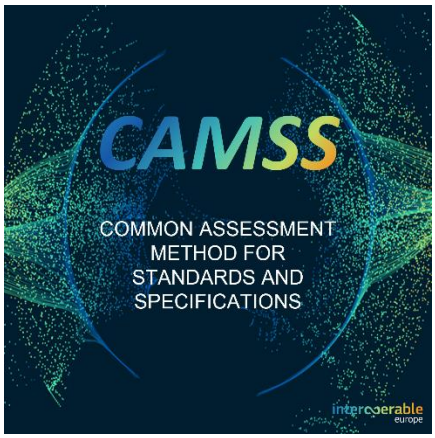

ASSESSMENT SUMMARY v1.0.0

Internet Protocol Version 4 (IPv4)[1]

Internet Engineering Task Force (IETF)[2]

[1] IPv4 specification: https://datatracker.ietf.org/doc/html/rfc791

[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 **IPv4** 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 Version 4 (IPv4) is designed for use in interconnected systems of packet-switched computer communication networks. Such a system has been called a "catenet". The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through "small packet" networks.

Moreover, IPv4 provides the basic networking infrastructure for devices, applications, and services to send and receive data over a network. This enables communication between systems that may be built on different technologies or platforms. The ability to route data across diverse networks, from a local private network to global networks like the internet, is the first step toward ensuring interoperability.

Finally, this specification first version was released in 1980, 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**
  IPv4 is included in 6 national catalogues of recommended specifications. They belong to Croatia, France, Germany, Netherlands, Norway, and Sweden. The National Interoperability Framework (NIF) of Sweden[5] and Netherlands[6] are aligned with at least 3 out of 4 scoreboards of the EIF

[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 Sweden: https://www.avropa.se/globalassets/dokument/open-it-standards.pdf?_t_id=1B2M2Y8AsgTpgAmY7PhCfg%3d%3d&_t_q=standards&_t_tags=language%3asv%2csiteid%3a95d515a5-23ca-47bf-87a9-

[6] National catalogue of Netherlands: https://www.forumstandaardisatie.nl/open-standaarden/lijst

Monitoring according to the National Interoperability Framework Observatory (NIFO) factsheets[7]. Nonetheless, countries like Germany[8] do not get a high performance.

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

- **Openness**

  Pv4 is widely adopted as a key protocol for making data, information, and resources available on the internet. However, it is worth noting that the newer version, IPv6, is being gradually adopted and incorporates several innovative solutions.

  The IPv4 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[9]. 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, IPv4 has sufficient market acceptance, as it was created in 1980. Since then, many assessments and improvements have been made in terms of security and privacy, for example. The IPv4 specification is widely adopted as a key protocol for making data, information, and resources available on the internet. However, it is worth noting that the newer version, IPv6[10], is being gradually adopted and incorporates several innovative solutions, such as built-in support for IPsec and stronger address allocation mechanisms.

- **Transparency**
  The purpose of the specification is not directly related to the visibility and enable the exposure of public interfaces to access the public administration's services. However, it can contribute to it offering addresses spaces allowing public services to have unique, globally routable IP addresses for every device. Although IPv4 is not addressed to these characteristics, it actively promotes and supports comprehensibility, enabling the establishment of IP connectivity to a network by assigning an IP address to an interface

- **Reusability**

[7] NIFO factsheets: https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory /digital-public-administration-factsheets-2024

[8] National catalogue of Germany: https://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/SAGA%205-aktuelle%20Version/saga_5_aktuelle_version_node.html

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

[10] IPv6 adoption reference: https://www.ipxo.com/blog/ipv6-adoption/

IPv4 is a sector agnostic specification that allows its implementation independently form the business domain.

- **Technological neutrality and data portability**
  IPv4 is the previous version of the Internet Protocol, but it is widely adopted and still prevailing. Thus, it is not dependent of any specific technology and platform and the adoption of IPv4 does not hamper the interoperability. Moreover, the IPv4 specification allows for extensions and partial implementations across various scopes, such as within the IP layer.

  Furthermore, the IPv4 specification plays a foundational role in enabling data portability between systems or applications in terms of network communication.

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

- **User-centricity**
  The Internet Protocol is a necessary specification for the implementation of the once-only-principle as it allows cross-border communications over the internet. For example, an IPv4 address can be reused and an address block can only be used by any party on the Internet with the permission of others. Specifically, an (Internet Service Provider) ISP that is asked to provide connectivity to the party, by "routing" their address block onto the Internet.

- **Inclusion and accessibility**
  The purpose of IPv4 is not related to e-accessibility. Therefore this criterion is considered not applicable to the specification.

- **Privacy**
  The IPsec protocol[11] helps secure communication by encrypting IP packets, ensuring that information exchanged between public administrations or between a government and its citizens remains protected and trustworthy. Additionally, IPv4 networks use Access Control Lists (ACLs)[12] to control who can access data, preventing unauthorized users from gaining access. ACLs filter network traffic by examining packets as they pass through routers or switches, allowing or blocking them based on predefined rules for specific devices or network segments. This combination of encryption and access control makes data exchanges safer and more secure.

  Moreover, IPv4 is mentioned in the "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Advancing the Internet : action plan for the deployment of Internet Protocol version 6

[11] IPsec protocol: https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

[12] IPv4 ACL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960l/software/15-2_6_e/configuration_guide/b_1526e_consolidated_2960l_cg/m_sec_acls_cg_danube_2960l_cdb.html

(IPv6) in Europe"[13], as a specification that has been updated to provide enhanced security services, similar to those in IPv6.

- **Security**

  The IPv4 specification can be used with the IPsec protocol, which guarantees the authentication of the roles agents involved in transactions, and establishes mechanisms to allow or deny their access to data. Moreover, can help prevent unauthorised changes with the AH and ESP transfer protocols[14], and can encrypt the message at network layer even if the protocols of application layer at user level didn't does not encrypt the message. With these implementations, IPv4 can help to accurately transfer data and guarantee data access control.

  In addition, there are other implementations such as Access Control Lists (ACL) for IPv4, which can establish an access control mechanisms to access data.

- **Multilingualism**
  The purpose of IPv4 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**
  By allowing communications over the internet, IPv4 contributes to the exchange of information between public administrations. Therefore, it reduces administrative burden.
  Moreover, IPv4 provides addressing and routing mechanisms that allow devices and systems to communicate over the internet. This is essential for digital service delivery channels such as websites, mobile applications, cloud services, and APIs that rely on the internet to deliver services.

- **Preservation of information**
  The purpose of IPv4 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**

[13] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Comittee of the Regions - Advancing the Internet : action plan for the deployment of Internet Protocol version 6 (IPv6) in Europe: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52008DC0313&qid=1730898345313

[14] AH and ESP protocols: https://www.ibm.com/docs/en/zos/2.1.0?topic=ipsec-ah-esp-protocols

There are existing documentation and studies assessing the effectiveness and efficiency of IPv4. The "A systematic review of transition from IPv4 to IPv6"[15] study, is one example of the multiple studies assessing efficiency and effectiveness. It examines and exposes how IPv4 has demonstrated reliability, compatibility with a wide range of protocols, applications and ease of implementation. In addition, it is made a comparison between IPv4 and IPv6, and how IPv6 can improve its predecessor.

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'.

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 "Firewall" ABBs of the Technical View of the current EIRA Library of Interoperability Specifications (ELIS)[16].

  IPv4 is relevant in both national and European scenarios. It is included in 6 Member States national catalogues[17], and is also mentioned in the "Alternative Bearers for Rail"[18] project. In the project, IPv4 is analysed, and some strategies for allowing the IPv4 and IPv6 interworking are proposed.

- **Legal Interoperability**

  IPv4 is developed by IETF which is based in the USA, thus the specification cannot be regarded as a European Standard. However, the Réseaux IP Européens (RIPE)[19] organisation act as the Regional Internet Registry (RIR) providing global Internet resources and related services (IPv4, IPv6 and AS Number resources) to members in his service region.

- **Organisational interoperability**

[15] "A systematic review of transition from IPv4 to IPv6" study: https://www.researchgate.net/publication/343820813_A_Systematic_Review_of_Transition_from_IPV4_To_IPV6

[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] "Alternative Bearers for Rail" project: https://cordis.europa.eu/project/id/101014517

[19] RIPE organisation: https://www.ripe.net/

While IPv4 is not related to the modelling of business processes, it promotes a common framework for communication, which can help facilitate agreements between organisations to define a unique method for communicating.

- **Semantic Interoperability**
  IPv4 indirectly encourages the creation of communities on national and European platforms sharing news and updates about IPv4 addresses, such as RIPE organisation.

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for **IPv4**. 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%	Sustainable
Core interoperability principles	1540/1700 (91%)	100%	Sustainable
Principles related to generic user needs and expectations	1120/1200 (93%)	100%	Sustainable
Foundation principles for cooperation among public administrations	500/500 (100%)	100%	Sustainable
Interoperability layers*	900/1000 (90%)	100%	Sustainable
Overall Score	4160/4500 (92%)[20]	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 92% (4160/4500) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.

[20] 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