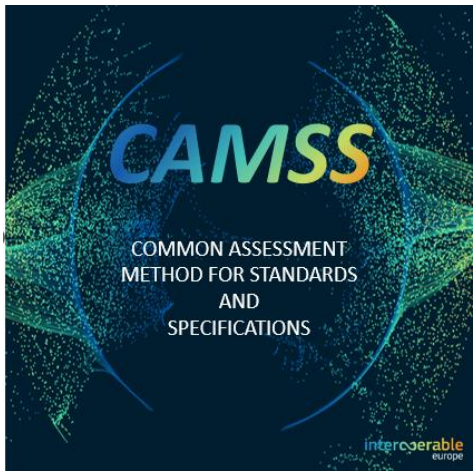

ASSESSMENT SUMMARY v1.0.0

Data Quality Vocabulary (TSP)[1]

World Wide Web Consortium (IETF)[2]

[1] TSP specification: RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) (ietf.org)

[2] IETF: IETF | Internet Engineering Task Force

Change Control

Modification	Details
Version 1.0.0	
Initial version	

TABLE OF CONTENT

1. INTRODUCTION

The present document is a summary of the assessment of the IETF 3161 Time-Stamp Protocol (TSP) carried out by CAMSS using the CAMSS EIF assessment scenario. The purpose of this scenario is assessing the compliance of a standard or specification with the European Interoperability Framework (EIF) .

2. ASSESSMENT SUMMARY

The IETF 3161 Time-Stamp Protocol (also known as TSP) is a cryptographic protocol for certifying timestamps using X.509 certificates and public key infrastructure, which is developed and maintained by the Internet Engineering Task Force (IETF). The timestamp is the signer's assertion that a piece of electronic data existed at or before a particular time. This protocol is an integral part of digital public services, as it facilitates the use of electronic signatures.

Moreover, TSP can significantly contribute to interoperability by providing a unified system for e-signature services. Interoperability ensures that various systems and organizations can work together seamlessly, which is crucial for the efficiency and effectiveness of digital public services. This standardization simplifies interactions between public administrations, making processes more straightforward and reducing bureaucratic overhead.

2.1. EIF Interoperability Principles

Interoperability principles are fundamental behavioural aspects that drive interoperability actions. They are relevant to the process of establishing interoperable European public services. They describe the context in which European public services are designed and implemented.

The specification fully supports the principles setting context for EU actions on interoperability:

- **Subsidiarity and proportionality**

  The specification is not included in any national catalogue of recommended specifications whose Member State NIF is fully aligned with at least 4 out of 5 sections of the EIF according to NIFO factsheets.

The specification fully supports the principles setting context for EU actions on interoperability:

- **Openness**

  The Time-Stamp Protocol (TSP) benefits from its open development process and widespread adoption. Developed and maintained by the Internet Engineering Task Force (IETF), a respected international standards organization, TSP incorporates public review into its decision-making process, encouraging stakeholder input. This collaborative approach, along with its public availability for free on the IETF webpage, has led to its widespread adoption across various layers of technology, including application, transport, internet, and link layers such as FTP and IP. This maturity and established user base make TSP a strong candidate for use in production environments, including innovative digital public services that rely on e-signatures.

- **Transparency**

  In those procedures where it's crucial to have a clear record of when certain actions were taken or when documents were modified, TSP can be a good visibility enabler given its capability to assig timestamps to each event or change, allowing administrators to create a detailed and verifiable log of the sequence of actions. This log can then be used to review procedures, and maintain historical records.

- **Reusability**

  TSP is a business domain agnostic specification that can be applied in any field requiring the management of transaction orders and ensuring data consistency.

- **Technological neutrality and data portability**

  Independent of any specific technology or platform, the Time-Stamp Protocol (TSP) offers flexibility in implementation. It supports partial deployments tailored to specific needs and system constraints, and allows for customization through the setup of a trusted timestamp management infrastructure. Extensions like ANSI X9.95[3] further enhance its capabilities.
  Although TSP primarily focuses on certifying the existence of data in transactions rather than data portability, it plays a crucial role in enabling trustworthy data exchange between systems and European Public Services.

The Technical Specification partially supports the principles related to generic user needs and expectations:

- **User-centricity**

  Ensuring accurate and consistent timestamps, the Time-Stamp Protocol (TSP) creates a reliable record of data changes and states over time, thus playing a vital role in maintaining data integrity and facilitating historical analysis.

- **Inclusion and accessibility**

  The purpose of TSP is not related to e-accessibility. Therefore, this criterion is considered not applicable to the specification.

- **Privacy**

  The Time-Stamp Protocol (TSP) offers a valuable tool for protecting personal data managed by public administrations. By using Time-Stamp Tokens, TSP can restrict document access to authorized requesters, such as specific public authorities. In essence, TSP acts as a Trusted Third Party (TTP) that generates timestamps verifying the existence of data at a specific point in time. This capability safeguards data integrity and prevents unauthorized modifications.

  Furthermore, TSP's importance is recognized in the "Commision decision of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006 /123/EC of the European Parliament

[3] ANSI X9.95 reference: https://webstore.ansi.org/standards/ascx9/ansix9952022

and of the Council on services in the internal market"[4]. This document establishes minimum requirements for the cross-border processing of electronically signed documents by competent authorities and mandates the implementation of technical means that support signed documents in specific formats (BES or EPES). One of the explicitly mentioned technical means is TSP, highlighting its official endorsement for secure data exchange within the European Union.

- **Security**

  The Time-Stamp Protocol (TSP) strengthens information security by adding a crucial layer of trust and verification to data transactions, even though it doesn't directly encrypt data. Reliable timestamps created by TSP enhance security when combined with other measures. These timestamps promote transparency, accountability, and the integrity of data throughout its lifecycle.

  For the access control, TSP, along with Time-Stamp Tokens and TSA authentication mechanisms, allows granting access to specific data fields while restricting access to others. In the case of Data Integrity, Verification Time-Stamp Tokens empower users to validate signatures and confirm data hasn't been tampered with, guaranteeing its integrity. By last, TSP establishes a verifiable record that data existed at a specific point in time, critical for sensitive transactions with deadlines or maintaining accurate logs.

  Remember that TSP safeguards data integrity but not necessarily its accuracy. Additional measures like validation checks, error correction algorithms, and quality control processes are necessary to ensure data correctness and precision.

- **Multilingualism**

  The purpose of TSP is not related to the delivery of multilingual public services. Therefore, this criterion is not applicable to the specification.

The Technical Specification partially supports the foundation principles for cooperation among public administrations:

- **Administrative Simplification**

  TSP tracks the creation and modification time of digital documents. Therefore, it fosters the creation and digitalisation of services at the same time that guarantees the data trustworthy exchange. By providing these capabilities to administrations, allows the reduction of administrative burden avoiding non-digital exchanges and the procedures for ensuring data reliability. Moreover, TSP enables digital service delivery channels in many ways among which we could highlight the maintenance of the data integrity, facilitation of compliance to regulaory requirements or enhancing security in transactions, that is why they are used in document and records management system.

[4] Commision decision of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006 /123/EC of the European Parliament and of the Council on services in the internal market: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011D0130&qid=1714025936203#ntc6-L_2011053ES.01006801-E0006

- **Preservation of information**

  The specification is used for the certification of time-stamps, which provides information about the creation or modifications of certain documentation or data, it can be used when archiving electronic records as a manner to preserve the integrity of such data. Therefore, the IETF 3161 Time Stamp Protocol (TSP) fosters the preservation of electronic documents by providing a mechanism for clearly identify time stamps for these electronic documents.

- **Assessment of effectiveness and efficiency**

  There are several studies and documentation analysing the use of the IETF Time Stamp Protocol with different purposes and putting emphasis on its usage as an efficient way to implement Time-stamp services. In "Design and Implementation of a RFC3161-Enhanced Time-Stamping Service" [5]it is designed and implemented a RFC3161-compliant trusted time-stamping service (TTS) over the Internet. Morover, in "Study about the impementation of Secure Time Stamp Device"[6], it is discussed the design of a Secure Time Stamp device used to securely timestamp digital data, such as computer documents, files, and raw binary data of arbitrary format.

2.2. EIF Interoperability Layers

The interoperability model which is applicable to all digital public services includes: - Four layers of interoperability: legal, organisational, semantic and technical; - A cross-cutting component of the four layers, 'integrated public service governance'; - A background layer, 'interoperability governance'.

The Technical Specification partially supports the implementation of digital public services complying with the EIF interoperability model:

- **Interoperability governance**

  IETF 3161 Time Stamp Protocol (TSP) is already associated with EIRA ABBs in the European Library Of Specifications (ELIS)[7]. More specifically, IETF 3161 Time-Stamp Protocol (TSP) can define the interoperability aspects of the "e-Timestamp Creation Service", and "e-Timestamp Verification and Validation Service" ABBs of the EIRA Technical View.

  Following the completion of the research into conformity tests and certifications, an open-source tool has been identified that enables the testing of implementations with time-stamping commands. This tool is designed to ensure that the implementations are developed appropriately.

[5] Design and Implementation of a RFC3161-Enhanced Time-Stamping Service: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.7115&rep=rep1&type=pdf

[6] Study about the impementation of Secure Time Stamp Device: https://www.sans.org/reading-room/whitepapers/vpns/analysis-secure-time-stamp-device-746

[7] EIRA Library of Interoperability Specifications (ELIS): https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss /solution/elis/release/600

TSP is also used in many European Member States for time-stamping services, utilizing TSA. One such country is Spain, where the sealing service allows electronic document stamps to be issued by the bodies providing the service.

Moreover, while the specification is not included in the open repository of standards at the national level, it is included in the open repository of standards at the European level. The European Union Agency For Network And Information Security [8]also includes it within a set of guidelines for implementing qualified electronic timestamps.

- **Legal interoperability**
  TSP is developed by IETF which is based in the USA. Therefore, the specification cannot be regarded as an European Standard.

- **Organisational interoperability**
  The purpose of TSP is not related to the modelling of business processes as well as to organisational interoperability. Therefore, this criterion is not applicable to the specification.

- **Semantic interoperability**
  No forum or debate has been found that can contribute to the creation of communities along with the sharing of their data and results. However, it is possible to find some topics talking about TSA but without exchange of information or results.

[8] ENISA Security guidelines on the appropriate use of qualified electronic time stamps: https://security.stackexchange.com/questions/173652/how-to-timestamp-a-document-without-electronic-signature-under-eidas

3. Assessment Results

This section presents an overview of the results of the CAMSS assessments for TSP. The CAMSS "Strength" indicator measures the reliability of the assessment by calculating the number of answered (applicable) criteria. On the other hand, the number of favourable answers and the number of unfavourable ones are used to calculate the "Automated Score" per category and an "Overall Score".

Category	Automated Score	Assessment Strength	Compliance Level
EIF Principle setting the context for EU actions on interoperability	20/100 (20%)	100%	Ad-hoc
Core interoperability principles	1700/1700 (100%)	72%	Seamless
Principles related to generic user needs and expectations	1100/1200 (89%)	75%	Seamless
Foundation principles for cooperation among public administrations	500/500 (100%)	100%	Seamless
Interoperability layers*	840/1000 (77%)	70%	Seamless
Overall Score	3160/3500 (90%)	78%	

**The technical interoperability layer is covered by the criteria corresponding to the core interoperability principle ''Openness''.*

With 78% of assessment strength, this assessment can be considered representative of the high specification compliance with the EIF principles and recommendations. The Overall Automated Score of 90% demonstrates that TSP highly supports the European Interoperability Framework in the domains where it applies.