



ADSS TSA Server

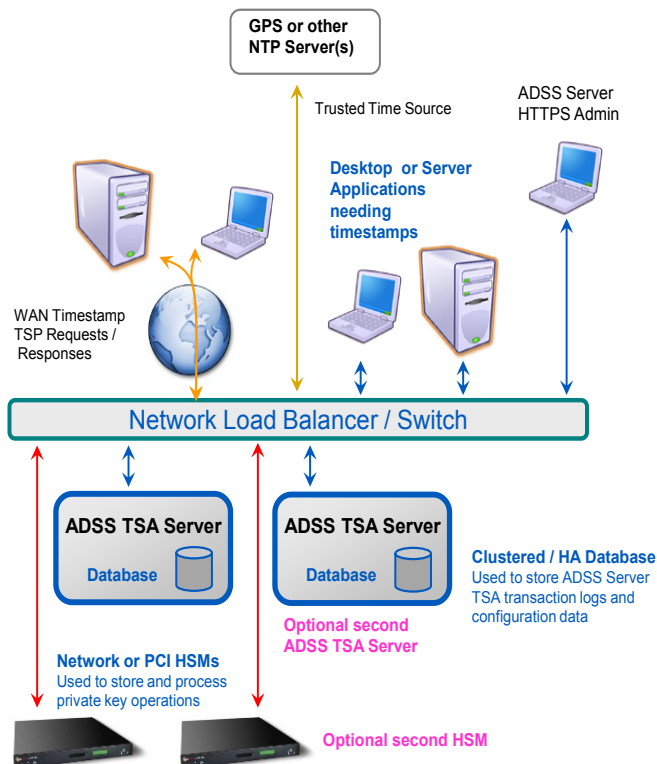


The Ascertia ADSS TSA Server provides independent and irrefutable proof of time for business transactions, e-documents and digital signatures. It can be used to create legal weight evidence that business transactions occurred at a defined moment in time, it can be used to notarise documents and data that they have not been altered since that date/time. It can also independently prove when a digital signature was applied or was accepted so that its validity can be verified even after the expiry or later revocation of a signer's certificate.

ADSS TSA Server complies with the IETF RFC3161 specifications and satisfies ETSI TS 101 861 and TS 102 023 requirements for TSA services. It can be used for internal enterprise TSA needs or used to provide infrastructure-class commercial TSA services to multiple external parties. The underlying technology for ADSS TSA Server is Ascertia's well-proven ADSS Server, which provides a range of trust services from digital signing, centralised signature verification and certificate validation, notarisation/archiving and key management services, all from the same secure platform.

Many TSA products do not provide adequate management facilities to allow effective commercial services to be offered. ADSS TSA Server uses Client SSL authentication to check the identity of the requestor and authorise access to the timestamp service. All timestamp requests and responses are stored in the tamper-evident server transaction logs. These logs provide good information for commercial accountability purposes and to meet any legislative or regulatory requirements for timestamp preservation as well as providing effective evidence for normal dispute resolution processes.

| Why use ADSS TSA Server | |
|-------------------------|---|
| ➔ | A highly effective, flexible Time Stamp Authority server designed for use as an Enterprise TSA or as a high volume commercial service TSA |
| ➔ | Can be deployed as a dedicated TSA server or a Virtualised TSA service. |
| ➔ | It can enforce strong requestor authentication using SSL client certificates to ensure that only subscribing users or organisations access the service. |
| ➔ | It retains timestamp tokens that are issued to support business needs to keep these for legislative or regulatory demands or simply as evidence to simplify dispute resolution processes. |
| ➔ | It supports strong signing algorithms: RSA 1024, 2048, 4096, ECDSA 192, 256, 384, 521 |
| ➔ | It supports strong hash algorithms currently SHA-1 and SHA-2 (256,384,512) and RipeMD. |
| ➔ | It supports FIPS 140-2 and CC EAL4+ HSMs. |
| ➔ | It provides detailed transaction logs, with effective viewing, searching, reporting and archiving options. |
| ➔ | It offers a human-readable transaction viewer for all timestamp protocol requests and responses. |
| ➔ | It supports multiple TSA profiles within a single server, each with own TSA keys and certificates. |
| ➔ | It is easy to install, configure and manage using secure web-browser management screens. |
| ➔ | It offers strong role-based access controls for administrators and features optional dual controls. |
| ➔ | It can monitor trusted NTP Servers and can this monitor server time drift and alert operations staff to time issues and if necessary stop the service. |
| ➔ | It provides system event & operator activity logging. |



Configuration Options

PCI(e) HSMs can be used with dedicated Windows or Linux servers

Networked HSMs can be used with Virtualised servers

To meet high availability requirements use two ADSS TSA Servers

ADSS TSA Server can be used as a management proxy for other TSAs

Key Features

Accountability: Timestamp requestors can be authenticated and specific reports can be produced based on requestor activity within a defined date range for commercial purposes. ADSS TSA Server provides detailed reports on authorised usage and also records the timestamp tokens issued.

Proven Technology: ADSS TSA Server uses the well proven ADSS Server to deliver the underlying platform features such as optional dual controls, secure web-based management screens, event logging, trust anchor management, key and certificate management, secure logging and reporting as well as support for HSMs.

Interoperability: ADSS TSA Server has been designed to work with a variety of timestamp clients, including Ascertia PDF Sign&Seal, PDF Signer Server, XML Signer Server, File Signer Server and third party products including Adobe® Acrobat®.

High-Availability: ADSS TSA Server can be easily implemented as a highly available service to meet demanding service level agreement needs. Multiple servers can work in parallel using standard load-balancing techniques and a resilient secondary site can also be established. Network HSMs, system platforms and database management systems can be used as required to meet availability requirements.

Flexible Trust Model: Timestamp server's keys can be self-certified, or a delegated certificate can be issued by an inbuilt CA module or external CA.

TSA Management: ADSS TSA Server has been designed to provide management services for back-end TSA servers. In this capacity it authenticates end-user requests and records all transactions for report generation and billing purposes. The interaction with back-end TSA servers is invisible to end-users.

TSA Proxy: Ascertia can optionally provide a local TSA proxy to enable end user or server systems to use a centralised requestor on behalf of the organisation. A client SSL certificate is used to allow the requests to be authenticated by the ADSS TSA Server.

Maximum Security: Timestamp services can be provided over SSL/TLS with client authentication, Operator access is also controlled with client certificates. Keys can be managed inside a secure FIPS approved HSM. Logs are tamper-evident. Dual control over operator actions is a supported option.

Multiple Instances: A single installation of ADSS TSA Server can run multiple TSA profiles each with their time stamping policy and with unique signing keys (e.g. for internal and external communities).

High Performance: ADSS TSA Server has been designed for high throughput and can be used in a load-balanced configuration.

Test Tools: TSA Crusher is licensed separately to check TSA performance. TSA Monitor is in R&D for continuous availability monitoring.

This screenshot shows the detail from just one of the management screens, in this case the transaction log viewer for the Timestamp Service.

As can be seen there are sophisticated options for filtering and searching as well as English language detail screens for the viewing the Timestamp protocol request and response messages and the TSA certificate.

| Timestamp Service > Transactions Log Viewer | | | | | | | | |
|--|-----------------|-------------------------|-------------------------|-------------|---------------|----------------------|----------------------|--------------|
| Showing page 1 of 5 | | | | | | | | |
| Order by: <input type="text" value="Log ID"/> <input type="text" value="Descending"/> <input type="text" value="Current"/> <input type="button" value="Go"/> | | | | | | | | |
| <input type="button" value="Clear Search"/> <input type="button" value="Search"/> <input type="button" value="k"/> <input type="button" value="<"/> <input type="button" value=">"/> <input type="button" value=">I"/> <input type="button" value="Export Logs"/> | | | | | | | | |
| Log ID | Response Status | Request Time | Response Time | Policy ID | Originator ID | Request/Response | TSA Cert | Forwarded To |
| 45 | 0 | 2007-09-05 19:58:29.767 | 2007-09-05 19:58:29.94 | 1.2.3.4.5.6 | 192.168.0.156 | View | View | |
| 44 | 2 | 2007-09-05 17:15:42.987 | 2007-09-05 17:15:43.047 | | 192.168.0.151 | View | View | |
| 43 | 0 | 2007-09-05 16:48:58.537 | 2007-09-05 16:48:58.647 | 1.2.3.4.5.6 | 192.168.0.25 | View | View | |
| 42 | 0 | 2007-09-05 16:30:10.42 | 2007-09-05 16:30:10.437 | 1.2.3.4.5.6 | 192.168.0.156 | View | View | |
| 41 | 0 | 2007-09-05 16:24:04.85 | 2007-09-05 16:24:04.867 | 1.2.3.4.5.6 | 192.168.0.156 | View | View | |
| 40 | 0 | 2007-09-05 16:20:34.663 | 2007-09-05 16:20:34.663 | 1.2.3.4.5.6 | 192.168.0.156 | View | View | |
| 39 | 0 | 2007-09-05 16:02:19.453 | 2007-09-05 16:02:19.673 | 1.2.3.4.5.6 | 192.168.0.156 | View | View | |
| 38 | 0 | 2007-08-29 18:51:40.067 | 2007-08-29 18:51:40.177 | 1.2.3.4.5 | 192.168.0.25 | View | View | |
| 37 | 0 | 2007-08-29 18:45:09.657 | 2007-08-29 18:45:09.847 | 1.2.3.4.5 | 192.168.0.25 | View | View | |
| 36 | 0 | 2007-08-29 18:20:45.107 | 2007-08-29 18:20:45.297 | 1.2.3.4.5 | 192.168.0.25 | View | View | |

ADSS TSA Server Standards Compliance:

Timestamp standard: RFC 3161 ETSI TS 101 861 and TS 102 023, Time Stamp Protocol (TSP) as specified in RFC3161
PKI standards: PKCS#10, PKCS#7, PKCS#11, SSL/TLS
For use with: Timestamped signatures, long term signatures to ETSI PAdES, XAdES, CAAdES, LTANS archiving
Platforms: Windows 2003 / 2008 Server, Linux 32 and 64 bit variants, Solaris 10 (Sparc and x86)
Databases: SQL Server 2005 / 2008 (and Express), Oracle 10g, 11g, PostgreSQL 8, MySQL 5
HSMs Network connected or PCI(e) HSMs form SafeNet, Thales nCipher, Utimaco, AEP and others

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
 © Copyright Ascertia Limited 2011. All Rights Reserved, E&OE