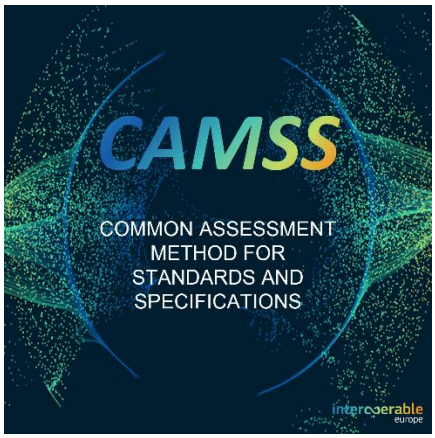

ASSESSMENT SUMMARY v1.0.0

Domain Name System (DNS)[1]

Internet Engineering Task Force (IETF)[2]

[1] DNS reference link: https://datatracker.ietf.org/doc/html/rfc8499

[2] IETF webpage: 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 **Domain Name System (DNS**) 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 **Domain Name System (DNS**) is the hierarchical and decentralized naming system used to identify computers reachable through the Internet or other Internet Protocol (IP) networks. The resource records contained in the DNS associate domain names with other forms of information. These are most commonly used to map human-friendly domain names to the numerical IP addresses computers need to locate services and devices using the underlying network protocols but have been extended over time to perform many other functions as well.

The basic concept for how DNS does its job is rather simple: each website address entered into a web browser (like Chrome, Safari, or Firefox) is sent to a DNS server, which understands how to map that name to its proper IP address.

DNS has been developed by the Internet Engineering Task Force (IETF), an open standards organization that develops and promotes voluntary Internet standards, in particular the technical standards that comprise the Internet protocol suite (TCP/IP).

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

- **Subsidiarity and proportionality**

  DNS is included in 9 national catalogues of recommended specifications. Some of these catalogues are:

  The National Interoperability Framework of France, Germany and Spain. The National Interoperability Framework of France, Germany and Spain is fully aligned with the 3 sections of the European Interoperability Framework (EIF) according to the National Interoperability Framework Observatory (NIFO)[5] 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] NIFO Factsheets in Joinup: https://joinup.ec.europa.eu/collection/national-interoperability-framework-observatory-nifo/nifo-factsheets

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

- **Openness**

  The DNS specification has been developed by the IETF, an open standards organization, which sticks to the basic principles of openness. This means that DNS is licensed under a royalty-free basis and it is publicly available for free on their webpage for anyone to study and implement. The IETF community is also in charge of conducting public reviews of the specification, making relevant stakeholders participate in the development process. In addition, the standard organization maintains and updates the specification as well.

  As DNS is a de-facto standard and is an essential component for the development of products and services on the web. Therefore, it can be considered sufficiently mature for the creation of digital solutions.

- **Transparency**

  The main functionality of DNS is to allow for associations of information to domain names, which in turn, facilitates the comprehension and enhances the visibility of data and services in a network. Under the same logic, it also eases the identification of interfaces thus, helping to ensure interoperability between systems and the data they handle.

  DNS facilitates the visibility of public administrations. As an example of ensuring their visibility, DNS might enhance the transparency of public administrations' networks. The European Commission is developing its own DNS service, the DNS4EU[6], which will allow the access to global Internet and will comply with EU regulations.

- **Reusability**

  DNS is publicly available for free to use at the IETF's website. It is domain and platform-agnostic, meaning that it can be implemented with no dependencies on operating systems, and it can be applied in any business domain.

  DNS is the hierarchical and decentralised naming system used to identify computers reachable through the Internet or other Internet Protocol (IP) networks. For that matter it can be used in any domain.

- **Technological neutrality and data portability**

  Although DNS performs some functionalities than cannot be implemented separately, it has been developed to support some requirements that are not mandatory but recommended, such as the DNS Security Extension (DNSSEC). The specification also provides extension mechanisms that address more security issues or for the integration of a conformance testing tool.

[6] DNS4EU initiative: https://www.joindns4.eu/

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

- **User-centricity**
  The purpose of DNS is not related to the reuse of information. Therefore, the principle of user-centricity does not apply to this specification.

- **Inclusion and accessibility**
  The purpose of DNS is not related to e-accessibility, therefore, the principle of inclusion and accessibility does not apply to this specification.

- **Privacy**
  DNS is recognised and integrated in the DNS4EU initiative, covering both European and national levels, especially those concerning privacy standards, policies and norms.

- **Security**
  Secure processing of data can be provided by DNS adding the DNS Security Extensions (DNSSEC), which is, in fact, almost a mandatory extension between major stakeholders, furthermore, DNS can provide several other transport protocol extensions to provide a safer data exchange by adding support to cryptographically signed responses or cryptographic authentication to authorize zone transfer or dynamic update operations.

- **Multilingualism**
  The purpose of DNS 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**
  When it comes to the identification of the content of domains, DNS helps the administrative simplification by associating a name to an IP.

- **Preservation of information**
  The specification's purpose is not directly the long-term preservation of electronic records.

- **Assessment of effectiveness and efficiency**
  There can be found in the internet many existing studies of the efficiency and effectiveness of the DNS. Particularly, there seems to be a general interest on the effectiveness and efficiency of the DNS Security extensions mechanisms, and on the DNS Tunnelling tools.

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:

- **Interoperability governance**

  At the moment of the assessment, DNS cannot be mapped with EIRA. Nonetheless, the specification is recommended and included in the national catalogues of nine member states, including France, Germany, Spain, Sweden, Malta, Greece, Croatia and the Netherlands. Moreover, at a European level, it has been identified as one of ICT standards for e-procurement. In terms of implementation conformity, there are several tools to assess DNS compliance against security standards.

  DNS is already associated to an EIRA ABB in the EIRA Library Of Specifications (ELIS). More specifically, DNS can define the interoperability aspects of the "Web Server" and "Data Exchange Application Component, "Application Server", "Domain Name Service" and "Data Exchange Application Service" ABBs of the EIRA Technical View.

- **Legal Interoperability**

  After being evaluated as compliant with the regulation on standardisation 1025/2012, DNS has been identified by Commission Implementing Decision and included in the European list of ICT Standards for e-procurement[7].

- **Organisational interoperability**

  As a standard protocol, DNS helps to ensure interoperability when it comes to defining processes for setting internet domain names, thus easing interoperability between devices, applications, data repositories, services and networks, this is why, among other reasons, it appears as one of the set standards for the "Commission Implementing Decision of 3 April 2014 on the identification of ICT technical specifications eligible for referencing in public procurement"

- **Semantic Interoperability**

  At a national level, there are many communities focused on DNS testing implementation. One of them is the GitHub repository, where a large community of developers maintaining discussions around the main issues and subjects that DNS arises. The Joinup repository, at a European level, comprises a large community of developers some of whom address different issues related to DNS.

[7] "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/ALL/?uri=CELEX%3A32017D0168

3. Assessment Results

This section presents an overview of the results of the CAMSS assessments for **DNS**. 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%)	88%	Seamless
Principles related to generic user needs and expectations	1140/1200 (95%)	58%	Seamless
Foundation principles for cooperation among public administrations	500/500 (100%)	80%	Seamless
Interoperability layers*	1000/1000 (100%)	100%	Seamless
Overall Score	3480/3700 (94%)[8]	82%	

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

With an 82% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 94% (3480/3700) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.

[8] 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