



A Quick Guide for ADSS TSA Server

This document aims to provide a quick '*do this and it works*' guide to evaluating ADSS TSA Server as an Enterprise or Infrastructure class TSA Server.

TSA Service Overview:

ADSS TSA Server provides a sophisticated RFC3161 compliant timestamp authority with features that make it suitable for deployment within a managed service environment or within an enterprise. ADSS Server includes very easy to use security management, detailed logging, detailed reporting, client authentication options and it also includes role based access control and optional dual controls for its security operators.

Key Features:

- HTTP and HTTP/S interfaces to the TSA using RFC3161 TSP
- Ability to set up multiple TSA profiles with their own TSA response signing keys/certificates
- Provides multiple policies per logical TSA
- Designed for enterprise use, multi-third party use and national or global managed services
- Can be used with internal and external trust schemes to minimise external traffic dependencies
- Provides high availability facilities by using two or more servers
- Provides a secure browser based management GUI that enforces role-based controls over operator actions enabling secure remote management. Optionally the use of dual control can also be configured
- Provides optimised internal TSA service to the ADSS signature service for long term signature creation according to ETSI and PDF standard profiles which require embedded timestamps
- Provides detailed event and transaction logging and reporting to aid help desk queries, management reporting, auditing as well as legal and regulatory compliance
- The TSA service can be configured and managed along with digital signature creation, verification, validation and certification authority services using the same underlying ADSS technology and management interface on one or multiple servers
- Supports multiple database technologies including MS SQL Server 2000/2005, Oracle 10g and PostgreSQL (ask about others).
- Supports the options of using various PKCS#11 HSMs for secure key management as well as smartcard based credentials for operator authentication
- Provides automated email and SMS alerting to warn specific system operators of key events occurring on the system

Further Information References:

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

- ADSS Server Installation Guide – detailed installation guide
- ADSS Server SQL Server 2005 / 2005 Express Installation Guide (also works with 2008)
- ADSS Server Oracle 10g Installation Guide (also works with 11g)
- ADSS Server Admin Manual – details all the administrative features. The manual is available online at the following location:
<http://www.ascertia.com/helpconsole/ADSS-Admin-Guide/default.aspx>

System Requirements:

The following requirements are for Windows operating systems. Please see the ADSS Server Installation Guide for other supported operating systems and databases, e.g. Solaris, PostgreSQL etc.

- Windows 2003 / 2008 Server (32/64) or Windows XP SP2
- Microsoft SQL Server 2005 and 2005 Express, Oracle 10g/11g, MySQL, PostgreSQL

Quick Installation and Configuration Steps:

ADSS Server can be quickly installed for evaluation purposes using the following 6 steps:

1. Install MS SQL Server and create a new, empty database
2. Install ADSS Server
3. Generate or import the Keys and Certificates for the TSA Service using the ADSS Key Manager
4. Use the ADSS Trust Manager to add the TSA certificate in the ADSS trust anchor.
5. Configure the TSA Service
6. Test the TSA Service using the inbuilt ADSS Server test feature or alternatively using Ascertia's PDF Sign&Seal product

The default installation configures ADSS Server to use its integral software crypto-libraries; however various hardware security modules (HSMs) can be supplied and used if required. For further information refer to the ADSS Server Admin Manual "Key Manager". We recommend that you contact us for advice and guidance if you configure an HSM.

Install MS SQL Server and create an ADSS Server database:

The following quick steps are for installing and configuring MS SQL Server 2005 Express. The other MS SQL Server databases have similar principles for database creation and configuration. The detailed installation and database creation steps are described in the ADSS SQL Server 2005 Express Installation Guide.

- If necessary, download and install both the Database Engine and SQL Server Management Studio Express.
 - At the time this document was written this can be done from: <http://msdn.microsoft.com/vstudio/express/sql/download/>
 - The Advanced Services downloads are **not** required
 - Ensure that **mixed mode** authentication is selected during the installation
- After installation use SQL Server Configuration Manager options SQL Server 2005 Network Configuration / Protocols for SQLEXPRESS and double-click on TCP/IP and enable all the IP addresses with TCP port set to 1433.
- Run Management Studio Express, login as "sa" using SQL Server Authentication and create a database for the ADSS Server evaluation.
- The owner of the database should be configured either as "sa" (the system administration user created during installation) or a newly created user, e.g. "ADSSdbo" with administrator permissions (note: language must be set to "English").
- Database ownership should be configured during database creation from <owner> or by right clicking on Security/Logins/<user>/properties and selecting User Mapping.
 - Note: User Mapping / role membership should be selected as db_owner and public for the ADSS Server evaluation database

Install ADSS Server:

- Extract the ADSS Server installation zip file to a target folder
 - Note: The folder path cannot have spaces so you cannot use “Program Files” or similar
- From <ADSS Installation Directory>/setup run **setup.bat** which will configure the installation files for use with the database that has been created
 - 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 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 clearly installing for the first time so select this option.
- Confirm the installation path and click Next >
- The default evaluation license path is then shown, click Next >
OR if you have been supplied with a full commercial or extended evaluation license then click browse to identify the supplied license file
- Select the Installation Mode as **Fresh configuration** (setup will initialise the **new** database created in the previous steps), click Next >
- 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:
 - a) That the IP configurations are not enabled (use SQL Server Configuration Manager)
 - b) That SQL Server 2005 Express was not installed with mixed mode authentication (it will need to be re-installed)
- Leave the default path for the logs folder 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 the default 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**.
- On some machines, ADSS Server Windows service fails to start with the error “The Ascertia-ADSS service terminated with service-specific error 0 (0x0)”. If this error is seen, then check that the file: “msvcr71.dll” is accessible to tomcat.exe on the ADSS server machine, e.g. is this available on the system path? If not, copy this file to the Tomcat/Bin folder. Tomcat v6 needs to be able to access this file during start-up.
- 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:8779/adss/console> to log into the ADSS Admin Console.
 - The browser will indicate that the server certificate is not trusted. A temporary certificate is used by ADSS Server at this time that can be changed later and trusted for production use. Select to continue
 - If you are presented with a list of client certificates to select from - 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 TSA service

Configure the TSA Service:

This quick guide deals with a simple configuration where the TSA Service is configured as a standalone Time stamp authority. Login to the ADSS Admin Console and follow these steps to configure the TSA Service:

- Select the Key Manager top menu and then the Key Manager side menu
- Generate a new Timestamp response signing key by clicking New, supplying the key alias information and a purpose as Timestamp Response Signing from the Purpose drop down - Click **OK** Check the radio button for the key now identified by the key alias entered in the previous step and click Certificates
- Either: (a) Click the Create Self-Signed Certificate and enter certificate details to create a self-signed TSA certificate to generate timestamp tokens
OR: (b) Click the Create PKCS#10 button and enter the certificate request details to be certified by an external CA. See the ADSS Server Admin Guide for further details. The certificate generated by the CA can be imported into ADSS Server by clicking the Import button on the certificates screen.
OR: (c) If you have an existing key to be used as timestamp authority then you can also import this existing key by using Import key button. Provide a key alias, certificate alias the path to the timestamp authority key with the relevant password and select the purpose as Timestamp Response Signing from the purpose drop down.
- Select the Trust Manager from the top menu
- Click the New button and enter an arbitrary Friendly Name for the TSA certificate which shall be used to generate timestamp tokens “browse” to import the certificate of this TSA
- Check the registration purpose as Time Stamping Authority (will be used to verify timestamp responses), click on Finish button
- Select the TSA Service top menu and then the Registered TSA Profiles side menu
- Provide a TSA profile Friendly Name, a TSA policy ID and the value for timeout
- Select to use In-built TSA and select a Timestamp Authority (TSA) certificate from the drop down. Select the alias for the certificate generated in above steps.
- Select a hashing algorithm, default is SHA-1 and click on the Insert button
- Restart the Windows service called “Ascertia-ADSS” to accept the trust manager settings changes and TSA configuration data
- Click on the management reporting option – this will provide high level or detailed reports of the TSA requests processed

The system is now installed and ready to process TSA requests

The Ascertia PDF Sign&Seal product and the ADSS Server > Global Settings > Timestamping module can be used to test the TSA service as described below

Testing the TSA Service:

Using Ascertia PDF Sign&Seal product:

- Download an evaluation version of PDF Sign&Seal from the Ascertia website
- Install the downloaded setup
- Run the application in the trial mode
- Open the Long-Term Signature Generation dialog in the Preferences (i.e. Tools > Preferences > Signature > Long-Term Signature Generation)
- Enable the option “Embed Time stamp (RFC3161 based) when signing
- Click on the “Add” button
- Enter the ADSS Server name and the TSA service address of the ADSS Server (i.e. <http://localhost:8777/adss/tsa>)
- Click on the “Test” button
- If the TSA service is properly configured and proper addresses are enter, then the response shall be “Successfully received Timestamp token”

Using ADSS Server Global Settings:

- Select the top menu **Global Settings** and sub menu **Timestamping**, click on **New** button
- Provide the ADSS TSA server address i.e. <http://localhost:8777/adss/tsa>, the TSA policy ID if this is required and a value for the TSA response timeout
- Optionally select the options to Include Nonce and Require Certificates and click OK button
- On the Global Settings > Timestamping page, select the TSA server and click on Test TSA button
- If the TSA server is configured successfully then the response message will be "Time Stamp Authority (TSA) connected successfully"

Troubleshooting ADSS Server:

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

- **Failed to connect to 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 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 process TSA requests**
 - Check the ADSS Server Windows service is started and is running
 - Check that the ADSS TSA service is running, by logging into the ADSS console and clicking on the TSA Service Manager.
 - Check the URL and port number for the server and client

Product Notes

- 1) The evaluation version of ADSS Server only allows up to 1000 TSA transactions within 30 days of the evaluation period starting from the day of installing the ADSS Server. 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 also provide a TSA Crusher client tool product which allows administrators to assess the performance of their TSA server(s). This tool sends a configurable batch of timestamp requests to the server and then monitors the time taken for the server to respond to these. Contact us for further info on this product.
- 3) Ascertia can provide free phone based assistance, paid onsite assistance, training and additional services for the ADSS Server.

Contact Details

For Commercial Sales: Rod Crook on +44 (0) 1256 895416, rod.crook@ascertia.com
For Support: email support@ascertia.com