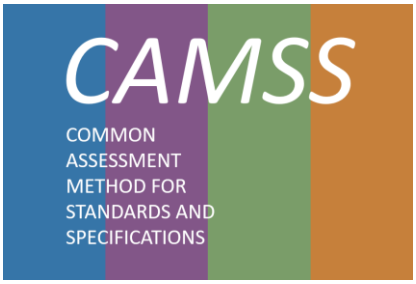

CAMSS ASSESSMENT SUMMARY v1.0.0

Internet Protocol Security (IPSec)[1]

European Telecommunications Standards Institute (IETF)[2]

[1] IPSec specification: RFC 4301 - Security Architecture for the Internet Protocol (ietf.org)

[2] IETF website: 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 **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.

IPSec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. IPSec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

The **Internet Engineering Task Force** (**IETF**) developed the IPSec protocols in the mid-1990s to provide security at the IP layer through authentication and encryption of IP network packets. IPSec originally defined two protocols for securing IP packets: **Authentication Header** (**AH**) and **Encapsulating Security Payload** (**ESP**).

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 does not support the principles setting context for EU actions on interoperability*:**

- **Subsidiarity and proportionality**
  According to the National Interoperability Framework Observatory (NIFO)[5] factsheets, IPSec is included in multiple national catalogue of different Member States.

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

- **Openness**
  IPSec is not related to the publication of public data as open data. The development process has been developed by IETF so all relevant stakeholders can formally appeal and/or raise objections to the development and approval of specifications.

[3] EIF Scenario: https://ec.europa.eu/eusurvey/runner/EIFScenario_v500

[4] EIF: https://ec.europa.eu/isa2/eif_en

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

Like all the IETF standards, IPSec is a free and open technical specification, built on IETF standards and licenses from the Open Web Foundation[6]. IPSec is therefore licensed on a royalty-free basis.

The specification has sufficient market acceptance for its use in digital solutions or services, as it is a widely used de-facto standard. Since 1995 IPSec overcame most of its initial problems and has been used by many products and services, for example, IBM[6] products and services and Oracle Solaris[7].

- **Transparency**
  As part of the "IP Stack", IPSec has been selected by 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[8] project, which provides a secure cross-border data communication network service for public administrations. The focus of IPSec is security. Although the specification does not directly prompt security considerations related to personal data management, IPSec enforces a security policy for databases management; therefore, the specification ensures the protection of personal data.

- **Reusability**
  IPSec is a business domain agnostic specification and therefore can be used and implemented in any domain.
- **Technological neutrality and data portability**
  IPSec is dependent on IPv4 and IPv6, however, IPSec is designed for this area of application and IPv4 and IPv6 are widely used standards. Therefore, this dependency on the specifications for which IPSec has been developed does not hamper interoperability. Also, IPSec allows the exchange of data between systems and is compatible with both versions of the Internet Protocol, IPv4 and IPv6. Therefore, it prevents the storage of data in silos that are incompatible with one another. As it allows the exchange of data between systems, it supports the evolution of European public services.

***The specification does not support the principles related to generic user needs and expectations*:**

- **User-centricity**
  There is no reference to IPSec and a European use case explicitly stating that the specification allows relevant information and data to be reused. Moreover, it is not focused on the implementation of the OOP.

[6] IBM Infrastructures: https://www.ibm.com/it-infrastructure/z/zos

[7] Oracle Solaris: https://www.oracle.com/solaris/solaris11/

[8] TESTA website: https://ec.europa.eu/isa2/solutions/testa_en

- **Inclusion and accessibility**
  The purpose of IPsec is to provide data authentication, integrity and confidentiality. Also defining the encryption, decryption and authentication of packets. Therefore, this criterion is considered not applicable to this specification.

- **Security and privacy**
  IPsec is a set of open standards and protocols for securing the exchange of data packets over a computer network, including data confidentiality, integrity, origin authentication and anti-replay. Therefore, it ensures secure and trustworthy data exchange between different stakeholders.

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

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

- **Administrative Simplification**
  The purpose of IPsec is to secure communications over a network which does not simplify the delivery of European public services. The specification does neither focus on the facilitation of digital service delivery channels.

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

- **Assessment of effectiveness and efficiency**
  Existing documentation and studies are assessing and analysing the performance, effectiveness and efficiency of IPsec in different contexts and application areas. For instance, ENISA[9] provides documentation recommending the use of IPsec to improve security.

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

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

- **Interoperability governance**
  IPsec is already associated with an EIRA ABB in the EIRA Library Of Specifications (ELIS[10]). More specifically, IPsec can define the interoperability aspects of the "Data Exchange Component" and "Data Exchange Service" ABBs of the EIRA Technical View.

- **Legal Interoperability**
  The rules on European standardisation allow the European Commission to identify information and communication technology (ICT[11]) technical specifications - that are not national, European or international standards - to be eligible for referencing in public procurement. After being evaluated as compliant with the regulation on standardisation 1025/2012, IPsec has been identified by Commission Implementing Decision. The positive evaluation of IPsec and its identification in European Regulations respond positively to this criterion.

- **Organisational Interoperability**
  After being evaluated as compliant with the regulation on standardisation 1025/2012, IPsec has been identified by Commission Implementing Decision. The positive evaluation of IPsec and its identification is considered an interoperability agreement, although no specific provisions are given to facilitate the drafting of such agreements.

- **Semantic Interoperability**
  There is no evidence found of the creation of any community along with the sharing of their data and results on national platforms. Therefore, this criterion does not apply to this specification.

[10] ELIS in Joinup: https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elis/release/v110

[11] European Commission ICT Technical Specifications: https://ec.europa.eu/growth/single-market/european-standards/ict-standardisation/ict-technical-specifications_en

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	2020/2200 (91%)	86%	Seamless
Principles related to generic user needs and expectations	500/500 (100%)	40%	Seamless
Foundation principles for cooperation among public administrations	420/500 (84%)	60%	Seamless
Interoperability layers*	900/1100 (81%)	82%	Seamless
Overall Score	3940/4300 (91%)	74%	

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

With an 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 91,62% (3940/4300) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.