# ADSS Server™ for Infrastructure Services

- Certificate Validation Authority services
  - OCSP Responder
  - XKMS Server
  - SCVP Server
- Time Stamp Authority services
- Web-services Certificate Issuance


**ADSS Server** provides certificate validation authority, time-stamp authority and where required certificate issuance and management services to meet the needs of service providers or for enterprise projects.

Although it offers OCSP, TSA, CA, XKMS and SCVP functionality only the services that are needed need to used. Of course other services can be licensed for use at a future date if required. To emphasise the functionality of the product we use various "ADSS" marketing names when a single service is being discussed to make it easier to find relevant information when conducting web-searches:

## ADSS OCSP Server

**An RFC 2560 compliant OCSP Responder for real time certificate status checking:** ADSS OCSP Server has been designed to operate as a robust validation hub solution, capable of providing OCSP certificate validation services for multiple Certificate Authorities (CAs). It offers class-leading flexibility for request and response handling, throughput and availability, CA integration, configuration management and reporting.

## ADSS TSA Server

**An RFC 3161 compliant Time Stamp Authority (TSA) used for the generation of secure cryptographic timestamps:** The TSA module provides independent proof of date and time for business data and digital signatures that provides legal weight evidence that business transactions occurred at a defined moment in time and that they have not been subsequently altered. Such timestamps can be used to prove when a digital signature was applied to a document so that its status can be verified in the long-term, even after the subsequent expiry or revocation of the signer's digital certificate.

## ADSS CA Server

**An RFC 3280 compliant Web Services CA for certificate issuance and management:** The CA Module offers Certificate Authority features via a high level XML/SOAP web services interface. This can be used to advantage for extranet applications where users need to be provided with a certificate to authenticate themselves via SSL or Email or applying a signature within a closed environment where the users are generally already well-known to the business – i.e. they are existing customers, partners or suppliers. These certification services can be easily integrated within a business application or a dedicated Registration Authority. In such cases Ascertia can also deliver project-based Registration Authority applications to meet specific business needs.

## ADSS XKMS Server

**An XML Key Management Specification 2.0 server:** The initial version of ADSS XKMS Server supports the X-KISS certificate validation services. A later version will support X-KRSS registration, re-issuance, revocation and recover services.

Interest in the W3C XKMS standard has being growing recently thus creating the market demand necessary to sustain such products. Ascertia continues its policy of investing in such areas.

## ADSS SCVP Server

**An RFC 5055 compliant SCVP Server intended for complete certificate chain validation:** ADSS SCVP Server will be available during 2009 and provide server-side validation of digital certificates. SCVP focuses on providing server-based path building and certificate chain validation.

## ADSS Server - Key features

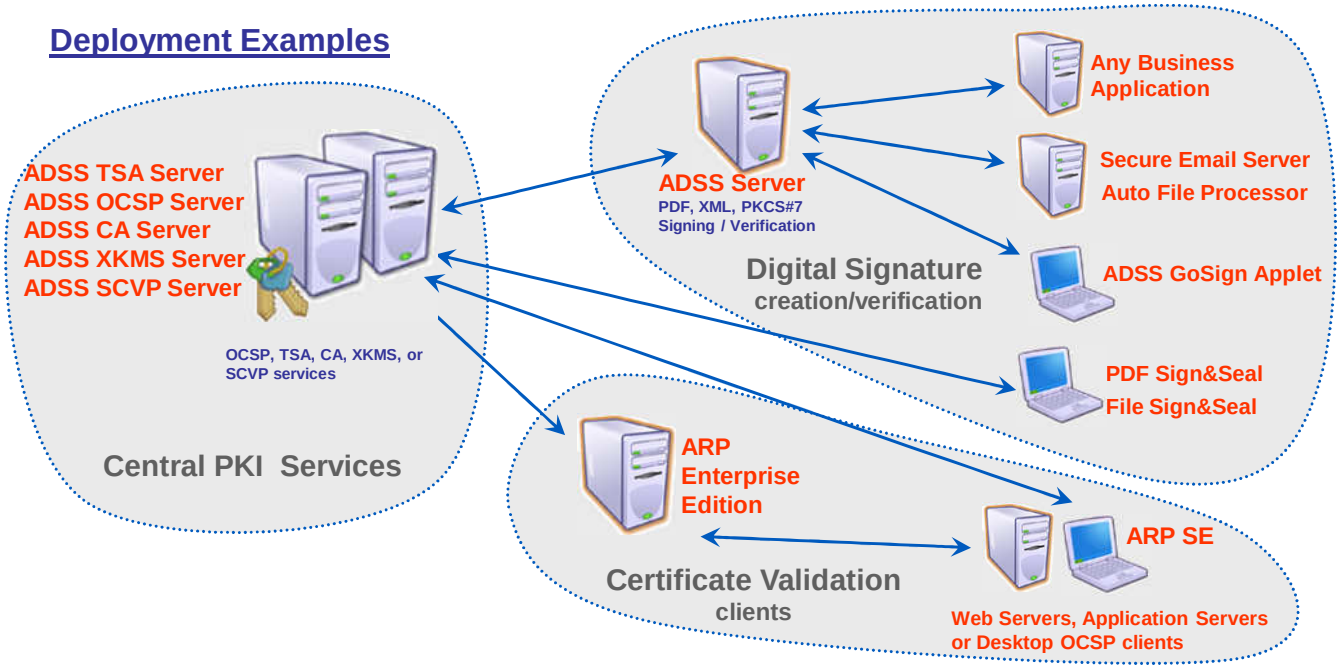
- **Service Management:**
  The web-based management interface has been designed to be easy to use and understand and be consistent between the various services. Each service uses policy-driven controls to determine how it responds to service requests.
- **Security:**
  ADSS Server provides detailed event and transaction logging; strong operator authentication, coupled with role based access controls; an email/SMS alert system; and support for various HSMs and tokens. The advanced security features include using HMAC protected configuration and log files, automatic database integrity checking and an option for using dual controls.
- **Scalability and Resilience:**
  ADSS Server takes advantage of its J2EE architecture to maximise scalability and availability on each system it runs on. Multiple load balanced servers can be used to provide parallel throughput and high availability.
- **Reporting:**
  ADSS Server includes an inbuilt reporting module that provides detailed analyses of overall service usage and per-client reporting. Reports can be created in PDF and CSV / spreadsheet formats.

# Certificate Validation, Timestamping and Certificate Management Services

In summary ADSS Server provides valuable trust services for certificate validation, timestamp issuance and also certificate issuance. These services can easily be used by any standards-compliant security client application. Of course most of Ascertia's other products can also act as clients for these services, including PDF Signer Server, XML Signer Server, File Signer Server, PDF Sign&Seal, File Sign&Seal, ARP Enterprise Edition (EE) and ARP Standard Edition (SE).

Today's demand for real-time eID validation, signing documents with embedded timestamp and validation data, archive signing, simple extranet client-side signing as well as server-based verification and countersigning are good examples of where ADSS Server adds considerable value to managed service providers.

## Deployment Examples




The diagram provides just a simple illustration of the capability – more information is available to suit your business or project requirement. Contact Ascertia or one of its partners now to discuss the product capabilities in more detail.

## Technical Details

Only the required services need be deployed and used. ADSS Server has been carefully designed to offer security, scalability, ease of use and management with various integration options to suit today's business applications. Key features include role based access control, service request authentication, detailed event and transactional logging – all essential requirements for a centralised trust services provider. The following table illustrates the broad set of features:

| | |
|---|---|
| **OCSP Services** | Multi-CA & multi-key support, unique validation policy per CA |
| **Timestamp Services** | Multiple TSA profiles & multi-key support, ability to proxy to back-end devices |
| **Archiving Services** | Secure archiving of signed and unsigned objects, ETSI ES-A format and IETF LTANS ERS format |
| **Key Lengths** | 1024-bit, 2048-bit, 4096-bit RSA, and with SHA-1 and SHA-2 (256, 384 and 512) algorithms |
| **Trust Anchors** | Use in-built CA(s), or back-end trust service providers |
| **Certificate Services** | X.509 certificates and CRLs, RFC 5280, CRL issuance and real-time OCSP certificate revocation |
| **External Security** | Strong authentication of requestors, email and SMS alerting of issues, detailed management reports |
| **Internal Security** | HMAC database integrity checking, secure logs, signed archives, optional dual control operations |
| **Scalability** | J2EE application providing high availability, scalability, resilience and multi-server load balanced throughput |
| **Interfaces** | XML/SOAP, RFC 2560, RFC3161, RFC5055, LTAN XMLERS & LTAP, W3C XKMS, HTTP/S |
| **Hardware devices** | SafeNet and nCipher HSMs, Smartcard, USB tokens and other PKCS#11 compliant devices |
| **Databases** | SQL Server 2005, 2008, Oracle 10g, 11g, PostgreSQL and MySQL |
| **Operating Systems** | Windows Servers (32 & 64bit), Solaris 10 (Sparc and x86), CentOS and other Linux variants |

Contact us now for more information:


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
01/07/2010 10:35:38 GMT +01:00