ADSS LTANS Server

LTANS Evidence Archive Services

ADSS LTANS 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.

Long-Term Archive & Notary Services Overview

Long-Term Archive and Notary Services (LTANS) servers are used to securely archive digital documents so that they may be protected and accessed in the future.

Business that operate in highly regulated industries, such as health care, law enforcement, financial services etc. are required to store documents, photos and evidence of a transaction taking place for many years.

When signing paper documents you implicitly trust the fact that the signature will be verifiable for several years into the future, however storing many years of paper documents requires storage facilities which can consume vast amounts of space and become very costly.

In the digital world the selection of files that need to be archived increases far beyond that of the traditional world and business need to look at how to provide long term archival services for many file types, in order to comply with internal policies, external regulation or legislative requirements, digital documents need to be verifiable for at least 7 to 10 years into the future. Strong security measures are required to ensure that the data can be proven to be both original and unchanged from the time of creation or, at the very least, from the time it was archived. This is done using RFC 4998 XMLERS security.

Ascertia ADSS LTANS Server is unmatched in this area

Key Features

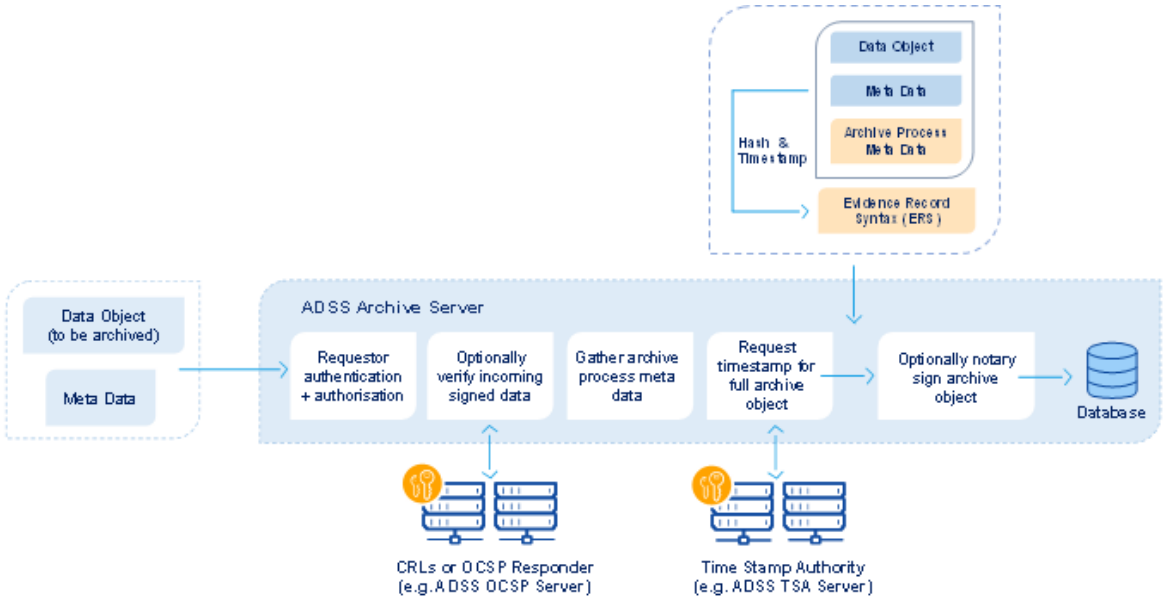
- **Interoperability and Flexibility:** Support for multiple archive profiles for different business requirements or document types and offers flexible retention policies, including the option of auto-deleting archive objects at the end of their retention period
- **Standards Compliance**: Fully complaint with RFC 4998 XMLERS. Documents can be protected through the entire archive period using secure timestamps (RFC 3161 and RFC 5816).
- **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 LTANS Server can be built to leverage various platforms using HSMs from various vendors, multiple internal or external TSAs and CAs.
- **Integrations:** Multiple integration options are supported including a high-level client API in Java and .NET driving HTTP and web-service protocols as well as ADSS AFP based watched folder processing
- **High Security**: Provenance data can be retained within the evidence record; existing signatures can have the verification information saved with the archived object and notary signatures can be applied to the archived object as an option and evidence records can be exported for independent storage or review

ADSS LTANS Server Architecture

ADSS Archive Server is a well-designed modular product that has the flexibility to enable the rapid deployment of an enterprise solution OR an infrastructure class Managed Service Provider solution for use by multiple organisations.

The advanced JEE architecture ensures support for load-balancing, high-availability and performance across multiple platforms.

Long-Term Archive and Notary Services (LTANS) protection is an action that can be taken at any stage of a business process, either just before sending documents out of an organisation or immediately after receiving documents. The following diagram illustrates the internal processes and how the Evidence Record Syntax (ERS) datafile is created



Supported Archive Services

This ADSS Archive Server supports these services:

- Archiving services for any type of data object – offers the ability to store the archive object in the trusted archive database or pass the archive object back to a Document Management system
- Export Services – offers the ability to export data objects out of the archive. Only suitably authorised trusted clients can request export services
- Retention and Deletion Services – offers the ability to delete objects from the trusted archive. Only suitably authorised trusted clients can request data deletion.

Archive Profiles

Multiple archive profiles can be configured and business applications can then be assigned these profiles to meet business requirements. Archive profiles provide options for:

- The archive retention period, i.e. how long the object will be saved in the archive
- What happens to the object once the retention period is reached (i.e. automatically deletion)
- Whether to Notary sign the archive object and if so which digital signature key/certificate to use
- When to renew the timestamp evidence which protects the archive object from untraceable manipulation, options include:
  - At fixed intervals, e.g. every 15 years
  - A certain period before the expiry of the current archiving timestamp
  - Based on operator action
- Which Time Stamp Authorities (TSAs) to request timestamps from

Usage Scenarios

ADSS Archive Server can be used as a secure long-term archive for any de-materialised business process:

- Secure archive of outgoing business documents and records, providing a permanent evidential record of what was sent
- Secure archive for incoming documents, so that any disputes about the data can be swiftly and clearly dealt with
- Securing internal documents, as in today's litigious society, businesses need trustworthy evidence to pursue supplier/ customer/ employee legal action.

Organisations requiring such systems include the health sector, insurance firms and government departments dealing with citizen information, digital libraries, law firms, patent offices, forensic laboratories and others.

Financial institutions also create documents that need to be provably original for many years to come.

ADSS LTANS Server is an advanced Long-Term Archive & Notary Server that supports multiple internal or external TSA and CA's.

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

Supported Operating Systems:

Microsoft Server 2022, 2019, 2016
Linux RedHat, SUSE, CentOS, Ubuntu

Supported Databases:

Microsoft SQL Server 2022, 2019, 2017
Oracle 19c, 18c
Azure SQL Database (Database-as-a-service)
PostgreSQL 14, 13, 12, 11
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 Product Officer

About Ascertia

Ascertia provides digital trust for people, devices, data and documents for everybody from individuals to Enterprises and Governments. Ascertia's PKI and digital signature technologies serve a global customer base and partner network via direct and indirect sales channels.

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