European Commission

CAMSS
COMMON ASSESSMENT METHOD FOR STANDARDS AND SPECIFICATIONS

ASSESSMENT SUMMARY

Internet Protocol Security (IPsec)[1]

Internet Engineering Task Force (IETF)[2]

[1] https://tools.ietf.org/html/rfc4301

[2] https://ietf.org/

1. INTRODUCTION

The present document is a summary of the assessment of IPsec 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)[3].

2. ASSESSMENT SUMMARY

The **Internet Protocol Security (IPsec)** is a secure network protocol developed by **the Internet Engineering Task Force (IETF)** that enables secure communications between computer network nodes. It is included in the Internet Protocol stack on the network layer. In fact, IPsec is a set of protocols interrelated that establish the mutual authentication between agents and the negotiation of cryptographic keys to use during sessions.

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**
  IPsec is included in the Spanish national catalogue[4] of recommended specifications. The Spanish 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**
  IPsec is an open specification available for everyone for 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. In terms of market acceptance, IPsec is widely used which demonstrates its maturity for the development of products and services or innovative solutions. However, the purpose of IPsec is not related to an area of application that is key for easing interoperability, the publication of open data.

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

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

- **Transparency**
  By allowing the secure communications over the internet, IPsec fosters the visibility of public data.

- **Reusability**
  IPsec is an open specification that is available for free and published in Joinup, the collaborative platform for the reuse of IT solutions funded by the European Commission. Additionally, it is a sector agnostic specification.

- **Technological neutrality and data portability**
  The purpose of IPSec is to secure communications using the Internet Protocol, a de-facto standard for communications over a network. The adoption of IPsec does not hamper interoperability nor data portability between systems.

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

- **User-centricity**
  The purpose of IPsec is not related to the exchange of data and therefore, it can not ease the implementation of the once-only principle

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

- **Security and privacy**
  The purpose of IPSec is to secure communication over a network.

- **Multilingualism**
  IPsec does not foster the delivery of multilingual European public services. The purpose of the specification is not related to multilingualism.

The Technical Specification is partially compliant with the **foundation principles for cooperation among public administrations:**

- **Administrative Simplification**
  The purpose of IPSec is to secure communications over a Network which does not reduce administrative burden.

- **Preservation of information**
  IPsec does not foster the long-term preservation of electronic records and other kinds of information. The purpose of the specification is not related to the preservation of information

- **Assessment of effectiveness and efficiency**
  There are existing studies[5] assessing IPsec 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**
  IPsec can be associated with European Interoperability Reference Architecture (EIRA) ABBs in the European Library of Specifications (ELIS). More specifically, IPSec defined the interoperability aspect of the "Network service" and "Network component" ABBs.

- **Integrated public service governance & Legal Interoperability**
  After being evaluated compliant with the regulation on standardisation 1025/2012, IPSec 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 IPSec and its identification is considered an interoperability agreement.

- **Organisational interoperability**
  IPsec does not foster organisational interoperability aspects. The purpose of the specifications is not related to organisational interoperability.

- **Semantic interoperability**
  The purpose of the specification is to secure communications over a Network, which is not related to Semantic Interoperability.

- **Technical interoperability**
  IPSec is a widely used open specification.

[5] http://ijns.femto.com.tw/contents/ijns-v20-n5/ijns-2018-v20-n5-p811-819.pdf

https://pdfs.semanticscholar.org/8971/9848f632259138d5d4b1052ad24ede803625.pdf

https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report/at_download/fullReport

https://www.researchgate.net/publication/228437109_Interoperability_Issues_for_VPN_IPsec_Solutions

3. *ASSESSMENT RESULTS*

This section presents an overview of the results of the CAMSS assessments of IPsec. 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	100%	88%	16	0	2
Principles related to generic user needs and expectations	100%	25%	2	0	2
Foundation principles for cooperation among public administrations	50%	67%	1	1	1
Interoperability layers	94%	77%	19*	1	2
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 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 93% demonstrates that the specification highly supports the European Interoperability Framework in the domains where it applies.

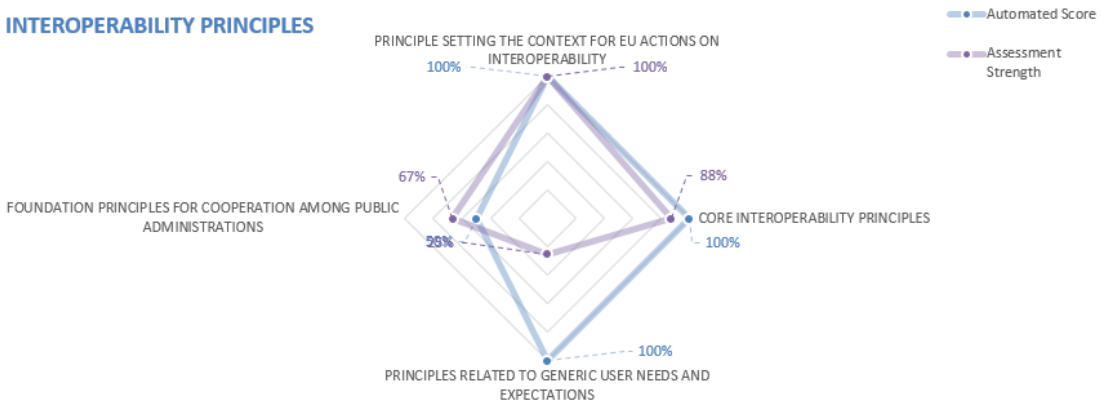

Figure 1 Assessment Results – Interoperability Principles

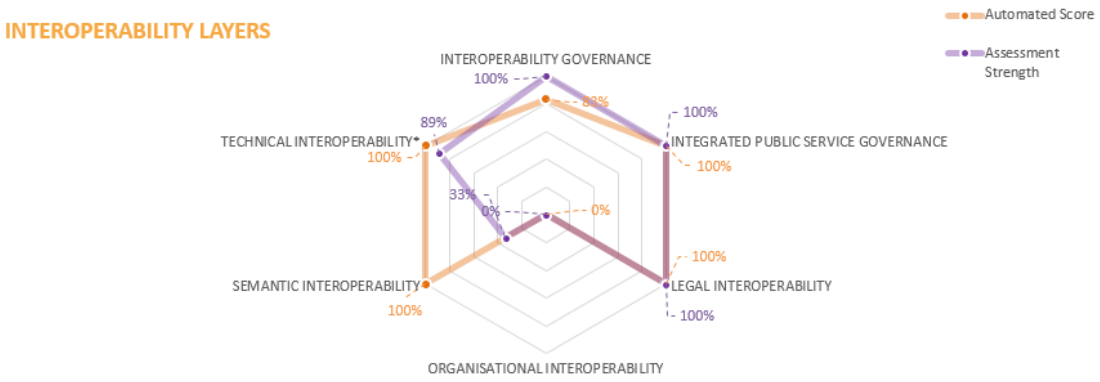

Figure 2 Assessment Results - Interoperability Layers