ADSS TSA Server

RFC 3161, 5816 and Authenticode timestamps

ADSS TSA Server is a well-proven, standards-based product that can be deployed on premise or as part of a cloud service. It offers high throughput and high availability, scalable to meet the most demanding needs. As a strategic product for Ascertia, it offers support for the latest Windows and Linux operating systems, databases and HSMs from the major vendors.

Timestamping Overview

Time Stamp Authority (TSA) servers are used to provide evidence that a document and any signatures existed at a defined moment in time. Timestamps make it mathematically infeasible to then manipulate the data, document, any fields or annotations or the signature and that are protected by the timestamp signature.

Digital signatures provide authenticity and integrity for digital documents, electronic messages, transactions, and software. So while digital signatures confirm who signed the data, timestamps confirm which trusted TSA witnessed and signed the data hash. TSA Servers normally have a much longer-lived certificate than the signer's certificate and so protect the document or data even after the expiry or any subsequent revocation of a signer's certificate. Additional timestamps can also be added to secure data into the distant future.

When verifying long term signatures the timestamp provides a trust date/time reference for the embedded OCSP and/or CRL data used to prove that the signer's certificate was valid at the timestamped time.

The increasing use of signed PDFs and signed evidential data is driving the need to use trusted digital timestamp services ensure that this data and associated signatures can be trusted for months and years into the future.

Ascertia is tracking the latest developments such as the SHA-3 hash and Quantum Safe signature algorithms and ADSS TSA Server will feature these in near term releases.

ADSS TSA Server uses RFC 3161 protocols to receive a hash, it generates a time stamp token, returns this to the business application, which then stores this with the data being signed, business applications can submit a document to a timestamp to refresh the timestamp on a regular basis in order to provide long term archival of a document.

Ascertia ADSS TSA Server is unmatched in this area.

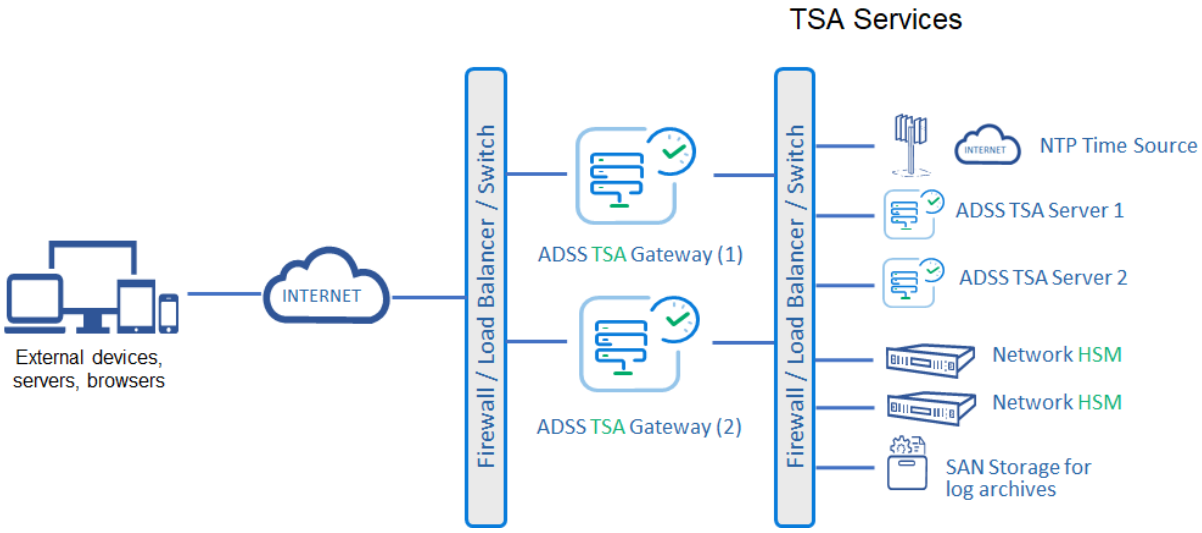
Key Features

- **High Performance:** A single ADSS TSA Server can produce thousands of timestamps per second.
- **Standards Compliance**: Fully compliant with RFC 3161 and RFC 5816, satisfies the Time Stamp Profile ETSI EN 319 422 V1.1.1 (2016-03) (formerly ETSI TS 101 861 V1.2.1 (2002-03)).
  Used for Qualified Timestamps and also AATL timestamps.
- **Interoperability**: ADSS TSA Server works with any RFC 3161, 5816 or Microsoft Authenticode compliant client including Microsoft Office and Adobe Acrobat.
- **Cryptography Support**: Supports strong signing & hash algorithms:
  - RSA 2048, 3072, 4096, 8192
  - ECDSA 256, 384, 521
  - SHA-256, SHA-384, SHA-512 and others
- **High-Availability**: ADSS TSA Server is well proven at offering high throughput, high availability and scales to meet the most demanding business needs.
- **Virtual TSAs:** A single instance 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).
- **CWA 14167-1 Compliant:** Meets the requirements for trustworthy systems including strong role-based access controls, optional dual controls, detailed and secure transactional, system event & operator activity logging.
- **NTP Support:** Works with Stratum2 & 3 NTP servers and GPS NTP Servers to ensure accurate, trusted time

ADSS TSA Server Architecture

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 it can be verified even after the expiry or later revocation of a signer's certificate.

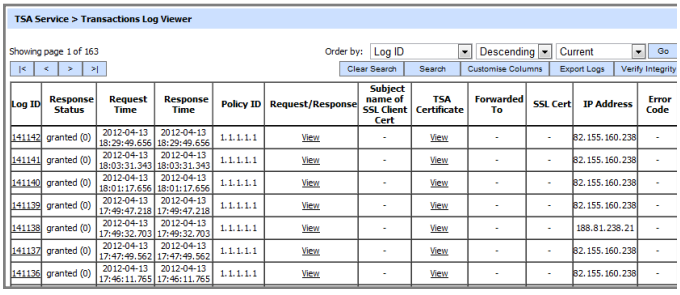
ADSS TSA Server complies with the IETF RFC 3161 and 5816 specifications and satisfies ETSI EN 319 422 V1.1.1 (2016-03) (formerly ETSI TS 101 861 V1.2.1 (2002-03)) and ETSI EN 319 421 V1.0.0 (2015-06) (formerly ETSI standard TS 102 023 V1.2.1 (2003-01)) requirements for TSA services. Microsoft Authenticode is also supported. It meets all requirements for an internal enterprise TSA or to power world-class commercial TSA services to multiple third 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 CWA 14167-1 certified product.



Ease of Use

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.


TSA Service > Transactions Log Viewer

Showing page 1 of 163 — Order by: Log ID — Descending — Current — Go

|< < > >| — Clear Search — Search — Customise Columns — Export Logs — Verify Integrity

Log ID	Response Status	Request Time	Response Time	Policy ID	Request/Response	Subject name of SSL Client Cert	TSA Certificate	Forwarded To	SSL Cert	IP Address	Error Code
141142	granted (0)	2012-04-13 18:29:49.656	2012-04-13 18:29:49.656	1.1.1.1.1	View	-	View	-	-	82.155.160.238	-
141141	granted (0)	2012-04-13 18:03:31.343	2012-04-13 18:03:31.343	1.1.1.1.1	View	-	View	-	-	82.155.160.238	-
141140	granted (0)	2012-04-13 18:01:17.656	2012-04-13 18:01:17.656	1.1.1.1.1	View	-	View	-	-	82.155.160.238	-
141139	granted (0)	2012-04-13 17:49:47.218	2012-04-13 17:49:47.218	1.1.1.1.1	View	-	View	-	-	82.155.160.238	-
141138	granted (0)	2012-04-13 17:49:32.703	2012-04-13 17:49:32.703	1.1.1.1.1	View	-	View	-	-	188.81.238.21	-
141137	granted (0)	2012-04-13 17:47:49.562	2012-04-13 17:47:49.562	1.1.1.1.1	View	-	View	-	-	82.155.160.238	-
141136	granted (0)	2012-04-13 17:46:11.765	2012-04-13 17:46:11.765	1.1.1.1.1	View	-	View	-	-	82.155.160.238	-

Advanced Features

Secure Logging: Every request and response is securely logged to enable operators to quickly review transactions in detail and resolve issues in minutes.

TSA Gateway: 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.

Performance Tuning: ADSS TSA Server provides the ability to fine tune the deployment to make best use of the platform on which the product is operating, this in turn enables organisations to tune TSA performance to meet the needs of their business.

Advanced Features (Cont.)

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.

Management Control and Reporting: Detailed role-based access controls make it easy to give staff the rights they need, for instance allowing help-desk staff to access log information so they can help customers whilst ensuring that they cannot view or change any configuration data.

ADSS TSA Server creates detailed event and transaction logs that can be used to create usage reports and identify high demand users, certificates or IP addresses. Advanced management reporting is provided as a standard feature.

Ease of deployment: ADSS TSA Server can be installed in minutes and quickly configured to offer effective timestamp services for a wide variety of needs. It provides very high throughput even using long-length keys and certificates and whilst providing detailed logging for later management analysis.

All timestamp requests and responses are stored in secure sequenced transaction logs. These 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 and for any technical issue resolution.

High availability deployment: Primary and secondary datacenters can be used to ensure continuous availability of TSA Servers.

ADSS TSA Server is an advanced Timestamping Server that supports multiple TSA policies, provides role based operator access controls and high availability configurations.

Secure web-based management is provided as standard together with advanced management configuration options and detailed reporting.

Supported Operating Systems:

Microsoft Server 2019, 2016, 2012 R2
Linux RedHat, SUSE, CentOS, Ubuntu

Supported Databases:

Microsoft SQL Server 2019, 2017, 2016
Oracle 19c, 18c, 12c
Azure SQL Database (Database-as-a-service)
PostgreSQL 12, 11, 10
MySQL 8, 5
Percona-XtraDB-Cluster 5

Supported Security Modules

Thales Luna and Protect Server
Entrust nShield
Utimaco SS & CS CP5
Microsoft Azure Key Vault
Amazon AWS Cloud HSM (Linux Only)

Mike Hathaway | Chief Technology Officer

For more info
info@ascertia.com
www.ascertia.com