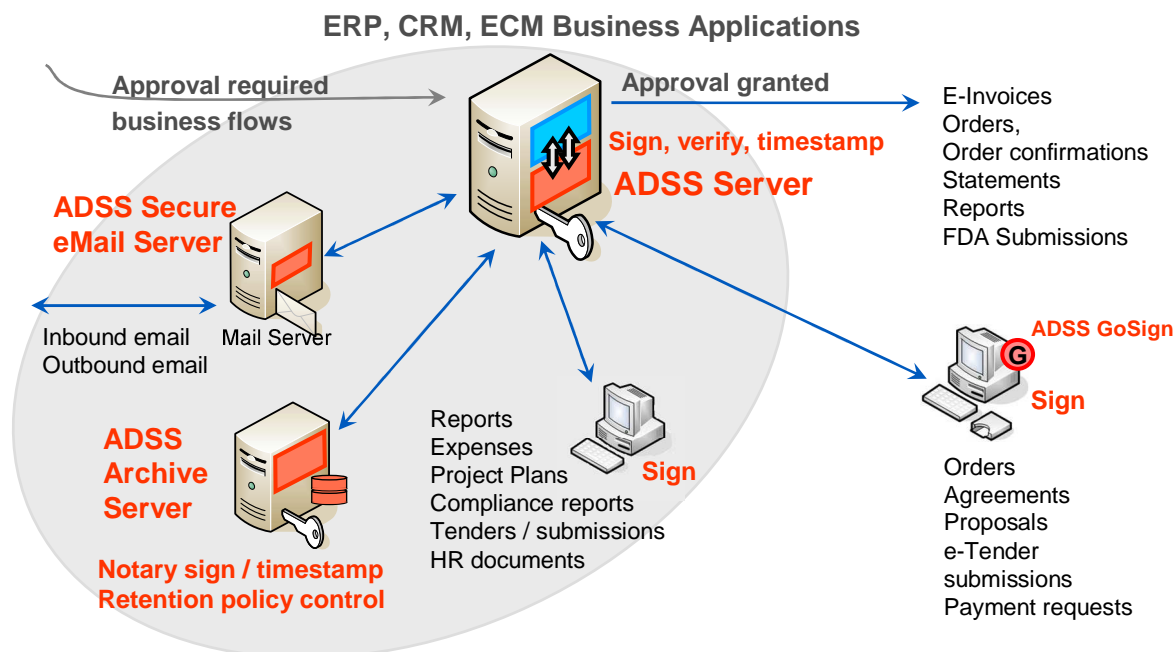
Organisations today are facing a variety of pressures to provide enhanced security of data, better accountability, traceability and audit to aid compliance with local legislation, regional directives and internal needs. From a commercial and efficiency perspective there is also a strong drive to replace 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 these 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



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
<b>ADSS Server Web Services</b>		
- via XML/SOAP messaging	✓	✓
- via a provided high level .NET API	✓	✓
- via a provided high level Java API	✓	✓
<b>Using ADSS GoSign</b>		
- Within a web-browser (GoSign Applet)	✓	✓
- Within a desktop .NET app (GoSign .NET)	✓	✓
- Within a desktop Java app (GoSign Java)	✓	✓
<b>Using ADSS Server Auto File Processor</b>		
- For one or more watched folders	✓	✓
<b>Using ADSS Gateway for confidentiality</b>		
- to extract signatures from documents	-	✓
<b>Using the Secure eMail Server</b>		
- to handle emails and/or attachments	✓	✓

### 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
  - Wrapping – e.g. PKCS#7 / CMS / XML
  - Detached (XML, PKCS#7, CMS)
  - Plus timestamp information (ETSI / PDF)
  - Plus validation status information (ETSI / PDF)
- Notary / archive / timestamp / evidence archive
- For use with any internal or external document
  - Use Corporate server signatures
  - User individual client-side signatures via GoSign

### Verification Capabilities

- Verify & Trust various document / data formats
  - PDF, XML, File, Form (PKCS#7) and S/MIME
- Verify various signature types
  - Embedded – e.g. PDF, XML
  - Wrapping – e.g. PKCS#7 / CMS / XML
  - Detached (XML, PKCS#7, CMS)
- Special options
  - Add/check timestamp information (ETSI / PDF)
  - Add/check validation status information (ETSI / PDF)
  - 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 meets the needs of small, large national and multi-national organisations. It does this by providing flexibility, resilience, scalability, combined with well designed internal security, management, audit logging and reporting. ADSS Server also offers CA, OCSP, XKMS, SCVP, TSA and LTANS Archiving services designed for Enterprise or Managed Service Provider use.

#### ADSS Server Standards Compliance:

<b>Signature generation:</b>	ETSI CAdES, XAdES (ES, -T, -C, -X-Long, -EPES, -A), PAdES, PDF & XML CMS/PKCS#7, S/MIME signatures
<b>Signature verification:</b>	One or multiple PDF, XML DigSig, ETSI CAdES, XAdES, PAdES, CMS/PKCS#7, S/MIME signatures
<b>Certificate validation:</b>	OCSP, CRLs, Delta CRLs, XKMS and SCVP
<b>Certificate generation:</b>	Generates PKCS#10 and accepts PKCS#12, PKCS#7, X.509v3 keys and certificates
<b>Time stamping:</b>	TSP (RFC3161)
<b>HSM Support:</b>	Any PKCS#11 compliant HSM, smartcard or token, e.g. SafeNet, nCipher and others
<b>Operating Systems:</b>	Windows 2003 / 2008 (32/64) Server, Solaris 10 and Linux versions
<b>Databases:</b>	SQL Server 2000/ 2005, Oracle 10g, MySQL, PostgreSQL
<b>Interfaces:</b>	OASIS DSS and DSS-X web services (including over SSL/TLS), HTTP(s) interface for administrators, Auto File Processor (AFP) Watched folders, S/MIME support for email integration, Java and .NET APIs
<b>Options:</b>	<b>ADSS Server can be used to provide advanced trust services</b> , e.g. TSA, OCSP

Ascertia Limited  
 Web: [www.ascertia.com](http://www.ascertia.com)  
 Email: [info@ascertia.com](mailto:info@ascertia.com)  
 Tel: +44 1256 895416 US: +1 508 283 1890  
 40 Occam Road, Guildford, Surrey, GU2 7YG, UK  
 © Copyright Ascertia Limited 2010. All Rights Reserved, E&OE