



ASSESSMENT SUMMARY v1.0.0

IPv6 – Internet Protocol Version 6¹

Internet Engineering Task Force (IETF)²

¹ IPv6 IETF: <https://www.rfc-editor.org/rfc/rfc2460>

² IETF working group: <https://www.ietf.org/>

Change Control

| Modification | | Details |
|-----------------|--|---------|
| Version 1.0.0 | | |
| Initial version | | |

TABLE OF CONTENT

1. INTRODUCTION..... 4

2. ASSESSMENT SUMMARY 4

EIF Interoperability Principles.....4

2.1. EIF Interoperability Layers7

3. ASSESSMENT RESULTS 10

1. INTRODUCTION

The present document is a summary of the assessment of the **IPv6 – Internet Protocol Version 6 (IPv6)** carried out by CAMSS using the CAMSS Assessment EIF scenario³. 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

IPv6 is an specification addressed to create larger and more complex IP directions than those created by the IPv4 specification. Moreover, the IPv6 is a new version of the Internet Protocol, designed as the successor to IP version 4 (IPv4), and includes some security and extensions changes, for example.

Moreover, the IPv6 specification addresses eGovernment by establishing a better way to be connected to the internet. Moreover, it is addressed to support the predicted growth of connected devices in IoT, manufacturing, and emerging areas like autonomous driving. Furthermore, it can also improve the privacy of public administrations by defining security improvements.

The IPv6 specification was created by IETF in 1998. Since then, it has been assessed in many forums and by some workings groups, improving it and sharing all functionalities in the community through the Internet. Although IPv6 was created in 1998, it is in constant development and is being maintained by IETF.

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

- **Subsidiarity and proportionality**

IPv6 is included in 7 national catalogues of recommended specifications. They belong to Austria, Croatia, France, Germany, Netherlands, Norway, and Sweden. The National Interoperability Framework (NIF) of Germany⁵ and Austria⁶ are fully aligned with at least 3 out of 5 sections of the European Interoperability Framework (EIF) according to the National Interoperability Framework

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 Germany: <https://www.cio.bund.de/Webs/CIO/DE/digitaler-wandel/architekturen-und-standards/architekturen-und-standards-node.html>

⁶ National catalogue of Austria: <https://ref.gv.at/ag-ii-austrian-intero.-framework>

Observatory (NIFO) factsheets⁷. Nonetheless, countries like Sweden⁸ do not get a high performance, being aligned with 3 out of 5.

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

- **Openness**

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. The group has a formal review and approval so that all the relevant stakeholders can formally appeal or raise objections to the development and approval of specifications. In addition, this specification is a free and open technical specification, built on IETF standards and licenses from the Open Web Foundation. Moreover, the IPv6 is being applied in many countries, although there are differences in the adoption level⁹. On the other hand, IPv6 also incorporates some improvements in terms of security and flexibility to its predecessor, IPv4. Finally, IPv6 is maintained and developed by IETF which is an international community developing open standards.

- **Transparency**

The main purpose of IPv6 is not to enhance visibility of administrative procedures, rules data, and services, but can contribute to it. This can simplify network management and enhance visibility, making it easier to organise and categorise network resources. In addition, IPv6 offers a larger address space compared to IPv4, allowing public services to have unique, globally routable IP addresses for every device.

- **Reusability**

IPv6 specification is versatile and applicable across various business domains, facilitating growth, innovation, and collaboration.

- **Technological neutrality and data portability**

The specification purpose is to enable communications over the Internet. IPv6 is the new version of IPv4 which is a widely used protocol, thus it is not dependent of any specific technology. It also allows for implementations and extensions that can be implemented incrementally or separately. And although the core specification is not customisable, there are aspects of its implementation and configuration that can be tailored to meet specific needs.

⁷ NIFO factsheets in Joinup: <https://joinup.ec.europa.eu/collection/nifo/nifo-factsheets>

⁸ National catalogue of Sweden: https://www.avropa.se/globalassets/dokument/open-it-standards.pdf?t_id=1B2M2Y8AsgTpgAmY7PhCfg%

⁹ IPv6 adoption reference: <https://www.ipxo.com/blog/ipv6-adoption/>

Furthermore, the specification addresses and enables data portability allowing data exchange between systems and being compatible with the previous version IPv4.

The specification partially 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, the mobile IPv6 protocol provides mobility support for IPv6 and it allows to keep the same internet address.

- **Inclusion and accessibility**

The purpose of IPv6 is not related to e-accessibility. Therefore this criterion is considered not applicable to the specification.

- **Privacy**

The IPsec protocol¹⁰, included in the IPv6 specification, guarantees that data is exchanged securely. For example, when IPsec operates in tunnel mode (Gateway-to-Gateway or Gateway-to-Host), the entire IPv6 packet is encrypted and authenticated, data exchanged between public administrations or citizens is protected. In addition, IPv6 can work with VPN's to guarantee restrictions on who can access to information.

Moreover, IPv6 can be found covering privacy aspects in the "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)¹¹" as a key protocol for the security of the public core of the open internet and the stability of its functioning. And can also be found in an "Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe¹²".

- **Security**

With the IPsec protocol it is possible to guarantee the authentication of the roles agents involved in transactions, and to allow or deny their access to data. Moreover, can help prevent unauthorised changes with the AH and ESP transfer protocols¹³, and can encrypt the message at network layer even if the protocols of application layer at user level does not encrypt the message. With these implementations, IPv6 can help to accurately transfer data and guarantee data access control.

¹⁰ IPsec reference : <https://www.rfc-editor.org/rfc/rfc6071>

¹¹ EurLex "Regulation (EU) 2019/881": <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0881&qid=1729248000483>

¹² EurLex "Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe" reference: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52008DC0313&qid=1729248000483>

¹³ AH and ESP transfer protocols: <https://www.ibm.com/docs/en/zos/2.1.0?topic=ipsec-ah-esp-protocols>

In addition, there are other implementations such as Access Control Lists (ACL)¹⁴ for IPv6, which can establish an access control mechanisms to access data.

- **Multilingualism**

The purpose of IPv6 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, IPv6 contributes to the exchange of information between public administrations, reducing administrative burden. Moreover, the specification supports digital service delivery channels by providing a much larger address space than IPv4, which facilitates the connection of a vast number of devices to the internet.

- **Preservation of information**

The purpose of IPv6 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 IPv6. The "IPv6 performance - and how to test it"¹⁵ is an example of a study that makes an assessment for measure the effectiveness of IPv6 using scores for city (Frankfurt in this case), region (Europe) and Global. Moreover, the assessment almost includes other themes such as connectivity. On the other hand, the "IPv4 and IPv6 Protocols: A Comparative Performance Study"¹⁶ study, aims to perform a comparative study on the performance and efficiency of IPv4 and IPv6 on voice and video network traffic flow using performance metrics such as jitter, typo, and packet loss.

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;

¹⁴ Access Control Lists for IPv6 reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960xr/software/15-2_5_e/configuration_guide/b_1525e_consolidated_2960xr_cg/configuring_ipv6_acls.html

¹⁵ "IPv6 performance - and how to test it" reference:
https://www.swissipv6council.ch/sites/default/files/images/sonar_article_02-2013-final.pdf

¹⁶ "IPv4 and IPv6 Protocols: A Comparative Performance Study" reference:
https://www.researchgate.net/publication/335863969_IPv4_and_IPv6_Protocols_A_Comparative_Performance_Study

- 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)¹⁷.

IPv6 is relevant in both national and European scenarios. It is included in 7 Member States national catalogues¹⁸, and is also mentioned in the "Commission Implementing Decision of 3 April 2014 on the identification of ICT technical specifications eligible for referencing in public procurement"¹⁹. In this decision, the IPv6 specification is set as one of the ICT technical specifications that may be eligible for referencing in public procurement.

- **Legal Interoperability**

IPv6 is developed by IETF which is based in the USA, thus the specification cannot be regarded as a European Standard. However, in Europe, IPv6 address space can be obtained from an upstream provider or from the regional internet registrar for Europe: Requirements for IPv6 in ICT Equipment (RIPE)²⁰.

- **Organisational interoperability**

While IPv6 does not addresses to the modelling of business processes, it facilitates organisational interoperability agreements. As an internet standard, IPv6 promotes a common framework for communication. For example, the "Requirements for IPv6 in ICT Equipment (RIPE)" is intended to provide a Best Current Practice (BCP) to support organisations to specify requirements for IPv6 functionality and compatibility when drafting tenders for Information and Communication Technology (ICT) equipment and support. Thus can help facilitate agreements between organisations to define a unique method for communicating.

¹⁷ EIRA Library of Interoperability Specifications (ELIS): <https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elis/release/v610>

¹⁸ List of recommended standards: <https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-list-standards>

¹⁹ "Commission Implementing Decision of 3 April 2014 on the identification of ICT technical specifications eligible for referencing in public procurement": <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014D0188>

²⁰ "Guidelines and Process: IPv6 for Public Administrations in Europe" reference: <https://joinup.ec.europa.eu/sites/default/files/document/2019-12/Plum-EC-IPv6-Guidelines.pdf>

- **Semantic Interoperability**

There are platforms to share results and information about IPv6. The IPv6 Forum²¹ is a world-wide consortium of worldwide leading Internet vendors, Industry Subject Matter Experts, Research & Education Networks, with a clear mission to advocate IPv6 by dramatically improving technology, market, and deployment user and industry awareness of IPv6.

²¹ IPv6 forum: <https://ipv6forum.com/?module=News&type=user&func=display&sid=9>

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for **IPv6**. 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 | 1540/1700 (90%) | 100% | Seamless |
| Principles related to generic user needs and expectations | 1080/1200 (90%) | 100% | Seamless |
| Foundation principles for cooperation among public administrations | 500/500 (100%) | 100% | Seamless |
| Interoperability layers* | 880/1000 (88%) | 100% | Seamless |
| Overall Score | 3700/4100 (90%) ²² | 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 90% (3700/4100) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.

²² 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>