# Electronic Media Storage in the Context of Trusted Services

Barbora Duffalová[1], Marek Vančo[1], Juraj Hájek[2]
[1]Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava, Slovakia
[2]Ardaco, a.s., Bratislava, Slovakia
duffalova.b@gmail.com, marek_vanco@stuba.sk, juraj.hajek@ardaco.com

*Abstract* - **This paper addresses the challenges and solutions of electronic archiving within the context of trusted services as defined by European legislation, particularly the eIDAS regulation. The work outlines the theoretical background of digital preservation, including signature formats, data integrity protocols, and archival models defined by ETSI. A hybrid archiving service is proposed and implemented, integrating MinIO object storage and PostgreSQL metadata management. The modular system is designed for long-term accessibility, document integrity, and regulatory compliance. Test scenarios confirm the system's effectiveness in handling preservation operations and data retrieval. The paper also presents real implementation details and evaluates the proposed architecture's strengths and limitations in comparison with existing solutions.**

**Keywords - electronic archiving; trusted services; eIDAS; digital signature; long-term preservation**

## I. Introduction

In today's digital environment, the long-term preservation of documents is not only a matter of convenience but also a legal necessity. Organizations across the public and private sectors face growing obligations to maintain documents securely, verifiably, and accessibly over decades. Electronic archiving—paired with trusted services—offers a reliable solution to this challenge.

As the volume of electronic data increases, so do the demands on systems tasked with storing it. Traditional paper-based archives are no longer sufficient due to limitations in physical storage, retrieval speed, and legal admissibility. Electronic systems must address concerns such as data integrity, regulatory compliance, and accessibility over time.

This paper introduces a hybrid archiving system designed in accordance with the eIDAS regulation and ETSI standards. The system integrates cloud object storage (MinIO) with a relational database (PostgreSQL), ensuring flexibility, scalability, and compliance. Sections of the paper delve into theoretical underpinnings, legal frameworks, system architecture, implementation details, and performance evaluations. Throughout the text, diagrams from the author's master thesis illustrate the system's conceptual and technical foundations.

## II. Theoretical Background

Archiving is a foundational activity for legal, historical, and operational continuity. While traditional archives focused on physical media, modern systems require digital formats that guarantee integrity, authenticity, and future readability.

### A. Core Concepts

According to the Open Archival Information System (OAIS) model defined by ISO 14721 [1], an effective archive must preserve not only content but also the metadata required to understand it. The model emphasizes six high-level services: ingest, archival storage, data management, administration, preservation planning, and access.
In the context of digital signatures, formats such as CAdES, XAdES, and PAdES are standardized for long-term validation. [3] These allow electronic signatures to remain verifiable even after years or decades, thanks to the use of timestamp tokens and certificate validation chains.

### B. Standards for Trusted Preservation

Several standards support trustworthy digital archiving:

- ISO 16363 – Repository audit and certification [4]
- ISO 14641-1 – Requirements for information systems managing electronic documents
- ETSI TS 119 511 – Describes preservation service models
- ETSI TS 119 312 – Lists approved cryptographic algorithms for trust services

These standards form the backbone of any compliance-focused digital archive.

### C. Existing Solutions

Several commercial and institutional systems exist for long-term electronic archiving, each with varying degrees of openness, standards compliance, and customizability.
Disig eArchive is a widely used Slovak solution that supports trusted long-term storage of electronically signed documents. It focuses on regulatory compliance and integrates with qualified timestamping and certification services. However, it functions as a closed system, limiting transparency and flexibility for institutional integration or modification.
Namirial Digital Archive offers a cloud-based archiving platform designed for eIDAS compliance. It supports multiple signature formats and provides user-friendly access controls. Nevertheless, it is a proprietary solution and may not be easily adaptable to specific institutional workflows or infrastructure [5].
Open-source solutions, such as Archivematica or DSpace, focus more on metadata management and OAIS model

implementation, often used by libraries and academic institutions. While they offer transparency and flexibility, their support for qualified trust services (e.g., eIDAS-compliant timestamping or signature renewal) is typically limited or must be integrated manually.

In contrast, the solution developed in this work emphasizes openness, modular design, and compliance with eIDAS and ETSI preservation models. It enables institutions to maintain control over their infrastructure while supporting trusted digital archiving aligned with European standards.

In broader practice, the field of long-term preservation faces several unresolved challenges. Institutions such as the Smithsonian Archives have emphasized the risks associated with proprietary file formats, media degradation, and inadequate metadata practices [6]. These technical issues are compounded by organizational and cultural barriers.

According to Giaretta [7], preservation efforts must also anticipate evolving technologies, ensure format sustainability, and support interpretability of digital objects far into the future. Duranti and Preston stress that human and institutional factors—such as the lack of long-term planning, accountability, and digital literacy—are often underestimated in preservation strategies [8].

Further analyses, such as by The ECM Consultant and CLIR (Council on Library and Information Resources), highlight the necessity of integrating legal and regulatory compliance into technological solutions [9][10]. Without a unified framework combining governance, technology, and legal safeguards, long-term trust in digital archives may be undermined.

The emergence of technologies such as blockchain and electronic ledgers opens new avenues, especially under the evolving regulatory environment shaped by eIDAS 2.0. However, these remain largely experimental due to the lack of standardized implementation procedures and clear operational models [11][12].

## III. Legal and Regulatory Framework

In the European Union, the eIDAS Regulation (EU 910/2014) defines the responsibilities and standards for electronic identification, signatures, seals, timestamps, and trusted services. [13] Among its key implications is the recognition of qualified electronic signatures as legally equivalent to handwritten ones.

### A. Trusted Services

eIDAS defines qualified trust service providers (QTSPs) and mandates strict obligations, such as cryptographic security, timestamping, and evidence preservation. Trusted archiving systems must provide:

- Data integrity verification
- Long-term signature validity
- Time-bound access logs
- Legal audit trails

### B. ETSI Preservation Models

ETSI TS 119 511 outlines three models of preservation services:

- WST (With Storage): Stores both documents and cryptographic evidence. [14]
- WTS (With Temporary Storage): Keeps hashes temporarily during processing. [14]
- WOS (Without Storage): Returns proofs without storing data. [14]

This project adopts the WST model, illustrated in Figure 1, as it offers maximum control and traceability.

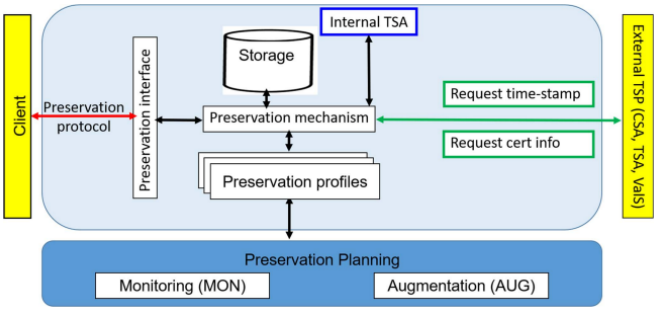


Figure 1. WST model [6]

## IV. System Design and Architecture

The proposed system is built as a modular service with a hybrid storage approach. It separates metadata management from document storage, enabling efficient indexing and reliable scalability.

### A. Hybrid Architecture

The system is built as a modular service using a hybrid approach to storage and control. As shown in Figure 2, clients interact with the system via a Preservation Protocol, which routes requests to the central Archivation Service.

At its core is the Archivation Controller, which coordinates operations across several components:

- The Archivation Service handles preservation logic and workflow management.
- The Expiration Manager enforces data lifecycle rules.
- The Signing Service secures documents with digital signatures and timestamps via a Timestamping Authority.
- The MinIO Service manages binary data storage using the S3 protocol, connecting to MinIO.
- The Persistence Service writes metadata and logs to PostgreSQL via JDBC.

This architecture ensures clean separation of logic, scalable storage, and standards-based communication with external systems.

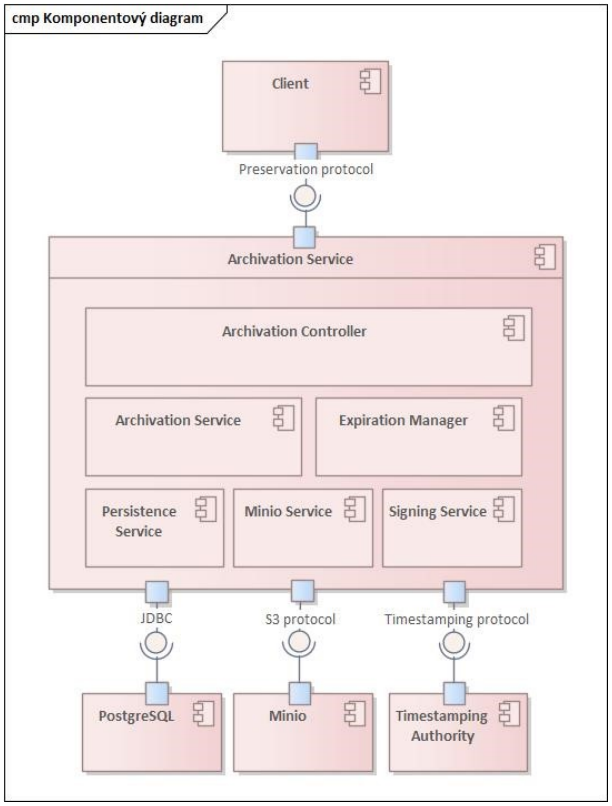


Figure 2. Component diagram of project architecture

### B. Data Flow

When a document is submitted for archiving:

- The document is encapsulated as a Preservation Object (PO).
- The Signing Service generates a signature and obtains a trusted timestamp.
- The document is stored in MinIO, while metadata is written to PostgreSQL.
- Confirmation and identifiers are returned to the client.

This approach ensures a clear separation between long-term storage and metadata management, improving performance and maintainability.

## V. Implementation

The system exposes its functionality through a RESTful API developed in Spring Boot. All endpoints are managed by the ArchivationController and documented using the OpenAPI Generator. Communication is handled in JSON format, and each operation aligns with the ETSI TS 119 512 standard. [15]

### A. API Operations

Key operations include:

- PreservePO Accepts preservation objects in Base64 format (binary or XML), along with metadata like mimeType and formatId. It returns a status response for each object processed.
- RetrievePO: Retrieves a preserved object by its poId. Returns the data or an error message if not found.
- DeletePO: Remove a document when requested based on given poId.
- RetrieveInfo: Retrieves archiving profiles based on the request attributes.

### B. Automatic Retimestamping

To ensure long-term validity of archived documents and their electronic signatures, the system implements a mechanism for automatic timestamp updating. This is necessary because cryptographic algorithms and certificates used in signatures may become obsolete or expire over time.

The Expiration Manager module monitors the validity period of each stored preservation object (PO). It tracks associated timestamp tokens and periodically checks whether a new timestamp should be applied. When a timestamp is nearing expiration—or when cryptographic policies require renewal. The system automatically requests a new timestamp from a trusted Time Stamping Authority (TSA).

The updated timestamp is then added to the metadata of the PO and stored alongside the original signature and proof. This process ensures that the document remains verifiable and compliant with ETSI TS 119 511 over long periods, even after the original certificates are no longer valid.

This timestamp updating logic helps maintain legal reliability and is an essential part of preserving the integrity and trustworthiness of archived electronic documents.

### C. User Interface

The system includes a fully functional graphical user interface (GUI) implemented in React, supported by the Material UI component library. This frontend provides users with a responsive and intuitive platform for managing archiving operations.

Users can:

- Select a preservation profile,
- Enter document identifiers,
- Upload signed files in ASiC-E format,
- Define relationships between archived objects.

The interface also offers additional tabs for retrieving and deleting previously stored documents using their identifiers. All communication between the frontend and backend is handled via a REST API built using FastAPI and deployed in a Node.js environment. The entire application is containerized with Docker, enabling scalable and efficient deployment.

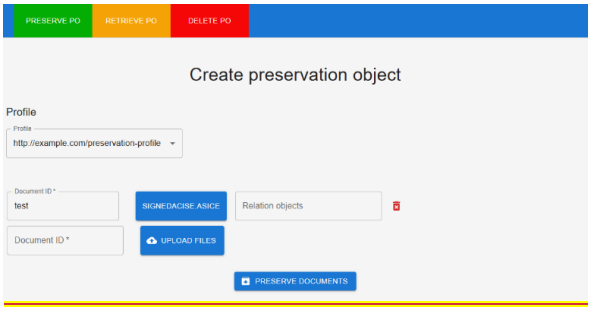


Figure 3. User Interface

### D. Testing

The system was tested using both unit tests and automated HTTP scenario tests to ensure correctness and stability.

For unit testing, the JUnit framework was used alongside Mockito and Spring Test. These tests targeted individual components of the system in isolation, verifying expected behavior and supporting regression testing. Mock objects were used to simulate interactions with services such as the database, MinIO storage, and the timestamping authority.

Postman was used for functional testing of the REST API. A collection of test scenarios was created in JSON format and executed using Postman Collection Runner. Each scenario simulated real user behavior and checked system responses using embedded JavaScript assertions. Tests covered all API operations and validated HTTP codes, response structure, and content integrity.

This multi-layered approach helped ensure implementation quality and provided a solid foundation for further development and maintenance.

## VI. Discussion

The developed archiving system fulfills its core goals of compliance, modularity, and long-term preservation. Thanks to the use of open-source technologies and standardized interfaces, the solution is cost-effective and easy to maintain.

A key strength is the modular architecture, which separates cryptographic operations, storage, and metadata management. This enables easier updates and scaling. The system also supports automatic timestamp renewal, ensuring documents remain verifiable over time.

One limitation is that only XAdES signatures are currently supported. Expanding support to include other formats like CAdES and PAdES would increase compatibility, especially for use cases involving invoices and legal documents.

### A. Potential Improvements

Several enhancements could further improve the system's robustness and usability:

- Versioning of archived documents: Adding support for storing multiple historical versions of the same document in the object store would improve transparency and enable detailed auditing. This functionality would be especially useful in environments where document revisions must be tracked over time.
- Blockchain integration: Storing cryptographic hashes of archived documents in a decentralized ledger could provide an independent, tamper-proof proof of integrity. This concept aligns with the upcoming eIDAS 2.0 regulation, which envisions qualified services based on trusted electronic ledgers [11]
- Support for additional signature formats: Currently, the system handles XAdES signatures. Extending support to CAdES and PAdES would improve compatibility with widely used formats, particularly in legal and financial sectors

These enhancements would align the system more closely with real-world institutional needs and position it for future regulatory developments.


## Acknowledgment

This paper was supported by DISIC (09I05-03-V2), NEXT (ERASMUS-EDU-2023-CBHE-STRAND-2), EULiST (ERASMUS), CYB-FUT (ERASMUS+), InteRViR (VEGA 1/0605/23).


## References


[1] ISO 14721:2012. *https://www.iso.org/.* [Online] 2012. https://www.iso.org/standard/57284.html.

[2] ISO 19005-1:2005. *https://www.iso.org.* [Online] 2005. https://www.iso.org/standard/38920.html.

[3] etsi.org. ETSI TS 119 511 V1.1.1. [Online] 2019. https://www.etsi.org/deliver/etsi_ts/119500_119599/119511/01.01.01_60/ts_119511v010101p.pdf.

[4] ISO 16363:2012. *https://www.iso.org/.* [Online] 2012. https://www.iso.org/standard/56510.html.

[5] Taurisano, Antonio. Namiral. namiral.com. [Online] 22. 5 2024. https://www.namirial.com/en/inspiration/the-rise-of-intelligent-trust-services.

[6] Smithsonian Institution Archives. Digital Preservation Challenges and Solutions. [Online] https://siarchives.si.edu/what-we-do/digital-curation/digital-preservation-challenges-and-solutions

[7] Giaretta, David. Advanced Digital Preservation. Springer, 2011.

[8] Duranti, Luciana and Preston, Randy. Records Management and Information Culture: Tackling the People Problem. Chandos Publishing, 2015.

[9] The ECM Consultant. 10 Challenges of Digital Preservation. [Online] https://theecmconsultant.com/challenges-of-digital-preservation

[10] Thibodeau, Kenneth. Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years. CLIR. [Online] https://www.clir.org/pubs/reports/pub107/thibodeau

[11] European Union (2024). eur-lex.europa.eu. [Online] https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng.

[12] European Commission. eIDAS 2.0 – A Toolbox for a European Digital Identity Framework. [Online] https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

[13] etsi.org. ETSI TS 119 511 V1.1.1. [Online] 2019. https://www.etsi.org/deliver/etsi_ts/119500_119599/119511/01.01.01_60/ts_119511v010101p.pdf.

[14] European Union. digital-strategy.ec.europa.eu. [Online] 2014. https://digital-strategy.ec.europa.eu/sk/policies/eidas-regulation.

[15] etsi.org. ETSI TS 119 512 V1.1.1. [Online] 2020. https://www.etsi.org/deliver/etsi_ts/119500_119599/119512/01.01.01_60/ts_119512v010101p.pdf