European
Commission

CAMSS

COMMON
ASSESSMENT
METHOD FOR
STANDARDS AND
SPECIFICATIONS

ASSESSMENT SUMMARY v1.0.0

Time-Stamp Protocol (TSP)

Internet Engineering Task Force (IETF)[1]

[1] https://www.ietf.org/

Change Control

Modification	Details
Version 1.0.0	
Initial version	

TABLE OF CONTENT

TABLE OF FIGURES

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].

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. The timestamp is the signer's assertion that a piece of electronic data existed at or before a particular time.

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 partially 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.

- **Openness**
  In the development of the specification, all the stakeholders have the opportunity to contribute and a public review is part of the decision-making process. TSP is publicly available for study and use at no cost on the IETF webpage. Time-Stamp Protocol (TSP) is widely used and implemented in the context of the application, transport, internet and link layers as FTP or IP. Its maturity and adoption are good indicators for its use in the production of products and services, including innovative digital public services requiring e-Signature.

- **Transparency**
  The purpose of the specifications is not related to the visibility or comprehensibility of administrative information, data or services.

- **Reusability**
  TSP is a business agnostic protocol that can be reused in a cross-domain way. Besides, the specification is available for its reuse and implementation for free at the IETF's website.

[2] https://ec.europa.eu/isa2/eif_en

- **Technological neutrality and data portability**
  It is widely adopted and used for this purpose and it is independent of any platform or software. The adoption of the specification to specify certified time stamps can be done independently from the amount of data and can be adapted to users' needs as long as implementations are conformant. These implementations can be used for administrations, citizens and businesses for the certification of documents.

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

- **User-centricity**
  By providing a method for the certification of certain data, it can be useful for administrations when implementing the once-only principle. It eases the reuse of certified information avoiding users to provide information several times.

- **Inclusion and accessibility**
  The purpose of TSP is not related to e-accessibility. Therefore, this criterion does not apply to this specification.

- **Security and privacy**
  The Time-Stamp Protocol or TSP is a cryptographic protocol for certifying timestamps using X.509 certificates and public key infrastructure. The timestamp is the signer's assertion that a piece of electronic data existed at or before a particular time. Therefore, it fosters a trustworthy data exchange between administrations and stakeholders.

- **Multilingualism**
  The purpose of TSP is not related to the delivery of multilingual public services. Therefore, this criterion does not apply to this specification.

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

- **Administrative Simplification**
  The specification allows to track the information related to the creation and modification of digital files. Allowing so, TSP fosters the creation and use of reliable digital services and, therefore, eases the administrative simplification by fostering the reduction of burden.

- **Preservation of information**
  Time Stamp Protocol (TSP) can ease the preservation of information since it is a mechanism for the certificate of existence of certain files or documents. This fact can ensure that information archived in long-time is valid and has the same value.

- **Assessment of effectiveness and efficiency**
  There are different documentation that takes into account the specification in terms of effectiveness and efficiency. One example is the Study about the implementation of Secure Time Stamp Device[3], and another piece is the study showing the possibilities of using the EITF 3161 Time Stamp Protocol for the enhancement of timestamp services[4].

2.1. 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 Specification partially supports the implementation of digital public services complying with the EIF interoperability model:

- **Interoperability governance**
  TSP is associated with EIRA ABBs in the European Library Of Specifications (ELIS). It can define the interoperability aspects of the " e-Timestamp Creation Service", and "e-Timestamp Verification and Validation Service" ABBs of the EIRA Technical View. Even the specification is not included within standard catalogues from CEN, CENELEC or ETSI, it is accessible from the ELIS, that can be considered as a catalogue of interoperability specifications supporting the creation of Interoperability Solutions. However, there is no member state recommending it in their National ICT Catalogue of specifications.

- **Integrated public service governance & Legal Interoperability**
  No evidence has been found of the specification being included in a formal interoperability agreement between organisations involved in the European public services provision, neither evidence of the specification in compliance with the standardisation regulation.

- **Organisational interoperability**
  TSP does not foster organizational interoperability. The purpose of the specification is not related to the topic.

[3] https://www.sans.org/reading-room/whitepapers/vpns/analysis-secure-time-stamp-device-746

[4] https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.7115&rep=rep1&type=pdf

- **Semantic Interoperability**
  TSP is a cryptographic protocol for certifying timestamps using X.509 certificates and public key infrastructure, but it is not defining a data model. Besides, the purpose of TSP is not related to the publication of public data as linked open data.

- **Technical interoperability**
  This technical interoperability layer is covered by the core interoperability principle ''Openness''.

3. Assessment Results

This section presents an overview of the results of the CAMSS assessments for **IETF 3161 Time Stamp Protocol**. 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	# Favourable	# Unfavourable	# Not Applicable
Principle setting the context for EU actions on interoperability	0%	100%	0	1	0
Core interoperability principles	82%	89%	13	3	2
Principles related to generic user needs and expectations	100%	50%	2	0	2
Foundation principles for cooperation among public administrations	100%	100%	3	0	0
Interoperability layers*	72%	82%	13	5	4
Overall Score	77%	77%	23	7	9

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

With a 77% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 77% demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.

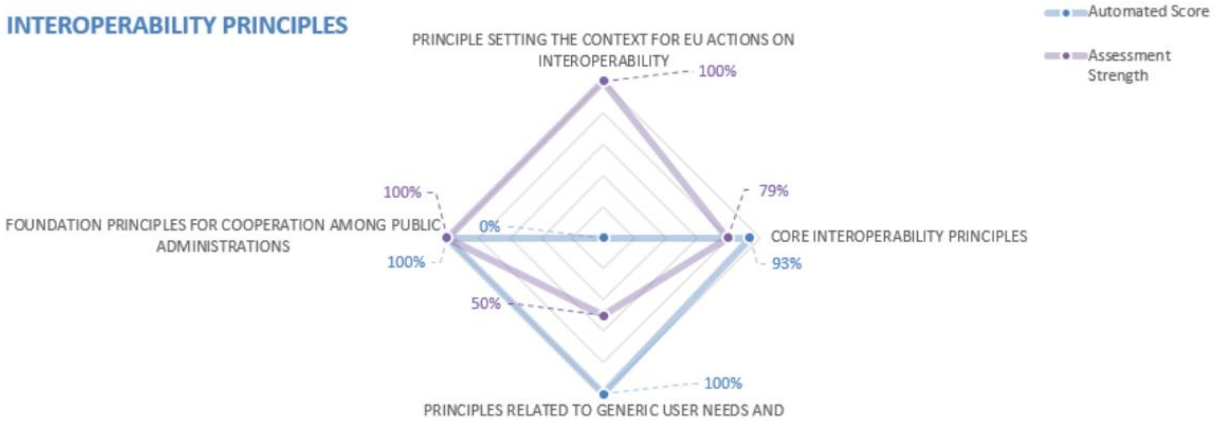

Figure 1. Interoperability principles Results

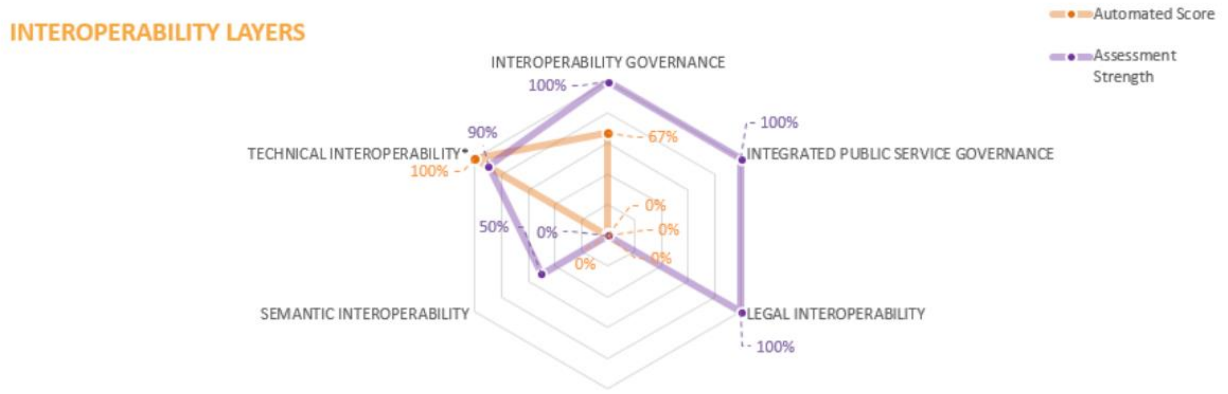

Figure 2. Interoperability layers Results