



Secure Solution

Ascertia eID validation and eID Signature Solutions

Ascertia is a global leader in delivering functionally rich, easy to deploy e-security solutions. The company focuses on digital signature creation, verification, timestamping and secure archiving products as well as eID validation. These key functions deliver the essential trust services needed by governments, financials, telco, healthcare and other organisations to conduct electronic business. Businesses need traceability, accountability and audit services plus clear originator authentication, signed approvals, assured data integrity and provenance to allow them to meet legislative, regulatory and internal controls requirements.

Design Philosophy

Ascertia's products are designed to be easy to integrate, configure and use in a wide range of business scenarios including

- (a) server-based centralised bulk signing of documents, such as e-invoices,
- (b) server-based user signing of workflow documents, such as project documents,
- (c) client-side signing using our web-based Go>Sign Applet accessing local or roamed credentials, such as document management and collaboration solutions,
- (d) using desktop products for off-line use and finally
- (e) being used within managed services for effective verification and validation.

Ascertia is committed to innovation with an over-riding design principle that our technology must be easy to deploy and configure and for busy business managers to use. We provide practical and authoritative advice on security solutions and offer sensible pricing based on feature usage for all our products. A global network of partners complements this approach.

ADSS

Digital Signature Creation and Verification for e-Business Documents and Data

ADSS Server

ADSS Highlight :

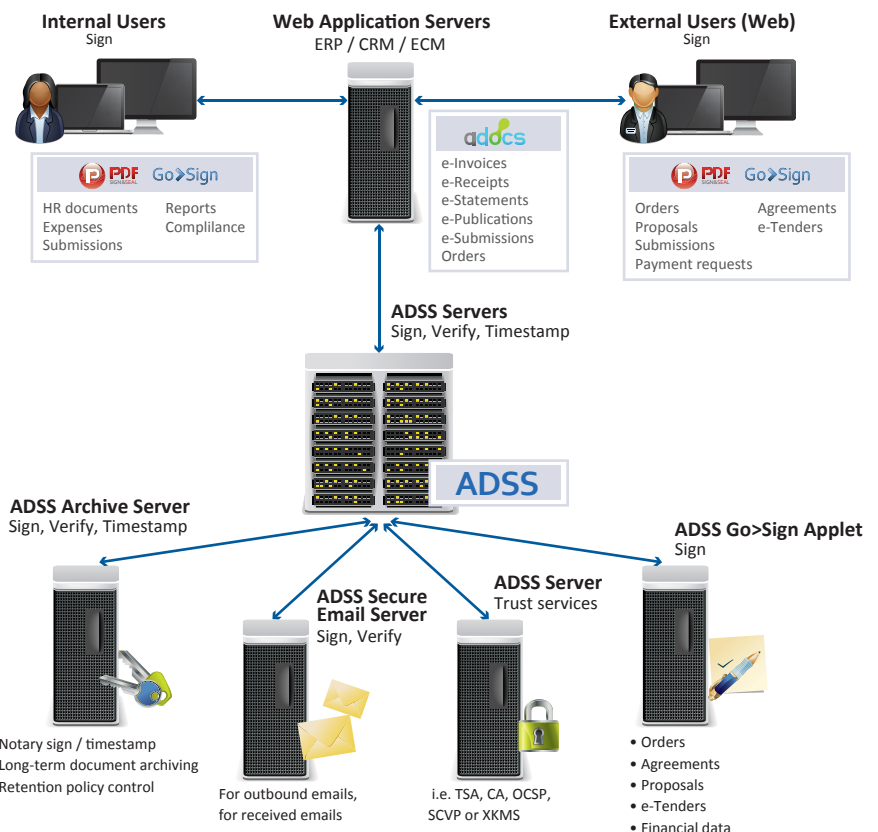
- for PDF, XML & PKCS#7 Signing & Verification
- Apply corporate server-based digital signatures
- Enable end-user client-side or server-side digital signatures
- Using OASIS DSS signing services
- OASIS DSS-X signature and certificate verification
- Using PEPPOL signature and certificate trust ratings

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.

ADSS Workflow

- ▶ 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



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	√	√

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 tables on left 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.

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 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:

Item	Specifications
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 Docs

Cloud-based Document Workflow and Digital Signature Approval

Ascertia Docs Highlight :

- Online document viewing and signing for internal and external users with full tracking of the business document approval process
- Individual user keys and certificates are used to create advanced digital signatures on PDF and PDF/A documents
- Available as a commercial cloud service and also as a software product for local deployment - you choose!

Substantial cost savings can be made when paper based processes are moved full on-line including print and send costs as the costs of searching and re-sending. For certain documents traceability, accountability and audit with clear legal integrity and individual signed approval are vital. Indelible digital signatures enable the on-line approval of any business documents such as agreements, orders, reports, insurance, expenses etc. Organisations need to show that their internal controls are effective and compliant with local legislation, regional directives and market expectations. And increasingly they need to demonstrate their commitment to the environment.

Ascertia Docs provides (or uses existing) e-IDs to create advanced digital signatures for persistent document security. The interface is intuitive and makes it easy for busy managers that want to use a system without being baffled by technology. Ascertia Docs provides a simple to use, document sharing, viewing and sign-off solution suited to any approval process. It cleverly implements industry standard advanced digital signature security to enable sign-off from anywhere!



PDF Sign&Seal

Advanced PDF Signing on the Desktop without Acrobat

PDF Sign&Seal Highlight :

- Advanced PDF Signatures
- Time-stamping
- PDF Creation
- PDF Encryption
- Form Filling

The cleverly packaged functionality within PDF Sign&Seal makes it easy for busy managers to digitally sign and approve business documents, be they purchase orders, invoices, financial and other reports, proposals, tenders, compliance statements or assessments. Professionals such as lawyers, accountants and engineers appreciate the way the product supports a full range of signature and appearance options for different types of document.

PDF Sign&Seal is focused on delivering comprehensive electronic digital signature capability to PDF documents. It can use any type of digital certificate including qualified certificates and Adobe CDS certificates. Options for simple, timestamped and full long-term signatures are included and the visible signature appearance can be designed to suit a range of business and document requirements. These can optionally include hand-signature images, business logos and signing data such as "reason for signing". PDF Sign&Seal is ISO 32000 PDF standard compliant and also ISO 19005 PDF/A compliant when signing.

Contact Us:

KUALA LUMPUR (HQ) SecureMetric Technology Sdn. Bhd.
Level 5-E-6, Enterprise 4, Technology Park Malaysia, Lebuhraya Sg Besi-Puchong, Bukit Jalil, 57000 Kuala Lumpur, Malaysia
T +603 8996 8225 F +603 8996 7225