ADSS Server Evaluation – Quick Guide

This document aims to provide a quick *'do this and it works'* guide to evaluating ADSS Enterprise Server as a PDF Signing Server both for server-side signing and also for client-side signing. For those people wishing to create more complex environments such as PDF verification, XML or File (PKCS#7) signing and verification services it will act as a good base which allows further exploration of the many capabilities of the ADSS Server.

Overview

ADSS Server offers comprehensive services for creating, verifying and validating digital signatures on PDF XML data and Files or Forms. It offers various options to integrate with business applications and workflows. This guide assumes that the ADSS Client SDK is used together with the sample code to interact with ADSS via web-services.

Key Features

- Business applications can be easily integrated using web-services directly or easier still using the ADSS Client SDK with high-level APIs.
- Very easy to install and configure without any special training requirements
- Strong, policy-based control over all operator and user interactions
- Sophisticated remote management workstation with role-based separation of administrator responsibilities.
- Provides access to detailed user reporting info to ease management burdens
- Offers multiple interfacing / interaction options to make it easy to deploy and integrate with business applications.
- Offers multiple signature policy options that enable applications to control the digital signature process -or have partial or no control as determined by ADSS policies
- Able to sign documents using server-held corporate keys and certificates
    - Using one or more keys in software
    - Using one or more keys held with an HSM
- Able to sign documents using end-user keys and certificates
    - When multi-user server-side signing is used, PDF Signer Server provides key generation and certification using either an in-built CA (rooted internally or externally) or via links to external CAs, e.g. Windows Certificate Server.
    - When Zero-footprint client-side signing is used then either software, USB or smart card based credentials on the user's system can be accessed using our Go>Sign Desktop/Applet.
- Able to verify and trust-check signatures on documents and pass various signer details to the application
- Able to offer historic verification of older digital signatures
- Allows multiple trust issuers to be registered and used by the system for enterprise, multi-third party, national or global environments
- Able to apply and verify timestamps
- Able to act as an On-line Certificate Status Protocol (OCSP) responder
- Able to create long-term signatures to ETSI and PDF standards
- Offers a simple intuitive web-based administration interface that offers substantial operational management advantages compared with other approaches.
- Signing, validation, certification, OCSP and TSA services can all be configured and managed from a single consistent browser-based remote management interface.
- Supports multiple database technologies. To see the details regarding all the supported databases, refer to *ADSS Server Installation Guide – System Requirements section*.

- Supports the options of using various HSMs for secure key management as well as smartcard based credentials for operator authentication

Further Information References

This document is a quick guide to get a simple configuration of the OCSP Service installed, tested and operational. More detailed information is available in the following documents:

- ADSS Server Installation Guide – detailed installation guide
- ADSS Server Admin Manual – details all the administrative features
- ADSS Server SQL Server Installation Guide
- ADSS Server Admin Manual – details all the administrative features. The manual is available online at the following location: http://manuals.ascertia.com/ADSS-Admin-Guide/default.aspx
- Ascertia has maintained an online knowledgebase for customer ease. You can follow these link for more details: http://faqs.ascertia.com/display/AKBS/Ascertia+Knowledge+base

The ADSS Client SDK documents should also be read:

- ADSS Developers Guide – detailed information on how to interact with ADSS Server

Additionally, the Go>Sign client side signing demonstrations can be configured and run once the evaluation installation is complete. They are part of the ADSS Client SDK document set:

- ADSS Go>Sign Developers Guide
- ADSS Go>Sign Desktop Installation Guide

Evaluation System Requirements

Please see the ADSS Server Installation Guide for supported operating systems, databases and other related information. You can also follow this online link: https://www.ascertia.com/products/system-requirements/

Quick Installation Steps

ADSS Server can be quickly installed for evaluation purposes using the following steps:

- Install MS SQL Server and create a new, empty database
- Install ADSS Server – Optionally choosing to use the sample evaluation data (*1)

(*1) The installer includes sample evaluation data which can be used to populate the ADSS Server database with the necessary cryptographic and profile data to start performing example signature, verification and certification transactions (explained later in this guide). This is a recommended option to help with the evaluation of ADSS Server. Do not select or use this option when you are installing ADSS Server in a production environment.

The evaluation uses the ADSS Server's software crypto libraries, however multiple hardware security modules (HSMs) can be used if required. For further information refer to the ADSS Server Admin Manual "Key Manager". It is recommended that you contact Ascertia for further configuration information when evaluating with an HSM.

Install MS SQL Server and create an ADSS evaluation database

Read the separate guide for installing and configuring MS SQL Server.

The key points to note are:

- Ensure that **mixed mode authentication** is selected during the installation. Using Microsoft Windows Authentication will lead to installation issues.
- Ensure that TCP ports are set to 1433 (for IP1, IP2 and IP All)
- Configure a database owner with administrator permissions

  → Ensure the language is set to **"English"**

Install ADSS Server

- Extract the ADSS Server installation zip file to a target folder, e.g. D:\ADSS-Server

  Note: The folder path cannot have spaces so you cannot use "ADSS Server" or similar

- From <ADSS Installation Directory>/setup run install.bat which starts a configuration Wizard

  Note: Setup cannot be run and completed more than once - If the evaluation needs to be re-installed then the ADSS Server installation directory needs to be deleted and the zip re-extracted

- The ADSS Server Installation Wizard shows a welcome screen then the license agreement and then asks if you wish to upgrade an existing installation or if you are installing for the first time. For new users you are installing for the first time so select this option. If you are adding a second server you are also installing for the first time.
- Confirm the installation path and click Next >
- Select the license type i.e. one of the evaluation license options offered, or provide the path for the commercial license if you already have got one.
- Uncheck the option to use the sample data and configurations – these are not that useful for OCSP services.
- Select SQL Server and Typical Configurations and click Next >
- Enter the connection details for the ADSS evaluation database and click Next>
- Setup now attempts to connect to the database. If this fails, check the connection details are correct, if they are then the problem is often found to be either:
  - That the IP configurations are not enabled (use SQL Server Configuration Manager)
  - That SQL Server was not installed with mixed mode authentication (it will need to be re-installed)
- Select "Typical installation" and click **Install**
- After the progress bar completes leave the default Service Settings selected and click **Finish**
- The Windows installation wizard will appear so that the ADSS Server admin key and certificate can be installed in the browser. The certificate allows an administrator to securely login to the ADSS Admin Console over an SSL/TLS session with client and server authentication. Follow the wizard instructions and install the certificate in the Windows Personal store. The password of the Default Admin certificate is: **password**. This is an initial certificate and it should be replaced once ADSS Server is running.
- After this an HTML page opens in the default web browser providing a link to the ADSS Admin Console. Click on this link if using Internet Explorer. If using Firefox then you must browse to https://localhost:8774/adss/console to log into the ADSS Admin Console Firefox also wishes to see the keys and certificates in its local trust store.
  - The browser will indicate that the server certificate is not trusted – this is because a temporary certificate is used by ADSS Server at this time that can be changed later and trusted for production use. Select continue
  - If you are presented with a list of client certificates - select the one called ADSS Default Admin
- At this point ADSS Server has been successfully installed and the ADSS Admin Console can now be used to configure the ADSS Server.

The system is now ready for evaluation use and is able to run sample transactions.

In addition to the documents specified above, you should read the readme.html documents in the ADSS Client SDK folders for details on how to run the samples and the client-side signing "zero-footprint" Go>Sign applet based demonstrations.

ADSS Server Concept

The way we divide ADSS Server into separate services has advantages when it comes to secure management. Reading through this short description will clarify what elements need to be configured and why:

1. Business applications make signing or verification requests to ADSS Server. (Auto File Processor is an Ascertia supplied application and it can be deployed to create watched folder processing for multiple files such as PDFs, XML data and other file types. See the separate AFP guide for further information).
2. ADSS Server authenticates the application request message based on an embedded OriginatorID, with optional SSL and optional signature.
3. The request is checked for authorisation by looking at the ADSS Client Manager Interface which lists all known clients, which services they can access, which service profiles and optionally which certificates can be requested.
4. The profiles within the services define the detail of the signing, verification or certification request, for signing PDFs these define detailed attributes.
5. The Key Manager is used to control all the keys used for signing and other tasks
6. The Trust Manager is used to control the Trust Authorities including locally issued certs Global settings are used to define the certificate templates for certificate requests, a connection to an external TSA, system integrity and other settings.

The evaluation database explained

The sample script populates the ADSS Server database with the following example data:

- **Keys and Certificates** – these are keys and certificates that are normally generated by the ADSS Admin Console under the Key Manager tab. They are selected for use by a client application during a signing, verification, certification, XKMS, OCSP, TSA, and SCVP transactions with ADSS. See the ADSS Admin Manual, Key Manager section, for further details.
- **Trusted CA** – this is a trust anchor certification authority that is normally configured by ADSS Admin Console under the Trust Manager tab and additionally under the Verification Service/Registered CA menu. It is used as a trust point (Trust Anchor) when a digital signature is being verified. See the ADSS Admin Manual Trust Manager and Verification Service Step 2 sections for further details.
- **Client's Originator ID** – this the ID that the client application uses to verify to the ADSS Server that it is authorised to communicate with ADSS, and which services are available to that application. It is normally configured under the ADSS Admin Console, Client Manager tab and additionally under the Verification Service/Client Manager Menu. See the ADSS Admin Manual Client Manager and Verification Service Step 4 for further details.
- **Signing Profiles** – these profiles determine for a particular ADSS signing transaction what type of document is to be signed, where the signature is to be placed on the page, the look of the signature and other signature information. It is normally configured by the Signing Service/Signing Profiles menu. See the ADSS Admin Manual Signing Service section for further details.
- **Signature Appearance Profiles** – these profiles determine how exactly the signature appearance fields are shown in the visible signature on signed PDF files. Operator can also specify whether to show or hide specific signature appearance fields.
- **Certification Profiles** – these profiles determine for a particular ADSS certification transaction, which CA is to be used (local or external) and the characteristics of the key that is to be generated for certification. It is normally configured by the Certification Service/Certification Profile menu. See the ADSS Admin Manual Certification Service section for further details.
- **Verification Profiles** – these profiles determine for a particular ADSS verification transaction, which type of signatures can be verified. It is normally configured by the Verification Service/Verification Profile menu. See the ADSS Admin Manual Verification Service section for further details.
- **TSA Profiles** – these profiles determine for particular timestamp request, which TSA certificate should be used to generate the timestamp token and some other settings for the timestamp transactions. It is normally configured by the TSA Service/Registered TSA Profile menu. See the ADSS Admin Manual TSA Service section for further details.
- **XKMS Profiles** – these profiles determine for a particular XKMS certificate validation request, which Trust Anchors to use, which path discovery and path validation mechanisms to be used for the service requests. It is normally configured by the XKMS Service/XKMS Profile menu. See the ADSS Admin Manual XKMS Service section for further details.
- **SCVP Policies** – these policies determine which Trust Anchors and path discovery and path validation mechanisms should be used for SCVP service requests. It is normally configured by the SCVP

Service/Validation Policies menu. See the ADSS Admin Manual SCVP Service section for further details.

- **LTANS Profiles** – these profiles determine for particular data archive requests, how the archived data should be produced, how the archived information should be stored, renewed and restored. It is normally configured by the LTANS Service/LTANS Profile menu. See the ADSS Admin Manual LTANS Service section for further details.

Troubleshooting the ADSS Server

If problems arise when installing or running ADSS Server then please check the following:

- **Failed to connect to the database when installing ADSS Server** – if ADSS Server setup wizard is unable to connect to the database then check that:
  - The database connection details are correct
  - The database server is up and running
  - The database user has sufficient access privileges
- **Failed to install ADSS Server using a new database** – if you are unable to install ADSS Server when using a new database then check that:
  - The database for ADSS Server has already been created
  - The same database has not been used for an earlier installation of ADSS Server
  - The database user has sufficient access privileges on the selected database
- **Unable to access the ADSS Server console** – if ADSS Server console is not accessible after installation then check that:
  - The default client authentication certificate i.e. ADSS Default Admin is installed in Internet Explorer personal key store of the Windows desktop being used
  - The appropriate default client authentication certificate i.e. ADSS Default Admin is being selected when accessing ADSS Server console
  - The ADSS Server Windows service is started and is running
  - The database service is started and is running. Re-start ADSS Server Windows service if database server goes down while ADSS Server was running (especially if testing on XP).
- **Unable to run sample programs in the Client SDK** – If you are unable to run the sample programs within the Client SDK then check that:
  - The loading of the database samples was requested during ADSS Server installation
  - Login to ADSS console and confirm that the sample profiles and data have been successfully populated within the ADSS Server.
  - The ADSS Server Windows service has been restarted and is running

Product Notes

1. The evaluation version of ADSS Server only allows up to 100 signing operations, 100 verification transactions. The number of keys that can be generated and certified is limited to 20. The number of Trust Authorities and clients that can be registered is also restricted.
2. Ascertia can provide free phone based assistance, paid onsite assistance, training and additional services for the ADSS Server.
3. There are a number of ways of using ADSS Server to suit a variety of business needs for enhanced sign-off, approval, traceability and accountability – speak to Ascertia or your local partner for further relevant information on how ADSS Server can meet your needs.

Contact Details

For Commercial Sales: +44 (0) 203 633 1177, sales@ascertia.com

For Technical Support: support@ascertia.com