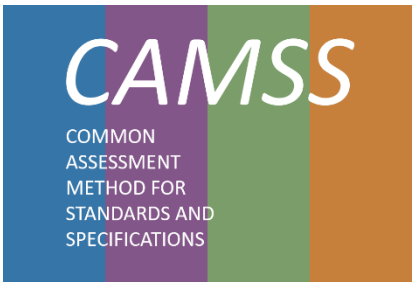

ASSESSMENT SUMMARY

Transport Layer Security (TLS 1.2)

Internet Engineering Task Force (IETF)

1. INTRODUCTION

The present document is a summary of the assessment of TLS 1.2 carried out by the CAMSS Team 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)[1].

2. ASSESSMENT SUMMARY

The **Transport Layer Security (TLS)** Protocol is protocol-independent security of internet connections where both sides can authenticate each other, after which an encryption algorithm and cryptographic keys are negotiated between both sides. These are applied for the remainder of the session. In this way, a protocol-independent secure connection is established. TLS is used for securing various application protocols, such as HTTPS, SMTP, POP3, IMAP and FTP to encrypt the data to be exchanged. This document assesses the version 1.2[2] of this protocol developed and maintained by the **Internet Engineering Task Force (IETF)**[3]

2.1. 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**
  TLS 1.2 is included in the Spanish and the Dutch national catalogues[4] of recommended specifications. Both Spanish and Dutch National Interoperability Framework (NIF) is fully aligned with the European Interoperability Framework (EIF) according to the National Interoperability Framework Observatory (NIFO) Factsheets.

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

- **Openness**
  TLS 1.2 is an open specification available for everyone to study or use. In the IETF, stakeholders have the opportunity to contribute to the development of the specification and the decision-making process includes a public review. Regarding market acceptance, TLS 1.2 was widely adopted and used in order to secure communications over the internet.

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

[2] https://tools.ietf.org/html/rfc5246

[3] https://ietf.org/

[4] https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html#CATALOGOESTANDARES

However, a new version was carried out and it is being highly adopted and implements some security features.

- **Transparency**
  The purpose of TLS 1.2 is not related to the availability of internal systems, therefore, the specification does not foster the availability of interfaces nor the visibility of administration data.

- **Reusability**
  TLS 1.2 is a defacto open specification that is available for free and published at the European Commission platform for the reuse of ICT solutions Joinup. Moreover, TLS 1.2 is a sector agnostic specification that can be used under any business domain.

- **Technological neutrality and data portability**
  By securing the communications over a computer network, TLS 1.2 helps on the proper data portability between administrations. Additionally, as an open standard it does not depends on other specifications or technologies. Even the new version of the specification, the adoption of TLS 1.2 does not affect interoperability.

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

- **User-centricity**
  As a specification to secure communications through the internet, allows European administrations to share and reuse information. Therefore, fosters the implementation of the once-only principle by avoiding administration stakeholders to provide information several times.

- **Inclusion and accessibility**
  TLS 1.2 does not foster e-accessibility. The purpose of the specification is not related to e-accessibility.

- **Security and privacy**
  The purpose of TLS 1.2 is to secure communication over a network and ensure the trustworthy of exchanged data.

- **Multilingualism**
  TLS 1.2 purpose is not related to multilingualism. Therefore, the specification does not foster European public services.

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

- **Administrative Simplification**
  As the purpose of the specification is to secure communications over the internet, it allows to administrations' stakeholders to exchange data digitally. This fact avoids the use of non-digital information exchanges helping to the reduction of administrative burden.

- **Preservation of information**
  The purpose of the specification is not related to the preservation of information. Therefore, TLS 1.2 does not foster the long term preservation of electronic data or other kinds of information.

- **Assessment of effectiveness and efficiency**
  There are existing studies[5] assessing the performance of TLS 1.2 in terms of effectiveness and efficiency.

2.2. 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**
  TLS 1.2 can be associated with European Interoperability Reference Architecture (EIRA) ABBs in the European Library of Specifications (ELIS). More specifically, TLS 1.2 defined the interoperability aspect of the "Network", "Networking Service", "Private Network" and "Public Network" ABBs from the EIRA technical view.

- **Integrated public service governance & Legal Interoperability**
  After being evaluated and compliant with the regulation on standardisation 1025/2012, TLS 1.2 has been identified by Commission Implementing Decision as a specification that can be referenced in procurement. During the evaluation process, all the Member States are invited to share their doubts. The positive evaluation of TLS 1.2 and its identification is considered an interoperability agreement.

- **Organisational interoperability**
  The purpose of the specifications is not related to organisational interoperability. Therefore, TLS 1.2 does not foster organisational interoperability aspects.

[5] http://www-brs.ub.ruhr-uni-bochum.de/netahtml/HSS/Diss/MeyerChristopher/diss.pdf

https://arxiv.org/pdf/1902.02531.pdf

- **Semantic interoperability**
  TLS 1.2 is available for free at the collaborative European platform for ICT solutions reuse Joinup. However, the purpose of the specifications is not related to the publications of Linked Open Data nor define a cross-sector reusable data model.

- **Technical interoperability**
  TLS 1.2 is a widely used open specification. Even though, there is an existing new version (TLS 1.3) that improves security aspects and that it is being highly adopted.

3. *ASSESSMENT RESULTS*

This section presents an overview of the results of the CAMSS assessments of TLS 1.2. The Assessment "Strength" indicator measures the reliability of the assessment by calculating the number of 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 categories.

Category	Automated Score	Assessment Strength	# Favourable	# Unfavourable	# Not Applicable
Principle setting the context for EU actions on interoperability	100%	100%	1	0	0
Core interoperability principles	85%	81%	11	2	3
Principles related to generic user needs and expectations	100%	50%	2	0	2
Foundation principles for cooperation among public administrations	100%	67%	2	0	1
Interoperability layers	88%	77%	15*	2	5
Overall Score	**93%**	**73%**	**30**	**2**	**5**

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

With a 73% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 93% demonstrates that the specification highly supports the European Interoperability Framework in the domains where it applies.

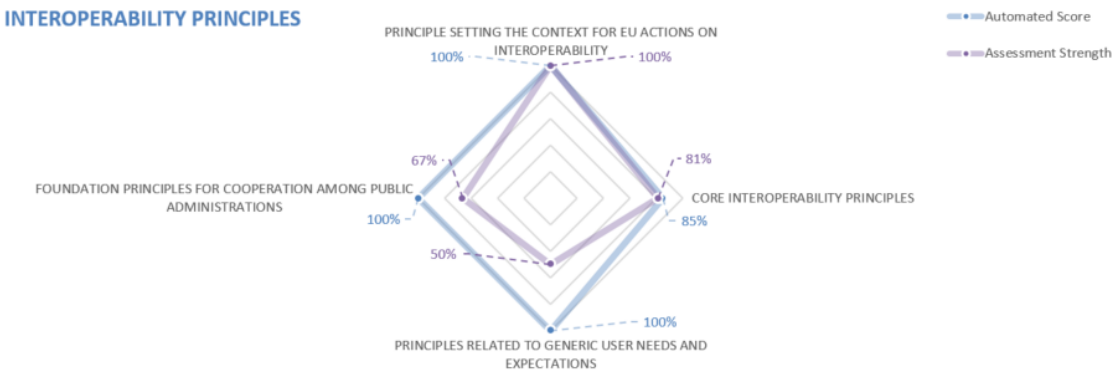

Figure 1 Assessment Results – Interoperability Principles

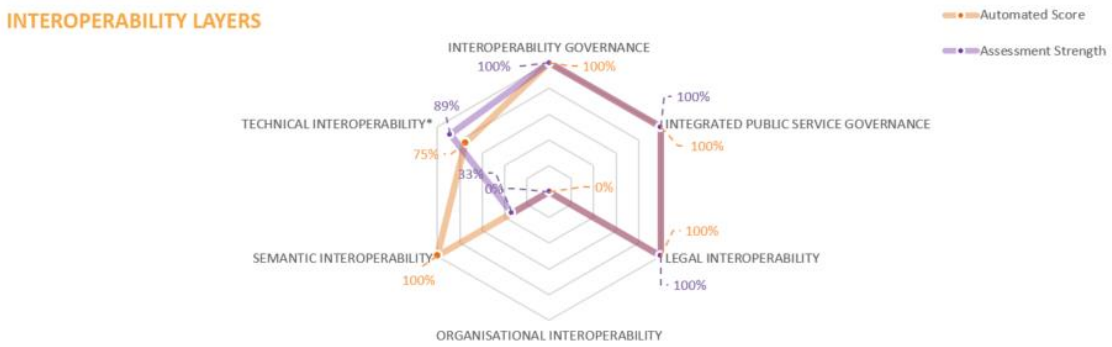

Figure 2 Assessment Results - Interoperability Layers