ADSS Archive Server

LTANS Evidence Archive Services

As part of complying with internal policies, external regulation or legislative requirements, certain business documents must be securely archived for a number of 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.

ADSS Archive Server offers these capabilities for any document type including PDF, Office and other files such as legal, financial, personnel, safety and even engineering drawings or project plans. All files, zip files and other data can be archived - the business simply needs to decide which documents need to be archived and under which archive policy.

The business need for secure archiving

The reasons for creating a secure archive include:

- **Proving compliance and for dispute resolution:** A trusted archive of documents can be independently proven to be original and unchanged using financial strength digital signatures and timestamps
- **Proving existence, authenticity and integrity:** Patents and other legal processes require evidence as to the trustworthy proof of the existence and integrity of data at a particular moment in time
- **Future proofing for 10 to 100 years and more:** To provide long-term protection of important documents beyond the validity period of current digital signatures and timestamps and beyond the lifetime of current cryptographic algorithms
- **Cost savings:** Using an electronic archive creates a substantial ROI as business processes migrate from expensive paper-based archive systems with time-consuming and error prone searching capabilities

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.

Why use ADSS Archive Server

- It protects documents through the entire archive period using secure timestamps (RFC 3161). The input data can be of any format and can be signed or encrypted
- It supports multiple archive profiles for different business requirements or document types
- It offers flexible retention policies, including the option of auto-deleting archive objects at the end of their retention period
- It automatically refreshes the timestamp evidence information based on a configured archive profile
- It supports today's strong algorithms including SHA-256, SHA-512, RSA 2048, 4096 and 8192, ECDSA 256, 384, 521 and enables algorithm flexibility for the future beyond these
- Provenance data can be retained within the evidence record; existing signatures can have the verification information saved with the archived object
- Notary signatures can be applied to the archived object as an option and evidence records can be exported for independent storage or review
- Business applications are securely authenticated using SSL client certificates or signed web services
- 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
- It securely authenticates system operators and provides role-based access control and optional dual controls for higher levels of security.
- It securely logs all archive request/response transactions in secure tamper-resistant logs. Also logs all operator actions and system events in secure and searchable logs
- High availability and high scalability solutions can be built on various platforms using HSMs from various vendors, multiple internal or external TSAs and CAs

ADSS Server - High Trust Archive Services

Supported Archive Services

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

Enterprise 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.

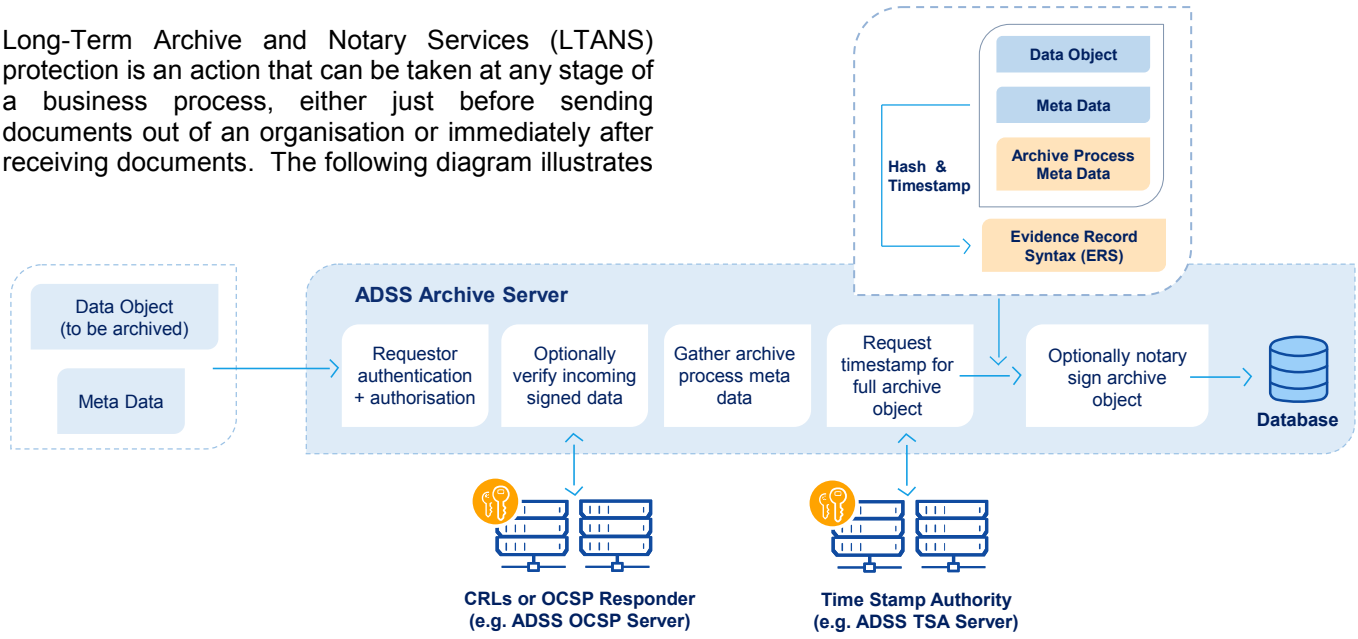
The advanced JEE architecture ensures support for load-balancing, high-availability and performance across multiple platforms.

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:

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



ADSS Archive Server Standards Compliance:	
Archive Protocol:	IETF LTANS (LTAP & XMLERS) Specifications
Signature support:	CMS signing with verification of CMS, PKCS#7, PDF, XML Dsig, ETSI XAdES and CAdES signatures
Algorithms and keys:	RSA 1024, 2048, 4096, 8192, ECDSA 256, 384, 521, SHA1, SHA-256, SHA-384, SHA-512
Certificate validation:	OCSP, CRLs
HSM support:	PKCS#11 or CAPI/CNG compliant HSMs, smartcards or tokens, Gemalto/SafeNet, Thales, Utimaco, Cloud HSMs including Azure Key Vault, Amazon AWS Cloud HSM
Systems support:	Windows Server 2016, 2012 R2, 2012, 2008 R2, Linux (RedHat, Centos, SuSe, others), Solaris
Database support:	SQL Server 2016, 2014, 2012, Oracle 12c, 11gR2, 11g, PostgreSQL 9, 8, MySQL 5.x (Percona & Oracle), Azure SQL
Interfaces:	XML/SOAP messaging (including over SSL/TLS), Java and .NET APIs, with large file handling
Options:	Other ADSS Server modules can be used to provide advanced trust services, e.g. TSA, Signature Verification

Ascertia Limited
Web: www.ascertia.com
Email: info@ascertia.com
Tel: +44 203 633 1177
40 Occam Road, Guildford, Surrey, GU2 7YG, UK

Signed by: Rod Crook
Signed at: 2017-11-14 15:52:12 +00:00
Reason: I approve this document