ADSS Server FAQs

Overview

ADSS Server provides comprehensive digital signature creation, verification and time-stamping services to any online application needing to trust documents and data that it sends out or receives. It is a single server product but market under various names depending on the modules selected. ADSS Server has been designed for internal enterprise use as well as external multi-party use and for Managed Service Providers.

Getting Started...

- Download a 30 day evaluation version
- Which OS privileges are required to install ADSS Server?
- How to obtain and install a commercial license of ADSS Server?

More...

Product Documentation

Release notes (PDF)
Installation guide (PDF)
Upgrade instructions (PDF)
Quick guide (PDF)
Admin guide

Support

General inquiries
Sale inquiries
Technical support
Live help
Live Skype support (ascertia.support)

Services & Modules

ADSS Signing Service

ADSS Signing Service provides a comprehensive solution for creating advanced digital signatures on any type of document, web form or online transaction data. Click here for details.

- How to prevent database bloating in ADSS Signing Service?
- How can I configure the PDF signature dictionary size?

More...

ADSS Verification Service

ADSS Verification Service provides the OASIS DSS and DSS-X compliant options for data and document signature verification services to any requesting client application. Click here for details.

- How to configure ADSS Verification Service to verify digital signatures?
- How to invoke verification profile for non-registered CAs?

More...

ADSS Certification Service

ADSS Certification Service provides the certificate authority services to client applications, which may act as RA and send public keys for certification and/ or request the creation of asymmetric key pairs. Click here for details.

- What is meant by an External CA?
- How to configure a Microsoft CA with ADSS Server?

More...

ADSS OCSP Service

ADSS OCSP Service is an advanced implementation of the Online Certificate Status Protocol (OCSP) for providing the revocation status of x.509 certificate, based on either CRLs or realtime certificate information. Click here for details.

- How to avoid a malformed request error when sending multiple Cert IDs in a single OCSP request?
- How to configure the ADSS OCSP Service to produce high speed OCSP responses?

More...

ADSS TSA Service

ADSS TSA Service provides an independent and irrefutable proof of time for transactions, documents and digital signatures. It can create legal weight evidence that business transactions occurred at a defined moment in time, and they have not been subsequently altered. Click here for details.

- How to include the full TSA certificate chain in ADSS TSA Server response?
- Is it reliable to use the system clock in a virtualised environment?

More...

ADSS XKMS Service

ADSS XKMS Service provides a sophisticated real-time certification Validation Authority, fully conformant with W3C XKMS and PEPPOL validation protocol. Click here for details.

- How to decide between the Basic Validation and Advanced Validation settings in an XKMS profile?
- How to invoke an XKMS profile for non-registered CAs?

More...

ADSS SCVP Service

ADSS Go>Sign Service

ADSS RA Service

ADSS SCVP Service supports the RFC5055 Server-based Certificate Validation Protocol (SCVP). This protocol is used to determine and validate the path between an X.509 digital certificate and a trusted root. Click here for details.

- How to ensure seamless processing of signature/ certificate validation request, when the CA chain is already registered in Trust Manager?
- How to invoke validation policy for non-registered CAs?

More...

ADSS Go>Sign Service is a complete client side solution for browser-based document viewing, form-filling, advanced signing/ authentication and centralised signature verification, by using the local and server held keys. Click here for details.

- How to configure the environment to use the Signotec Tablet with the Go>Sign Service?
- How to configure the environment to use the Wacom STU-500 Tablet with the Go>Sign Service?

More...

ADSS RA Service acts as a gateway between PKI end-entities that include human users, servers or devices, and the back-end secure Certificate Authorities (CAs). Click here for details.

- How does ADSS RA Service process the certification requests?
- How to make the certification requests received over the RA web service interface to be processed synchronously?

More...

Key Manager

The ADSS Key Manager module is responsible for managing all the keys used within the ADSS system (i.e. for any of the service modules). The keys can be generated, stored and used inside a PKCS#11 compliant HSM or within the ADSS database in case of software mode. Click here for details.

- How to configure ADSS Server to use Key Encryption Key (KEK)?
- How to attach multiple HSMs to ADSS Server?

More...

Trust Manager

The ADSS Trust Manager module is used to register all the acceptable Trust Authorities (TAs). It is a global utility, supporting various other modules of ADSS Server to verify signed objects such as certificates, OCSP responses, CRLs or timestamp tokens. Click here for details.

- How to replace an expired CA certificate?
- How to link a CA to the relevant TSAs to in ADSS Trust Manager?

More...

CRL Monitor

The ADSS CRL Monitor module provides an automated monitoring for multiple CRL issuers, it provides effective management reporting, failure alerting through email and SMS and other advanced options. Click here for details.

- Why is ADSS CRL Monitor not downloading CRLs against a configured CA?
- How to implement real time revocation?

More...

Global Settings

The ADSS Global Settings module is used to configure ADSS Server settings that are applicable throughout the ADSS modules. Click here for details.

- How to import ADSS Server configurations from one server to another?
- How to configure SMS Alerts in ADSS Server?

More...

Manage CAs

The Manage CAs module provides the capability to configure multiple local CAs/ AAs and/ or external CAs for the certification purposes. Click here for details.

- How to replace an existing local CA?
- How to import a CA and its issued certificates into ADSS Server?

More...

Access Control

The ADSS Access Control module provides a secure authentication and authorization mechanism via ADSS Server Console. Click here for details.

- How to register a new operator in ADSS Server Console?
- How to ensure the accessibility of ADSS Server Console?

More...

Operational Management

This section describes 'How to Operate' ADSS Server and other operator actions that may need to be performed from time to time. Click here for details.

- Installation & Configuration
- Software upgrade

More...

Third Party Integration

Some of the third party system integrations that are available for ADSS Server:

- DMZ / Load-balancing configurations
- HSM configurations

More...

ADSS Server Error Codes

Here are the system defined error messages sent by ADSS Server to client applications:

- Certification service
- Signing service

More...

Miscellaneous

- Producing PAdES-LTV signatures in ADSS Server that are verifiable in Adobe Reader
- Trusting a Root CA certificate in the Adobe Reader

More...