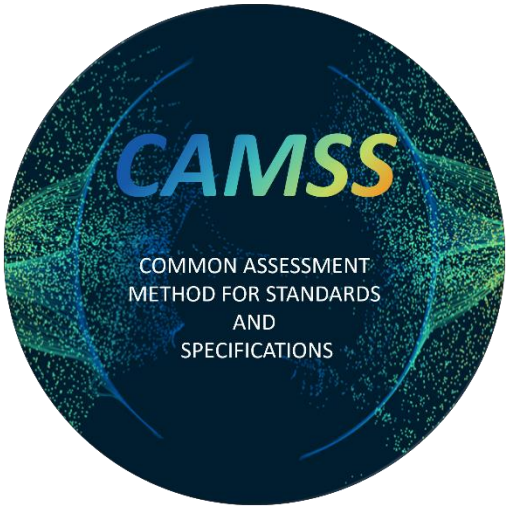

ASSESSMENT SUMMARY v1.0.0

Internet Protocol Security (IPsec)[1]

Internet Engineering Task Force (IETF)[2]

[1] IPsec specification: https://www.rfc-editor.org/rfc/rfc6071.html

[2] IETF organisation: https://www.ietf.org/

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 **IPsec** carried out by CAMSS using the CAMSS Assessment EIF scenario[3]. The purpose of this scenario is to assess the compliance of a standard or specification with the European Interoperability Framework (EIF)[4].

2. ASSESSMENT SUMMARY

The Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data sent over an internet protocol network. It is used in virtual private networks.

Moreover, IPSec is an open standard protocol, which means that it is supported by a wide range of vendors and can be used in heterogeneous environments. It can also help by establishing a specific system for securing communications between organisations.

Finally, this specification first version was released in 1992, and has been developed by IETF. The IETF organisation. The IETF makes voluntary standards that are often adopted by Internet users, network operators, and equipment vendors, and it thus helps shape the trajectory of the development of the Internet. Moreover, it is a open community in which anyone can participate, improving the developed specifications.

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

- **Subsidiarity and proportionality**

  IPsec is included in 5 national catalogues of recommended specifications. They belong to France, Greece, Malta, Netherlands and Spain. The National Interoperability Framework (NIF) of Greece [5] and Spain[6] are aligned with at least 3 out of 4 scoreboards of the EIF Monitoring according to the National Interoperability Framework Observatory (NIFO)[7] factsheets.

[3] CAMSS Assessment EIF Scenario: https://ec.europa.eu/eusurvey/runner/CAMSSAssessmentEIFScenario6

[4] Isa2 programme website: https://ec.europa.eu/isa2/eif_en

[5] National catalogue of Greece: http://www.e-gif.gov.gr/portal/pls/portal/docs/1/211041.PDF

[6] National catalogue of Spain: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html#CATALOGOESTANDARES

[7] NIFO factsheets: https://joinup.ec.europa.eu/collection/national-interoperability-framework-observatory-nifo/nifo-factsheets

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

- **Openness**

  The IPsec specification is a key protocol for data security and privacy. This specification was firstly designed to be part of the IPv6 specification, but security became important and it was finally designed to be an independent internet protocol for security.

  The IPsec specification is maintained and developed by IETF which is an international community developing open standards developing open standards. Thus, like all the IETF standards, this specification is a free and open technical specification, built on IETF standards and licenses from the Open Web Foundation[8]. In addition, the IETF is a consensus-based group, and authority to act on behalf of the community requires a high degree of consensus and the continued consent of the community.

  On the other hand, IPsec has sufficient market acceptance, as it was created in 1992. Since then, all information about IPsec, including details about extensions and implementations that work with IPsec, have been published on the IETF datatracker[9] website. Moreover, IPsec has been integrated into the latest version of the Internet protocol (IPv6), and it can also be integrated with IPv4 as an extension.

- **Transparency**
  IPsec can contribute and promote the visibility of administrations, but it is not its main purpose. In this context, IPsec has been selected by several public administrations for secure data exchange over the internet. By allowing the secure exchange of data, the specification fosters the visibility of data across borders. An example of its implementation is the TESTA project[10], which provides a secure cross-border data communication network service for public administrations.
  However, the specification does not scope comprehensibly administrative procedures and services, neither enables the exposure of interfaces.

- **Reusability**
  IPsec is a sector agnostic specification that allows its implementation independently form the business domain.

[8] Open Web Foundation: https://www.openwebfoundation.org/?lang=en

[9] Datatracker IETF: https://datatracker.ietf.org/

[10] TESTA ISA2 project: https://ec.europa.eu/isa2/solutions/testa_en/

- **Technological neutrality and data portability**
  IPsec is a specification that can be enabled with IPv4 and IPv6 to ensure more security in these specifications. The specification is an independent internet protocol, although it was designed to be part of IPv6. In this sense, IPsec is technology and platform agnostic.
  Moreover, IPsec can be customised, for example, modifying IPsec tunnels created by the IPsec wizard.
  Finally, the specification also allows data portability between systems and is compatible with both IPv4 and IPv6.

***The specification support the principles related to generic user needs and expectations*:**

- **User-centricity**
  The purpose of IPsec is not related to the reuse of information when needed. Therefore this criterion is considered not applicable to the specification.

- **Inclusion and accessibility**
  The purpose of IPsec is not related to e-accessibility. Therefore this criterion is considered not applicable to the specification.

- **Privacy**
  IPsec offers various mechanisms to ensure data protection, including those related to tunneling and confidentiality. Thus, public administrations can use some of these mechanisms to safeguard personal data. Moreover IPsec can also enable features to guarantee restrictions who can access to information.
  On the other hand, the specification has also been included in many European projects focused on privacy aspects. One such project is Demo 4 from the GRID4EU European project[11].

- **Security**
  The IPsec specification provides various mechanisms for enhancing security. The specification can use extension headers to secure data exchange, and also to trustworthiness and integrity of transferred data. Moreover, it also provides mechanisms to enhance the authenticity of the roles agents involved in data transactions and the integrity of transferred data, such as XAuth (Extended Authentication)[12] and MAC (Message Authentication Code)[13]. Therefore, IPsec offers many features to enhance security.

[11] IPsec in GRID4EU project reference: http://www.cired.net/publications/workshop2014/papers/CIRED2014WS_0107_final.pdf

[12] XAuth authentication mechanism: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/277729/using-xauth-authentication

[13] Message Authentication Code (MAC) mechanism: https://www.twingate.com/blog/ipsec

- **Multilingualism**
  The purpose of IPsec is not related to the delivery of multilingual services. Therefore this criterion is not applicable to this specification.

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

- **Administrative Simplification**
  While the main purpose of IPsec is not to simplify the delivery of public services, it can play a significant role. Public administrations often share sensitive data, and IPsec can protect this information. Moreover, IPsec can establish secure Virtual Private Network (VPN) connections, allowing authorised users to access services and data securely over the internet.

- **Preservation of information**
  The purpose of IPsec is not related to long term preservation of electronic records. Therefore, this criterion is considered not applicable to this specification.

- **Assessment of effectiveness and efficiency**
  There are existing documentation and studies assessing the effectiveness and efficiency of IPsec. The "Testing topologies for the evaluation of IPsec implementations"[14] study, is one example of the multiple studies assessing effectiveness. In this study, IPsec is tested in order to achieve confidence in its effectiveness and correctness.
  On the other hand, the “A cryptographic evaluation of IPsec”[15] study, assesses efficiency by focusing on the ISAKMP identity protection exchange and the IKE main mode exchanges.

2.1. 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’.

[14] "Testing topologies for the evaluation of IPsec implementations" study: https://www.researchgate.net/publication/221435103_Testing_Topologies_for_the_Evaluation_of_IPSEC_Implementations

[15] "A cryptographic evaluation of IPsec" study: https://idorosen.com/mirrors/schneier.com/paper-ipsec.pdf

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

- **Interoperability governance**
  At the time of elaborating this assessment, this specification is included in the "Data Exchange" and "Virtual Private Network" ABBs of the Technical View of the current EIRA Library of Interoperability Specifications (ELIS)[16].
  IPsec is relevant in both national and European scenarios. It is included in 5 Member States national catalogues[17], and it has also been identified as a standard by Commission Implementing Decision and included in the European list of ICT Standards for e-procurement.
  Finally, the IPsec specification has been included in the GRID4EU project[18], improving the information transport.

- **Legal Interoperability**
  IPsec is developed by IETF which is based in the USA, thus the specification cannot be regarded as a European Standard.

- **Organisational interoperability**
  While IPsec is not related to the modelling of business processes, it promotes a common framework for security in communication between organisations, which can help facilitate agreements between organisations to define a unique method for securing communications.

- **Semantic Interoperability**
  There are platforms for sharing results, information, and discussing IPsec. One of these platforms, where people can discuss implementations and new versions of IPsec, is the Netgate forum[19]. Many entries addressing issues with implementing IPsec and discussions about IPsec can be found there. In addition, IPsec is also available in the Joinup repository (Interoperable Europe Portal)[20].

[16] EIRA Library of Interoperability Specifications (ELIS): https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss /solution/elis/release/v610

[17] List of recommended standards: https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-list-standards

[18] GRID4EU project: https://cordis.europa.eu/project/id/268206

[19] Netgate IPsec forum: https://forum.netgate.com/category/17/ipsec

[20] Joinup (Interoperable Europe Portal): https://interoperable-europe.ec.europa.eu/

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for **IPsec**. 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 is 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	100/100 (100%)	100%	Seamless
Core interoperability principles	1640/1700 (96%)	100%	Seamless
Principles related to generic user needs and expectations	1200/1200 (100%)	100%	Seamless
Foundation principles for cooperation among public administrations	500/500 (100%)	100%	Seamless
Interoperability layers*	800/1000 (80%)	100%	Sustainable
Overall Score	3540/3800 (93%)[21]	100%	

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

With an 100% 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% (3540/3800) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.

[21] See the "results interpretation" section of the CAMSS Assessment EIF Scenario Quick User Guide:

https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/camss-assessment-eif-scenario/results-visualisation-and-interpretation