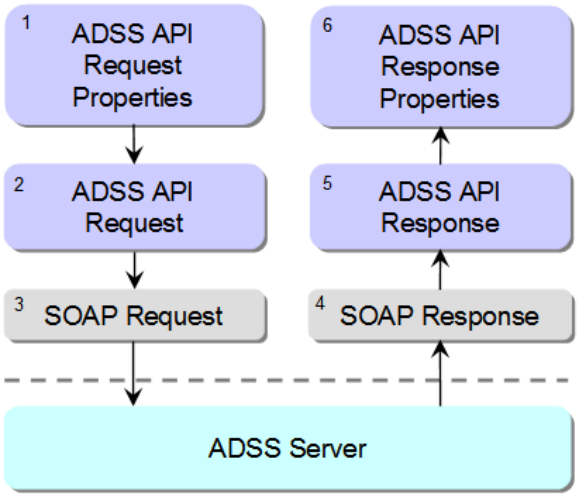
ADSS Client SDK™

- Enables applications to quickly and easily integrate with ADSS Server
- Offers high-level Java APIs
- Offers high level .NET APIs
- Provides source code examples
- Provides multi-platform support

Business applications need to provide enhanced security of data, better accountability, traceability and audit to aid compliance with local legislation, regional directives and internal needs. User Identity, system identity and digital signature verification and validation can add significant value to providing trust and traceability within such business processes. Substantial cost savings can be derived by replacing paper-based processes with secure, electronic ones.

The biggest issue is how can new and any existing applications be readily trust enabled. The answer is by using Ascertia's client software, ADSS Client SDK. Ascertia Client SDK also powers Ascertia's Auto File Processor and Secure Email Server applications. Ascertia's web-site also shows live demos.

ADSS Client SDK offers high level APIs that give simple access to the appropriate protocols for various service requests and responses. It supplies all the libraries necessary to easily integrate with business applications. The following diagram shows how ADSS Server can be integrated with high-level calls to the Ascertia Java or .NET based client web-services library:



One license for ADSS Client SDK is provided with each ADSS Server. ADSS Go>Sign Applet is also included within the software since this is often used with ADSS Client SDK however a separate license is required to use the ADSS Go>Sign Applet software.

ADSS Client SDK includes these options:

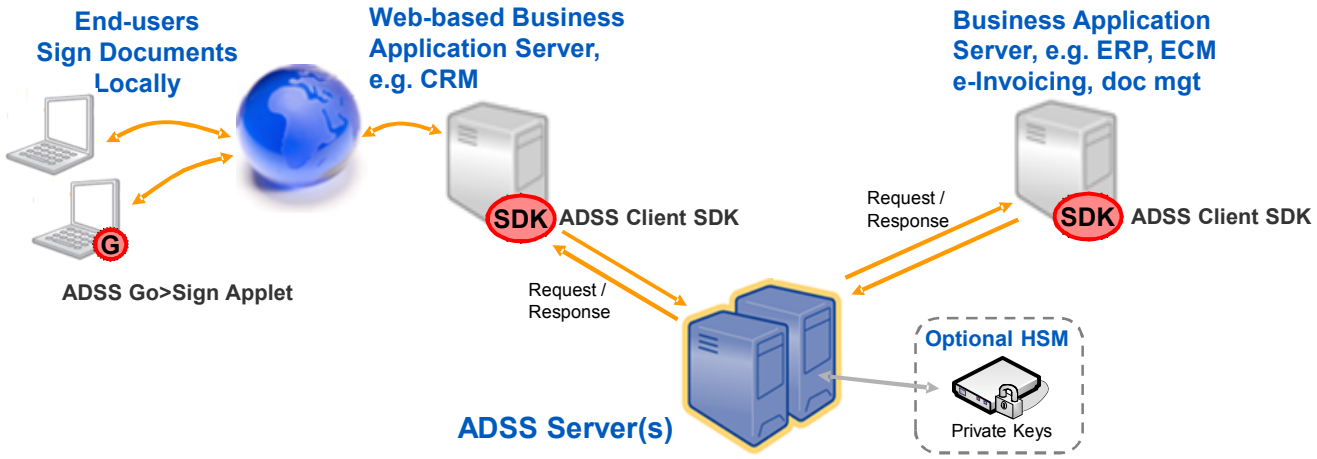
- Java API
  with an OASIS DSS XML/SOAP web services interface, plus an optimised HTTP interface for signing, supported on Java 5 and Java 6 application environments
- .NET API
  with an OASIS DSS XML/SOAP web services interface, plus an optimised HTTP interface for signing, uses .Net Framework 2.0+

Why use ADSS Client SDK

- One copy of ADSS Client SDK is licensed for use with each production ADSS Server license that is purchased.
- The SDK provides easy access to these functions:
  - Signing and verifying PDF, XML data, Files etc, using OASIS DSS and DSS/X protocols
  - Timestamping
  - Validation using SCVP, XKMS (and OASIS DSS)
  - Archiving using ETSI AdES-A and LTANS
  - Decryption using DSS (e.g. used when Go>Sign Applet has encrypted in-bound data ideal for tenders, health data, etc.)
- Supports PDF, XML DSig, PKCS#7, CMS & S/MIME plus ETSI AdES -BES, -T, -C, -X, -X-Long and -A formats.
- Supports local hashing of data and signature handling and embedding for PDF documents.
- Supports the signing of one or multiple documents in a single call to ADSS Server.
- Facilitates the verification of signatures with a full range of "Respond With" attributes as well as PEPPOL signature and certificate trust ratings.
- Facilitates the use of ADSS Go>Sign Applet by providing the linkage to ADSS Server for back-end services such as obtaining long-term signature data and verifying the local Go>Sign signatures that have been created.
- Always keeps in step with ADSS Server features to ensure easy access to, and use of, the latest features.
- Developers are also able to create their own web-service calls to ADSS Server using the supplied WSDL files. It should be noted that the ADSS Client SDK will save considerable development and test time.
- ADSS Client SDK also offers the option of using direct HTTP/S based signing services to save the overheads of handle large documents via web services.
- Java versions are available for virtually any platform. Java 6 versions are available from the product download site and Java 5 versions are available on request.
  .NET versions are available for Windows platforms (requires .NET framework v2+).

Making it easy to deploy trust services to business applications & workflows

The following diagram illustrates how ADSS Client SDK is used to advantage within ERP, ECM CRM applications today for internal and external sign-off and approval, signature verification, bulk document signing and indeed any trust service request made to ADSS Server.



ADSS Client SDK provides APIs for signing, verification and encryption, using OASIS DSS, APIs for certificate management using CMC, certificate validation using OCSP, SCVP and XKMS and archiving services using LTANS (as well as ETSI AdES-A signing).

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.

ADSS Client SDK enables this interaction and simplifies the task. It is quite possible to get an initial application integrated within just four hours – this is feedback from one of our customers that downloaded our evaluation software and with no prior knowledge added signing to their documents.

Further Information

With so many options Ascertia and its partners can help to define the best options to meet various business, legislative and regulatory needs and reduce the risks and costs involved in creating, sending, receiving and storing e-business documents. The many 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 national and multi-national organisations, managed service providers and regional trust schemes. It does this by providing flexibility, resilience, scalability, combined with strong internal security, management, audit logging and reporting.

ADSS Server Gateway Edition enables signatures to be extracted from sensitive documents so that no loss of privacy occurs when using centralised verification services from a third party.

ADSS Client SDK Standards Compliance:	
Signature generation:	PDF signatures. XML DSig, ETSI PAdES, CAdES, XAdES (-T, -C, -X-Long, -EPES, -A), CMS/PKCS#7, S/MIME
Signature protocol:	OASIS DSS v1.0 over SOAP/XML and HTTP/S
Signature verification:	One or multiple CMS/PKCS#7, PDF, XML DigSig, ETSI CAdES, XAdES, S/MIME signatures
Verification protocol:	OASIS DSS & DSS/X v1.0 over SOAP/XML
Certificate validation:	OCSP, CRLs, CRLs (includes delta and indirect), SCVP and XKMS (also available using OASIS DSS-X protocols)
Certificate generation:	Generates PKCS#10 and accepts PKCS#12, PKCS#7, X.509v3 (the ADSS CA service supports CMC protocols)
Long-Term Archiving:	IETF LTANS Specifications (LTAP and XMLERS)
HSM support:	Any PKCS#11 compliant HSM, smartcard or token, e.g. SafeNet, nCipher and others
Operating Systems:	Windows 2003 / 2008 (32/64) Server, Solaris 10, Linux (e.g. Suse, RedHat, CentOS)
Languages:	Java 6 (Java 5 on request) for any platform plus .NET on Windows 32/64 servers
Databases:	SQL Server 2005/ 2008, Oracle 10g, 11g, MySQL 5, PostgreSQL 8

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

Signed By: Rod Crook
Reason: I approve this document
11/01/2011 22:55:36 GMT +00:00