Draft ID: de13147a-882b-43c6-9f95-dfd8eab4c053
Date: 28/03/2024 10:17:25

CAMSS Assessment EIF Scenario v6.0.0

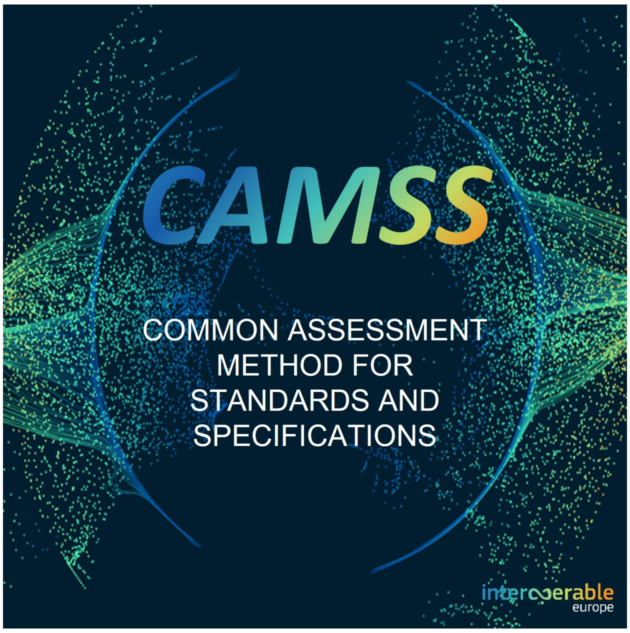
Fields marked with * are mandatory.

CAMSS Assessment EIF Scenario v6.0.0

Release Date: 14/04/2023

Scenario Version: 6.0.0

INTRODUCTION



EIF Scenario

The European Interoperability Framework (EIF) provides guidance to public administrations on how to improve governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that existing and new legislation do not compromise interoperability efforts.

This CAMSS Scenario allows to assess the compliance of **interoperability specifications** with the EIF. The objective of the obtained assessment is to determine the suitability of the assessed interoperability specification for the delivery of interoperable European public services.

Background

CAMSS is the European guide for assessing and selecting standards and specifications for an eGovernment project, a reference when building an architecture, and an enabler for justifying the choice of standards and specifications in terms of interoperability needs and requirements. It is fully aligned with the European Standardisation Regulation 1025/2012.
The main objective of CAMSS is achieving interoperability and avoiding vendor lock-in by establishing a neutral and unbiased method for the assessment of technical specifications and standards in the field of ICT. This method will be compliant with Regulation 1025/2012 on European Standardisation.
While ICT solutions have specific characteristics at the political, legal, and organisational levels; semantic and technical interoperability are based mostly on technical specifications or standards. Within the context of the elaboration of their National Interoperability Frameworks, Member States organise the assessment of technical specifications or standards, in order to establish their national recommendations. Deciding on the recommended technical specifications or standards often calls for a resource-intensive and time-consuming assessment. In order to tackle this, the Digital Europe Programme (DEP) defines an action focused on the development of a common assessment method for standards and specifications (CAMSS).

The purpose of CAMSS is:

- to ensure that assessments of technical ICT specifications or standards and interoperability profiles are performed according to high and consistent standards;
- to ensure that assessments will contribute significantly to the confidence in the interoperability of systems implementing these specifications and profiles;
- to enable the reuse, in whole or in part, of such assessments;
- to continuously improve the efficiency and effectiveness of the assessment process for ICT technical specifications, standards, and interoperability profiles.

The expected benefits of the CAMSS are:

- Ensuring greater transparency throughout the selection of standards in the context of ICT strategies, architectures, and interoperability frameworks. This will be achieved through the establishment of a commonly agreed assessment method, assessment process, and a list of assessment attributes.

- Reducing resource and time requirements and avoiding duplication of efforts. (Partial) sharing of finalised assessments of standards and specifications.

- Allowing easier and faster assessments, and reusing the ones already performed through the creation and maintenance of a library of standards.

Your compliance level of the specification assessed depends on the scores you achieved in each section of the survey. Please see below the survey score conversion table below for guidance.

			Compliance Level		
Section	**Ad-hoc**	**Opportunistic**	**Essential**	**Sustainable**	**Seamless**
Principles setting the context for EU Actions on Interoperability	20	40	60	80	100
EIF Core Interoperability Principles	0 to 340	341 to 680	681 to 1020	1021 to 1360	1361 to 1700
EIF Principles Related to generic user needs and expectations	0 to 240	241 to 480	481 to 720	721 to 960	961 to 1200

EIF Foundation principles for cooperation among public administrations	0 to 100	101 to 200	201 to 300	301 to 400	401 to 500
EIF Interoperability Layers	0 to 200	201 to 400	401 to 600	601 to 800	801 to 1000

The following table shows the 'compliance levels' that a specification can reach depending on the assessment score.

Compliance Level	Description
Ad-hoc	Poor level of conformance with the EIF - The specification does not cover the requirements and recommendations set out by the EIF in this area.
Opportunistic	Fair level of conformance with the EIF - The specification barely covers the requirements and recommendations set out by the European Interoperability Framework in this area.
Essential	Essential level of conformance with the EIF - The specification covers the basic aspects set out in the requirements and recommendations from the European Interoperability Framework.
Sustainable	Good level of conformance with the EIF scenario - The specification covers all the requirements and recommendations set out by the European Interoperability Framework in this area.
Seamless	Leading practice of conformance level with the EIF - The specification fully covers the requirements and recommendations set out by the European Interoperability Framework in this area.

Contact: For any general or technical questions, please send an email to DIGIT-CAMSS@ec.europa.eu. Follow all activities related to the CAMSS on our CAMSS community page.

USER CONSENT

Disclaimer:
By no means will the Interoperability Specification assessment imply any endorsement of the EC to the assessed specification. Likewise, the use of CAMSS Assessment EIF Scenario implies that the user accepts that the EC is not liable on the assessment nor on any direct or indirect consequence/decision of such assesment.

The CAMSS Assessment EIF Scenario is based on EU Survey, by accepting the CAMSS Privacy Statement the user also accepts EU Survey Privacy Statement and the Terms of use.

* Please, fill in the mandatory* information to start the assessment

☑ *I have read and agreed to the following CAMSS Privacy Statement: here

□ I agree to be contacted for evaluation purposes, namely to share my feedback on specific DEP solutions and actions and on the DEP programme and the European Interoperability Framework in general.

This assessment is licensed under the European Union Public License (EUPL)

IDENTIFICATION

Information on the information provider

Your Last name

Your First Name

CAMSS Team

Your Position / Role

* Your Organisation

European Commission DG - DIGIT

Your Contact phone number

* Would you like to be contacted for evaluation purposes in the context of your assessment? To see how your data is handled, please check again the Privacy statement here

In case you would like to be contacted, please select "yes" and provide your email.

○ Yes
● No

* Where did you learn about CAMSS?

○ DEP Programme (DEP website, DEP social media)
○ Joinup (e.g., CAMSS Collection, Joinup social media)
● European Commission
○ Public Administrations at national, regional or local level
○ Standards Developing Organizations (SDOs)
○ Other

If you answered "Other" in the previous question, please specify how:

Information on the specification

* Specification type

Specification: Set of agreed, descriptive, and normative statements about how a specification should be designed or made.
Standard: Specification that is largely adopted and possibly endorsed.
Application Profile: An application profile "customises one or more existing specifications potentially for a given use case or a policy domain adding an end to end narrative describing and ensuring the interoperability of its underlying specification(s)".
Family: A family is a collection of interrelated and/or complementary specifications, standards, or application profiles and the explanation of how they are combined, used, or both.

● Specification
○ Standard
○ Application Profile
○ Family of Specification

* Title of the specification

DNS Queries over HTTPS (DoH) RFC 8484

* Version of the specification

15.0.0

* Description of the specification

DNS over HTTPS (DoH) is protocol for sending Domain Name System (DNS) queries and getting DNS responses over HTTP using HTTPS URIs. Each DNS query-response pair is mapped into an HTTP exchange. It establishes default media formatting types for requests and responses but uses normal HTTP content negotiation mechanisms for selecting alternatives that endpoints may prefer in anticipation of serving new use cases.

* URL from where the specification is distributed

https://datatracker.ietf.org/doc/html/rfc8484

* Name and website of the standard developing/setting organisation (SDO/SSO) of the specification

○ W3C (https://www.w3.org)
○ OASIS (https://www.oasis-open.org/)
○ IEEE (https://standards.ieee.org/)
○ ETSI (https://www.etsi.org/)
○ GS1 (https://www.gs1.fr/)
○ openEHR (https://www.openehr.org/)

● IETF (https://www.ietf.org/)
○ Other (SDO/SSO)

Contact information/contact person of the SDO
a) for the organisation
b) for the specification submitted

Information on the assessment of the specification

Reason for the submission, the need and intended use for the specification.

If any other evaluation of this specification is known, e.g. by Member States or European Commission projects, provide a link to this evaluation.

Considerations

Is the functional area of application for the formal specification addressing interoperability and eGovernment?

● YES
○ NO

Additional Information

The goal of DoH is to offer a standard protocol for performing remote DNS resolution via the HTTPS protocol. The integration with HTTP provides a transport suitable for both existing DNS clients and native web applications seeking access to the DNS. Thanks to DoH, user privacy and security is improved by preventing eavesdropping and manipulation of DNS data by man-in-the-middle attacks, which could improve eGovernment services.

EIF PRINCIPLES SETTING THE CONTEXT FOR EU ACTIONS ON INTEROPERABILITY

This category is related to the first underlying principle (UP) of the EIF Subsidiarity and Proportionality (UP1). The basis of this principle is to ensure that the EU Actions are taken or stated to improve national actions or decisions. Specifically, it aims to know if National Interoperability Frameworks are aligned with the EIF.

Please note that some of the questions have a prefilled answer depending on the SDO. To ensure it, please see that these questions include a help message that remarks it.

Subsidiarity and Proportionality

* **A1 - To what extent has the specification been included in a national catalogue from a Member State whose National Interoperability Framework has a high performance on interoperability according to National Interoperability Framework Observatory factsheets?**

EIF Recommendation 1: Ensure that national interoperability frameworks and interoperability strategies are aligned with the EIF and, if needed, tailor and extend them to address the national context and needs.

This criterion assesses if the specifications have been included within the National Catalogues of Specifications of the Member States that are highly aligned with the higher level of performance in terms of interoperability.

The Digital Public Administration Factsheets use three categories to evaluate the level of National Interoperability frameworks in accordance with the EIF. The three categories are 1. CONCEPTUAL MODEL FOR INTEGRATED PUBLIC SERVICES PROVISION; 2 INTEROPERABILITY LAYERS, and 3. INTEROPERABILITY PRINCIPLES. National Interoperability Frameworks reports can be found here: https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets-2021

○ Not Answered

○ Not Applicable

● The specification has not been included within the catalogue of any Member State.

○ The specification has been included within the catalogue of a Member State with a lower performance than stated in the Digital Public Administration Factsheets from the NIFO.

○ The specification has been included within the catalogue of a Member State with a middle-lower performance than stated in the Digital Public Administration Factsheets from the NIFO.

○ The specification has been included within the catalogue of a Member State with a middle-upper performance than stated in the Digital Public Administration Factsheets from the NIFO.

○ The specification has been included within the catalogue of a Member State with a higher performance than stated in the Digital Public Administration Factsheets from the NIFO.

* Justification

DoH is not included in any national catalogue of recommended specifications whose Member State NIF has a high performance on interoperability according to the NIFO factsheets.

CAMSS List of Standards:
https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-list-standards

2023 NIFO factsheets: https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets-2023

EIF CORE INTEROPERABILITY PRINCIPLES

In this category, elements related to the core interoperability principles (UP) are encompassed, which are: openness (UP 2), transparency (UP3), reusability (UP4), technological neutrality and data portability (UP5).

Openness

*** A2 - Does the specification facilitate the publication of data on the web?**

EIF Recommendation 2: Publish the data you own as open data unless certain restrictions apply.

Relates to the ability of the specification to publish data as open data or not.

○ Not Answered
● Not Applicable
○ The specification does not support the publication of data on the web.
○ The specification supports the publication of data on the web but under a non-open license.
○ The specification supports the publication of data on the web with an open license, but in an unstructured format.
○ The specification supports publication of data on the web with an open license and in a structured, machine-readable format.
○ In addition to the previous question, the specification does not require proprietary software for the processing of its related data.
○ In addition to the previous question, the specification is or incorporates open standards (e.g. W3C).

* Justification

DNS over HTTPS (DoH) is a protocol that encrypts DNS queries and their responses to enhance privacy and security, therefore it is not directly related to the publication of data on the web.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

*** A3 - To what extent do stakeholders have the opportunity to contribute to the development of the specification?**

EIF Recommendation 3: Ensure a level playing field for open-source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.

Relates to in which measure the different stakeholders that a specification can benefit have the opportunity to participate in the working groups focused on the development of certain specifications.

○ Not Answered
○ Not Applicable
○ There is no information on the working group of the specification.
○

The working group is open to participation by any stakeholder but requires registration, fees, and membership approval.

○ The working group is open to participation by any stakeholder but requires fees and membership approval.

○ The working group is open to participation following a registration process.

● The working group is open to all without specific fees, registration, or other conditions.

Justification:

IETF 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.
Each distinct version of an Internet standards-related specification is published as part of the "Request for Comments" (RFC) document series. This archival series is the official publication channel for Internet standards documents and other publications.
During the development of a specification, draft versions of the document are made available for informal review and comment by placing them in the IETF's "Internet-Drafts" directory, which is replicated on a number of Internet hosts. This makes an evolving working document readily available to a wide audience, facilitating the process of review and revision.

Standard process IETF:
https://www.ietf.org/standards/process/

Internet Best Current Practices IETF:
https://tools.ietf.org/html/rfc2026

Additional Information

In case you need to add further justification.

* **A4 - To what extent is a public review part of the release lifecycle?**

EIF Recommendation 3: Ensure a level playing field for open-source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.

A public review consists of the public availability of the specification's draft for stakeholders to provide inputs for the improvement and fix of possible bugs.

○ Not Answered

○ Not Applicable

○ Specification releases do not foresee public reviews.

○ Public review is applied to certain releases depending on the involved changes.

○ All major releases foresee a public review.

○ All major and minor releases foresee a public review but, during which, collected feedback is not publicly visible.

● All major and minor releases foresee a public review during which collected feedback is publicly visible.

Justification:

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 process of creating and Internet Standard is straightforward: a specification undergoes a period of development and several

iterations of review by the Internet community and revision based upon experience, is adopted as a Standard by the appropriate body... and is published. In practice, the process is more complicated, due to (1) the difficulty of creating specifications of high technical quality; (2) the need to consider the interests of all the affected parties; (3) the importance of establishing widespread community consensus; and (4) the difficulty of evaluating the utility of a particular specification for the Internet community. The goals of the Internet Standards Process are:
- Technical excellence;
- prior implementation and testing;
- clear, concise, and easily understood documentation;
- openness and fairness; and
- timeliness.
The goal of technical competence, the requirement for prior implementation and testing, and the need to allow all interested parties to comment all require significant time and effort. The Internet Standards Process is intended to balance these conflicting goals. The process is believed to be as short and simple as possible without sacrificing technical excellence, thorough testing before adoption of a standard, or openness and fairness.

Standard process IETF:
https://www.ietf.org/standards/process/

Additional Information

In case you need to add further justification.

* **A5 - To what extent do restrictions and royalties apply to the specification's use?**

EIF Recommendation 3: Ensure a level playing field for open-source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.

Additionally to the EIF's recommendation that refers to open-source software it applies to a specification in itself at any interoperability level (legal, organisational, semantic, or technical)

○ Not Answered
○ Not Applicable
○ The specification has no public definition of its Intellectual Property Right (IPR) policy or licence.
○ Use of the specification is restricted and requires the payment of royalty fees.
○ Use of the specification is royalty-free but imposes an Intellectual Property Right (IPR) policy or licence that goes against Fair, Reasonable and Non-Discriminatory (F/RAND) principles.
● Use of the specification is royalty-free and its Intellectual Property Right (IPR) policy or licence is aligned with Fair, Reasonable and Non-Discriminatory (F/RAND) principles.

Justification:
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. Therefore it is licensed on a royalty-free basis. No IPR disclosures have been submitted directly on this RFC.

Intellectual Property Rights in IETF:
https://datatracker.ietf.org/doc/html/rfc8179

Additional Information

In case you need to add further justification.

* **A6 - To what extent is the specification sufficiently mature for its use in the development of digital solutions/services?**

EIF Recommendation 4: Give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support, and innovation.

Maturity related to the stability of the specification, meaning that it has been evolved enough and mechanisms for its development have been put in place (Change Management processes, monitoring, etc.)

○ Not Answered
○ Not Applicable
○ The specification has no published releases and no publicly accessible information on its development state.
○ The specification is under development without published releases.
○ The specification is under development with published preview releases.
○ The specification has published major releases but without public documentation on its supporting processes (e.g. change management and release management).
● The specification, in addition to having major releases available, has published documentation on its supporting processes (e.g. change management and release management).

* Justification

RFC 8484 is currently on its 15th version, published in 2018 and has a public document history where any action related to the specification's content is reported. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). The process of creating a standard under IETF is clear: a specification undergoes a period of development and several iterations of review by the Internet community and revision based upon experience are taken place. Furthermore, The IETF welcomes the critical evaluation of protocols and has provided guidance for it.

RFC 8484 History: https://datatracker.ietf.org/doc/rfc8484/history/

IESG IETF: https://www.ietf.org/about/groups/iesg/

Standard process IETF: https://www.ietf.org/standards/process/

Protocol Vulnerabilities IETF: https://www.ietf.org/standards/rfcs/vulnerabilities/

* **A7 - To what extent has the specification sufficient market acceptance for its use in the development of digital solutions/services?**

EIF Recommendation 4: Give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support, and innovation.

Relates to how the specification is supported by the market, taking as a reference whether or not the specifications are widely used or implemented. There is an exception, and it is when the specification is used to implement innovative solutions, then, the specification should not be considered as failing to meet the requirements of the criterion.

○

Not Answered

○ Not Applicable

○ There is no information about the specification's market uptake.

○ The specification has known implementations but not enough to indicate market acceptance.

○ The specification has widespread use indicating market acceptance.

○ The specification has widespread use and relevant independent reports proving its market acceptance.

● The specification does not have market acceptance because it is directly used to create innovative solutions.

* Justification

DNS over HTTPS (DoH) is the foundation for many different innovative solutions. For instance, BIND 9 by the Internet Systems Consortium (ISC). BIND (9.17.10) comes with initial support for DNS-over-HTTPS (DoH). Deployment of DoH is also a significant stepping stone for wider adoption of the Encrypted Client Hello (ECH) and Encrypted Server Name Indication (ESNI) features of the Transport Layer Security (TLS) protocol. These features further improve users' privacy by preventing third parties from snooping, and by making it harder to block websites by analysing and intercepting TLS handshake requests.

ISC DoH in BIND 9: https://www.isc.org/blogs/bind-implements-doh-2021/

Transport Layer Security (TLS) Protocol RFC 8446: https://www.rfc-editor.org/rfc/rfc8446

*** A8 - To what extent has the specification support from at least one community?**

EIF Recommendation 3: Ensure a level playing field for open-source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.

Related to whether or not communities exist around the specification at any level legal, organisational, semantic, or technical contributions to its enhancement and development.

○ Not Answered

○ Not Applicable

○ There is no community linked to the specification.

○ Specification support is available but as part of a closed community requiring registration and possibly fees.

○ There is no specific community to support the specification but there are public channels for the exchange of help and knowledge among its users.

○ There is a community providing public support linked to the specification but in a best-effort manner.

● There is a community tasked to provide public support linked to the specification and manage its maintenance.

* Justification

DNS over HTTPS (DoH) is maintained by the Internet Engineering Task Force (IETF). The development and maintenance of DoH is carried out within the Internet Engineering Steering Group (IESG), who is responsible for technical management of IETF activities and the Internet standards process. Furthermore, there is a section in the RFC Editor where any user can report doubts or comments regarding RFC 8484.

IESG IETF: https://www.ietf.org/about/groups/iesg/

RFC 8484 Editor Errata: https://www.rfc-editor.org/errata/rfc8484

Transparency

* **A9 - To what extent does the specification enable the visibility of administrative procedures, rules data, and services?**

EIF Recommendation 5: Ensure internal visibility and provide external interfaces for European public services.

○ Not Answered
● Not Applicable
○ The specification hinders visibility.
○ The specification neither promotes nor hinders visibility.
○ The specification can contribute and promote the visibility of administrations, but it is not its main purpose.
○ The specification can enable the visibility of administrations if combined with other specifications.
○ The specification actively promotes and supports visibility.

* Justification

While DoH enhances the confidentiality of DNS queries, visibility into administrative procedures, rules data, and services is more closely associated with other technologies and standards. For visibility into web services, you might consider protocols like HTTP, HTTPS, or APIs that define how data and services are accessed and interacted with over the web.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

* **A10 - To what extent does the specification scope comprehensibly administrative procedures, rules data, and services?**

EIF Recommendation 5: Ensure internal visibility and provide external interfaces for European public services.

○ Not Answered
● Not Applicable
○ The specification hinders comprehensibility.
○ The specification neither promotes nor hinders comprehensibility.
○ The specification can contribute and promote the comprehensibility of administrations, but it is not its main purpose.
○ The specification can scope the comprehensibility of administrations if combined with other specifications.
○ The specification actively promotes and supports comprehensibility.

* Justification

While DoH plays a crucial role in enhancing the security and privacy of DNS communication, it doesn't comprehensively address or provide visibility into administrative procedures, rules data, or services. These aspects are typically managed through other networking protocols, configurations, and tools at different layers of the networking stack.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

* **A11 - To what extent does the specification enable the exposure of interfaces to access the public administration's services?**

EIF Recommendation 5: Ensure internal visibility and provide external interfaces for European public services.

Relates to ensuring availability of interfaces with internal information systems. As the EIF defines: *Public administrations operate a large number of what are often heterogeneous and disparate information systems in support of their internal processes. Interoperability depends on ensuring the availability of interfaces to these systems and the data they handle. In turn, interoperability facilitates the reuse of systems and data and enables these to be integrated into larger systems.*

○ Not Answered
○ Not Applicable
○ The specification prevents the exposure of such interfaces.
○ The specification neither promotes nor hinders the exposure of such interfaces.
● The specification can contribute to the exposure of interfaces, but it is not its main purpose.
○ The specification can enable the exposure of interfaces if combined with other specifications.
○ The specification enables exposure of such interfaces.

* Justification

While DoH does not directly enable or expose interfaces for accessing public administration services, it may be used by applications to perform DNS resolution to reach public administration services. DoH facilitates secure communication between clients (such as web browsers or applications) and servers hosting the services. HTTPS, in particular, ensures secure and encrypted communication, providing confidentiality and integrity for the exchanged data, which would indirectly help by making API access more secure and reliable or bypass DNS-based filtering or blocking

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

Reusability

*** A12 - To what extent is the specification usable beyond the business-specific domain, allowing its usage across business domains?**

EIF Recommendation 6: Reuse and share solutions, and cooperate in the development of joint solutions when implementing European public services.

Relates to the use of the specification beyond a specific business domain. E.g. a specification developed under the eHealth domain that can be used in other domains or not.

○ Not Answered
○ Not Applicable
○ The specification is tied to a specific domain and is restricted from being implemented or used in other domains.
○ The specification is associated with a specific domain but its implementation and/or use in other domains is difficult.
○ The specification is associated with a specific domain but could be partially implemented and/or used in other domains.
○ The specification is associated with a specific domain but could be implemented and/or used 'as-is' to other domains.
● The specification is domain-agnostic, designed to be implemented and/or used in any domain.

* Justification

DNS over HTTPS (DoH) usability extends beyond a specific business domain, and it can be employed across various sectors and contexts. DoH can be used by individuals, organisations, and businesses across different industries for securing DNS traffic. Any entity, regardless of the business domain, can benefit from using DoH to protect sensitive information and prevent eavesdropping on DNS traffic.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

Technological Neutrality and Data Portability

* A13 - Is the specification technology agnostic?

EIF Recommendation 8: Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs.

Technology-neutrality relates to not being dependent on any other ("sister") specifications, and platform-neutrality, not being dependent on any specific environment, web platform, operating system.

○ Not Answered
○ Not Applicable
○ NO
● YES

* Justification

DNS over HTTPS (DoH) is designed to be technology agnostic meaning that it operates at the application layer of the networking stack and can be implemented across different platforms and technologies. DoH focuses on securing the communication between clients (such as web browsers or applications) and DNS resolvers by encrypting DNS queries using the HTTPS protocol.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

* A14 - Is the specification platform agnostic?

EIF Recommendation 8: Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs.

Technology-neutrality relates to not being dependent on any other ("sister") specifications, and platform-neutrality, not being dependent on any specific environment, web platform, operating system.

○ Not Answered
○ Not Applicable
○ NO
● YES

* Justification

DNS over HTTPS (DoH) is designed to be platform agnostic. It operates at the application layer of the networking stack, and its implementation is independent of specific operating systems or platforms. This platform agnosticism allows for consistent usage across various devices and environments.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

*** A15 - To what extent does the specification allow for partial implementations?**

EIF Recommendation 8: Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs.

Partial implementations refer to the application of specifications, not in their whole, but part of the requirements or features defined in the documentation.

It can also be understood as the implementation of different profiles, which is also related to a certain set of requirements depending on the context of implementation.

○ Not Answered
○ Not Applicable
○ The specification is only meant to be used as a whole.
○ The specification could be partially implemented but does not make specific provisions towards this.
○ The specification could be partially implemented but includes only guidelines towards this rather than sets of requirements.
○ The specification explicitly foresees sets of requirements that can be implemented incrementally.
● The specification explicitly foresees sets of requirements that can be implemented incrementally or separately.

* Justification

DNS over HTTPS (DoH) allows for partial implementations. Implementing DoH can be done selectively for specific clients, applications, or DNS queries, rather than applying it universally across an entire network. This flexibility enables organizations to adopt DoH gradually or in a targeted manner. For instance, organisations can adopt DoH gradually by implementing it on a subset of devices or services.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

*** A16 - Does the specification allow customisation?**

EIF Recommendation 8: Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs.

A clear example of customizations is Core Vocabularies, which define a set of general requirements that could fit in any context and allow for the customization to fit specific business requirements in the implementation.

○ Not Answered
○ Not Applicable
○ NO
● YES

* Justification

DNS over HTTPS (DoH) allows for customisation but the extent of customisation may vary depending on the DNS resolver or client software being used. For instance, ssers and administrators can choose the specific DNS resolver that supports DoH. In addition, users can also specify the URLs of the DoH servers they want to use, allowing flexibility in choosing service providers.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

* **A17 - Does the specification allow extension?**

EIF Recommendation 8: Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs.

A clear example of extension is Core Vocabularies, which are a set of general requirements fitting in different contexts that can complement each other in a sort of extensibility practice to fit specific business requirements in any implementation.

○ Not Answered
○ Not Applicable
○ NO
● YES

* Justification

DNS over HTTPS (DoH) is designed to be extensible, enabling the addition of new features, options, or improvements over time. This extensibility is crucial for accommodating evolving requirements, addressing new challenges, and incorporating feedback from the user community. DoH uses option codes to enable the inclusion of additional parameters or features in DNS queries and responses and provides a flexible structure that allows for the inclusion of extensions while maintaining compatibility with existing implementations.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

* **A18 - To what extent does the specification enable data portability between systems/applications supporting the implementation or evolution of European public services?**

EIF Recommendation 9: Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evolution of European public services without unjustified restrictions, if legally possible.

○ Not Answered
○ Not Applicable
○ The specification prevents or does not support data portability.
○ The specification neither addresses data portability nor prevents it.
○ The specification addresses data portability but without specific provisions to enable it.
● The specification introduces certain aspects that can contribute to enabling data portability.
○ The specification explicitly addresses and enables data portability.

* Justification

DNS over HTTPS (DoH) can contribute to data portability between systems and applications as it secures DNS (Domain Name System) queries by encrypting the communication between the client and the DNS resolver, which is crucial in security and privacy matters. It allows secure access to data, avoids censorship filters, and improves overall privacy allowing for a secure environment for data portability.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

EIF PRINCIPLES RELATED TO GENERIC USER NEEDS AND EXPECTATIONS

This category includes all underlying principles from the EIF which are related to user needs. Principles included here are user-centricity (UP6), inclusion and accessibility (UP7), security and privacy (UP8), and multilingualism (UP9).

User-Centricity

*** A19 - To what extent does the specification allow relevant information to be reused when needed?**

EIF Recommendation 13: As far as possible under the legislation in force, ask users of European public services once-only and relevant-only information.

The Once-Only Principle is related to making the operations or transactions between administrations and stakeholders more efficient. It implies avoiding the provision of certain data or information twice or more when this information is already available for public administrations.
First European Data Space, Once Only Technical System (OOTS):
https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Once+Only+Technical+System
Additional and relevant information can be found here: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Principle

○ Not Answered
○ Not Applicable
○ Information needs to be provided whenever this is needed.
○ There is limited reuse of provided information.
○ Provided information is reused, but this is not consistently done.
● Provided information is reused, but not in all scenarios.
○ Information is provided once-only and reused as needed.

* Justification

Within the DoH protocol, information (in this case, DNS query responses) is effectively provided once and then reused as necessary, leveraging caching mechanisms to optimize web browsing experience and network efficiency while maintaining privacy and security. In section 5.1 of the specification, Cache Interaction is explained, where caching mechanisms can be filtered and adjusted depending on the assigned HTTP freshness lifetime.

Section 5.1 DoH specification: https://datatracker.ietf.org/doc/html/rfc8484#section-5.1

Inclusion and Accessibility

*** A20 - To what extent does the specification enable the e-accessibility?**

EIF Recommendation 14: Ensure that all European public services are accessible to all citizens, including persons with disabilities, the elderly, and other disadvantaged groups. For digital public services, public administrations should comply with e-accessibility specifications that are widely recognised at the European or international level.

Examples of specifications addressing e-accessibility are, for instance, WAI-ARIA (https://www.w3.org/WAI/standards-guidelines/aria/) included within Web Content Accessibility Guidelines (WCAG) Overview (https://www.w3.org/WAI/standards-guidelines/wcag/).

○ Not Answered
● Not Applicable
○ The specification prevents or does not support e-accessibility.
○ The specification neither addresses e-accessibility nor prevents it.
○ The specification can contribute and promote e-accessibility, but it is not its main purpose.
○ The specification can enable e-accessibility if combined with other specifications.
○ The specification explicitly addresses and enables e-accessibility.

* Justification

The purpose of the DNS Queries over HTTPS (DoH) is not related to e-accessibility. Therefore, this criterion is considered not applicable to this specification.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

Privacy

*** A21 - To what extent does the specification ensure the protection of personal data managed by Public Administrations?**

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

Relates to the actions that Public Administrations establish concerning sensitive information for the proper delivery of public services. The different actions imply the reception, classification, and exchange of such information.

Securing the right to the protection of personal data, by respecting the applicable legal framework for the large volumes of personal data of citizens, held and managed by Public administrations.

○ Not Answered
○ Not Applicable
○ The specification hinders the protection of personal data.
○ The specification does not address the protection of personal data but neither prevents it.
○ The specification includes certain data protection considerations but without being exhaustive.
● The specification explicitly addresses data protection but without referring to relevant regulations.
○ The specification explicitly addresses data protection and its alignment to relevant regulations.

* Justification

DoH encrypts DNS queries, making it more challenging for third parties, including Internet Service Providers (ISPs), to intercept and analyse the content of DNS requests. This encryption adds a layer of confidentiality to the communication, but it does not directly address other aspects of data protection, such as data retention or access policies. It does not extend its protection to other layers of the communication stack or to the handling of personal data within applications or services.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

*** A22 - Does the specification provide means for restriction of access to information/data?**

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

The principle of confidentiality defines that only the sender and the intended recipient(s) must be able to create the content of a message. Confidentiality have compromised if an unauthorized person is able to create a message.

○ Not Answered
○ Not Applicable
○ The specification prevents or does not support the implementation of confidentiality mechanisms/features.
○ The specification neither addresses confidentiality nor prevents it.
○ The specification addresses confidentiality but without specific provisions to enable it.
○ The specification introduces certain aspects that can contribute to enabling confidentiality.
● The specification explicitly addresses and enables the implementation of features to guarantee confidentiality.

* Justification

DNS Queries over HTTPS (DoH) security and privacy considerations are based on RFC 8446, IETF's Transport Layer Security (TLS) Protocol. The standard defines confidentiality and how the record layer of the protocol should provide it. AEAD encryption provides confidentiality and integrity for the data.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

Transport Layer Security (TLS) Protocol RFC 8446: https://www.rfc-editor.org/rfc/rfc8446

*** A23 - Is the specification included in any initiative at European or National level covering privacy aspects?**

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

Securing the right to the protection of personal data, by respecting the applicable legal framework for the large volumes of personal data of citizens, held and managed by Public administrations.

Relates to the actions that Public Administrations establish concerning sensitive information for the proper delivery of public services. The different actions imply the reception, classification, and exchange of such information.

For example, the ETSI (Electronic Signatures and Infrastructures) family of specifications are part of the trust establishment of the eDelivery solution, ensuring that its implementation is salient to guarantee security and privacy.

○

Not Answered

○ Not Applicable

○ Yes, but at national or regional level.

● Yes, at European level.

* Justification

DNS Queries over HTTPS (DoH) is included in the EU-funded SAPPAN project, which seeks to introduce a privacy-preserving sharing and automation platform to facilitate efficient response to and recovery from cyberattacks. DoH has been created to improve users' privacy on the internet and it will develop a cyberthreat intelligence system to assist security and IT personnel within and across organisations in timely responding to threats.

SAPPAN Project: https://sappan-project.eu/

DoH Insight: https://dl.acm.org/doi/10.1145/3407023.3409192

Security

Data processing and exchange

*** A24 - To what extent does the specification enable the secure exchange of data?**

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

This relates to the actions that Public Administrations establish concerning sensitive information for the proper delivery of public services. The different actions imply the reception, classification, and exchange of such information.

○ Not Answered

○ Not Applicable

○ The specification prevents or does not support the secure and trustworthy exchange of data.

○ The specification introduces certain aspects that can contribute to enabling the secure exchange of data.

○ The specification addresses data security and trustworthy data exchange but does not foresee specific provisions to enable them.

○ The specification addresses data security and trustworthy data exchange but specific provisions to enable them are limited.

● The specification explicitly addresses and enables the secure and trustworthy exchange of data.

* Justification

DNS over HTTPS (DoH) enhances the security of data exchange at the DNS layer by encrypting DNS queries and responses. It provides a layer of confidentiality and integrity for these communications. Section 4 of the protocol focuses on the HTTPS Exchange, from the request where a DoH client encodes a single DNS query into an HTTP request, to the response.

Section 4 DoH specification: https://datatracker.ietf.org/doc/html/rfc8484#section-4

* **A25 - To what extent does the specification enable the secure processing of data?**

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

Relates to the actions that Public Administrations establish concerning sensitive information for the proper delivery of public services. The different actions imply the reception, classification, and exchange of such information.

- ○ Not Answered
- ○ Not Applicable
- ○ The specification prevents or does not support the secure and trustworthy processing of data.
- ○ The specification introduces certain aspects that can contribute to enabling the secure processing of data.
- ● The specification addresses data security and trustworthy data processing but does not foresee specific provisions to enable them.
- ○ The specification addresses data security and trustworthy data processing but specific provisions to enable them are limited.
- ○ The specification explicitly addresses and enables the secure and trustworthy processing of data.

* Justification

DNS over HTTPS (DoH) primarily focuses on securing the transport of DNS queries and responses, adding an additional layer of security to the DNS resolution process. DoH significantly improves online security and privacy by securing DNS queries and minimizing exposure of sensitive information during resolution processes, which is crucial in secure processing of data.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

Data authenticity

* **A26 - To what extent the specification guarantees the authenticity and authentication of the roles agents involved in the data transactions?**

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

Authentication defines that users are who they request to be. Availability defines that resources are available by authorized parties; “denial of service” attacks, which are the subject matter of national news, are attacks against availability. The concerns of information security professionals are access control and Nonrepudiation. Authorization defines the power that it can have over distinguishing authorized users from unauthorized users, and levels of access in-between. Authenticity defines the constant checks that it can have to run on the system to make sure sensitive places are protected and working perfectly.”

- ○ Not Answered
- ○ Not Applicable
- ○ The specification prevents or does not support the implementation of authentication features.
- ○ The specification neither addresses authenticity nor prevents it.
- ○ The specification addresses the implementation of authenticity features but without specific provisions to enable it.
- ● The specification introduces certain aspects that can contribute to enabling authenticity features.

○ The specification explicitly addresses and enables the implementation of authenticity features.

* Justification

DoH encrypts DNS traffic and requires authentication of the server. DoH improves the security of DNS queries by guaranteeing the authenticity of DNS resolves over HTTPS, thus preventing certain types of cyber-attacks and ensuring that the communication has not been tampered with. However, the typical use of DoH focuses on server authentication (authenticity) and does not usually involve explicit client authentication beyond the basic security measures provided by HTTPS such as SSL/TLS certificates to authenticate the identity of the server.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

Data integrity

*** A27 - To what extent information is protected against unauthorised changes?**

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

Integrity defines that information is protected against unauthorized changes that are not perceptible to authorized users; some incidents of hacking compromise the integrity of databases and multiple resources.

○ Not Answered
○ Not Applicable
○ The specification prevents or does not support the implementation of data integrity mechanisms /features.
○ The specification neither addresses data integrity nor prevents it.
○ The specification addresses data integrity but without specific provisions to enable it.
○ The specification introduces certain aspects that can contribute to enabling data integrity.
● The specification explicitly addresses and enables the implementation of features to guarantee data integrity.

* Justification

DNS over HTTPS (DoH) provides protection against unauthorized changes to DNS information by encrypting DNS queries and responses, thereby ensuring the integrity of the data during transmission and preventing DNS spoofing and tampering. However, the HTTPS connection does not provide the response integrity of DNS data provided by DNSSEC.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

Data accuracy

*** A28 - To what extent does the specification ensure and enable data processing accuracy?**

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

The accuracy and completeness of information systems and the data supported within the systems should be an administration concern. The information which has been inappropriately changed or destroyed (by external or employees) can impact the organization. Each organization should make controls to provide that data entered into and saved in its automated files and databases are complete and accurate and provide the accuracy of disseminated data.

○ Not Answered
○ Not Applicable
○ The specification prevents or does not support the implementation of data accuracy mechanisms/features.
○ The specification neither addresses data accuracy nor prevents it.
● The specification addresses data accuracy but without specific provisions to enable it.
○ The specification introduces certain aspects that can contribute to enabling data accuracy.
○ The specification explicitly addresses and enables the implementation of features to guarantee data accuracy.

* Justification

DNS over HTTPS (DoH) primarily focuses on securing the DNS (Domain Name System) communication by encrypting DNS queries and responses. While DoH ensures the confidentiality and integrity of DNS transactions, it does not directly address data processing accuracy beyond the DNS layer. Even so, concepts like mitigation of DNS spoofing and authentication of DNS resolvers help improve data processing accuracy as it ensures the security and authenticity of every data exchange.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

Access Control

*** A29 - To what extent does the specification provide an access control mechanism?**

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

The principle of access control decides who must be able to access what. For example, it must be able to define that user A can view the data in a database, but cannot refresh them. User A can be allowed to create updates as well. An access-control mechanism can be installed to provide this. Access control is associated with two areas including role management and rule management. Role management applies on the user side, whereas rule management targets the resources side.

○ Not Answered
○ Not Applicable
○ The specification does not provide access control mechanisms.
○ The specification neither addresses nor prevents access control mechanisms.
○ The specification addresses access control mechanisms but without specific provisions to enable them.
● The specification introduces certain aspects that can contribute to enabling access control mechanisms.
○ The specification explicitly foresees a set of requirements for the enabling of access control mechanisms.

* Justification

DNS over HTTPS (DoH) primarily focuses on securing the communication between clients and DNS resolvers by encrypting DNS queries and responses. While DoH itself does not define access control mechanisms in the traditional sense, it relies on the existing security mechanisms of the HTTPS protocol, including server authentication through digital certificates.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

Multilingualism

*** A30 - To what extent could the specification be used in a multilingual context?**

EIF Recommendation 16: Use information systems and technical architectures that cater to multilingualism when establishing a European public service. Decide on the level of multilingualism support based on the needs of the expected users.

○ Not Answered
○ Not Applicable
○ The specification cannot be used in a multilingual context.
○ The specification could be used in a multilingual context but has no specific provisions to facilitate this.
● The specification foresees limited support for multilingualism.
○ The specification foresees support for multilingualism but this is not complete.
○ The specification is designed to fully support multilingualism.

* Justification

The DNS over HTTPS (DoH) protocol itself is language-agnostic, and its functionality is not dependent on the language used for communication. Additionally, the User-Agent and Accept-Language request header fields often convey specific information about the client version or locale but, these aspects are typically addressed at the application layer rather than in the DoH protocol itself.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

EIF FOUNDATION PRINCIPLES FOR COOPERATION AMONG PUBLIC ADMINISTRATIONS

This category includes the criteria aiming to evaluate principles related to collaboration amongst public organisations, business, and citizens. This is related to the underlying principles of administrative simplification (UP10), preservation of information (UP11), and assessment of effectiveness and efficiency (UP12).

Administrative Simplification

*** A31 - Does the specification simplify the delivery of European public services?**

EIF Recommendation 17: Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users’ requests and reduce the administrative burden on public administrations, businesses and citizens.

A positive answer would cover every specification easing digitalisation and administratice simplification by for example helping an Identification service access a Digital Portfolo with citizens information.

○ Not Answered
○ Not Applicable
○ NO
● YES

* Justification

DNS over HTTPS (DoH) itself does not directly simplify the delivery of European public services. However, it can impact positively on the delivery of European public services as it improves security and privacy measures and facilitates interoperability between systems, which can be useful when establishing a reliable infrastructure.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

* **A32 - Does the specification enable digital service delivery channels?**

EIF Recommendation 17: Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens.

A positive answer would cover that a specification eases or provides better means of delivering public services as a good asset for digitalisation and administrative simplification. For instance, a specification directly related to API performance easing and improving the delivery of a Digital Public Service through an API.

○ Not Answered
● Not Applicable
○ NO
○ YES

* Justification

DNS over HTTPS (DoH) is not directly designed to enable digital service delivery channels. Instead, DoH contributes to the security of DNS transactions. Therefore, this criterion is considered not applicable to this specification.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

Preservation of Information

* **A33 - To what extent does the specification enable the long-term preservation of data/information /knowledge (electronic records included)?**

EIF Recommendation 18: Formulate a long-term preservation policy for information related to European public services and especially for information that is exchanged across borders.

Relates to the capacity of the specification to contribute to the long-term preservation of information.

○ Not Answered

● Not Applicable
○ The specification prevents or does not support long-term preservation.
○ The specification neither addresses the long-term preservation nor prevents it.
○ The specification addresses the long-term preservation of electronic resources (information, data, etc) in a limited manner.
○ The specification addresses long-term preservation of electronic resources (information, data, etc), but not in a complete manner.
○ The specification explicitly addresses and enables long-term preservation.

* Justification

DNS over HTTPS (DoH) is not designed to address the long-term preservation of data, information, or knowledge, including electronic records. DoH is a protocol that focuses on securing the DNS (Domain Name System) communication by encrypting DNS queries and responses.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

Assessment of Effectiveness and Efficiency

*** A34 - To what extent are there assessments of the specification's effectiveness?**

EIF Recommendation 19: Evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality, and balance between costs and benefits.

Related to the degree to which the specification is effective while using it. There are indirect methods to determine that the specification is effective, for instance when a solution that has an effective performance and uses the specification to deliver the expected service.

Effectiveness: *the extent to which the specifications reach the expected action according to its purpose.*

○ Not Answered
○ Not Applicable
○ There are no such assessments.
○ There are such assessments that indirectly address the specification.
○ There are such assessments evaluating digital solutions' effectiveness that involve the specification.
○ There are such assessments addressing the specification and its effectiveness together with other specifications.
● There are such assessments directly addressing the specification.

* Justification

The effectiveness of DNS over HTTPS (DoH) is often evaluated through various means, including practical implementations and pilot projects. A 2019-paper related to the 17th International Conference on Emerging eLearning Technologies and Applications (ICETA) discusses DNS security in V2X networks and highlights DoH as a way to secure name services in V2X networks, which demonstrates the effectiveness of the specification.

An overview of DNS security in V2X networks: https://ieeexplore.ieee.org/abstract/document/9040111

* **A35 - To what extent are there assessments of the specification's efficiency?**

EIF Recommendation 19: Evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality, and balance between costs and benefits.

Related to the good use of time and resources not wasted unnecessarily by a specification being used. There are indirect methods to determine that the specification is efficient, for instance, a solution delivering a service with an efficient performance that uses the specification.

Efficiency: times and means needed to achieve the results using the specification.

○ Not Answered
○ Not Applicable
○ There are no such assessments.
○ There are such assessments that indirectly address the specification.
○ There are assessments evaluating digital solutions' efficiency that involve the specification.
○ There are such assessments addressing the specification and its efficiency together with other specifications.
● There are such assessments directly addressing the specification.

* Justification

Assessments of the efficiency of DNS over HTTPS (DoH) primarily involve evaluating the performance, scalability, and practicality of implementations. For instance, a 2020-paper related to the 3rd International Conference on Information and Computer Technologies (ICICT) describes the impact of DoH on cyber systems. The assessment explains that DoH is one of the latest enhancements implemented to address security against malware and other vulnerabilities, which proves the specification's efficiency.

On the Impact of DNS Over HTTPS Paradigm on Cyber Systems: https://ieeexplore.ieee.org/abstract/document/9092077

EIF INTEROPERABILITY LAYERS

This category is aligned with the related interoperability models described in the EIF and apply to all the public services. It includes six layers: interoperability governance, integrated public service governance, legal interoperability, organisational interoperability, semantic interoperability, and technical interoperability covered by criteria A2 to A10 under the Openness category.

Interoperability Governance

* **A36 - Is the (or could it be) specification mapped to the European Interoperability Architecture (EIRA)?**

EIF Recommendation 20: Ensure holistic governance of interoperability activities across administrative levels and sectors.

The EIRA defines the required capabilities for promoting interoperability as a set of Architecture Building Blocks (ABBs). The association of specification to these ABBs means the capacity to enable Legal, Organisational, Semantic, or Technical aspects needed for the development of interoperable public services. This association can be taken from ELIS the EIRA Library of Interoperability Specifications (ELIS) but also can be established ad-hoc.

○ Not Answered
○ Not Applicable
○ NO
● YES

* Justification

DNS Queries over HTTPS (DoH) is associated with EIRA ABB's in the EIRA Library of Interoperability Specifications (ELIS). More specifically, DoH is associated with the "Integrity Verification" ABB from the Technical Application view, and the "Domain Name Service" ABB from the Technical-Infrastructure View.

EIRA Library of Interoperability Specifications (ELIS):
https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elis/release/600rf

* **A37 - To what extent can the conformance of the specification's implementations be assessed?**

EIF Recommendation 21: Put in place processes to select relevant standards and specifications, evaluate them, monitor their implementation, check compliance and test their interoperability.

Relates to the implementation of the specification being conformant with the requirements established in the text of the specification. There are different methods to ensure the conformance of an implementation: check manually if the implementation meets the requirements in the specification text (if any), use additional methods or resources provided to this purpose or use specific tools provided by the SDO developing the specification.

○ Not Answered
○ Not Applicable
○ The specification does not include a definition of conformance.
○ The specification defines conformance but not as a set of measurable requirements.
○ The specification defines conformance as requirements that can be measured manually.
● The specification defines conformance as requirements with resources to enable automated measurement.
○ The specification is complemented by a conformance testing platform to allow testing of implementations.

* Justification

Conformance requirements of DNS queries over HTTPS (DoH) are expressed with a combination of descriptive assertions. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in the normative parts of this document are to be interpreted as described in BP14.

BCP 14: https://www.rfc-editor.org/info/bcp14

* **A38 - Is the specification recommended by a European Member State?**

EIF Recommendation 23: Consult relevant catalogues of standards, specifications, and guidelines at the national and EU level, in accordance with your NIF and relevant DIFs, when procuring and developing ICT solutions.

Recommended specifications are these specifications that the Member States provide as examples for the implementation of certain digital public services or for being used when procuring these digital public services or solutions.

○ Not Answered

● Not Applicable
○ NO
○ YES

* Justification

No he encontrado aparentemente ninguna recomendacion, si sabes de alguna pagina estaria bien.

*** A39 - Is the specification selected for its use in a European Cross-border project/initiative?**

EIF Recommendation 23: Consult relevant catalogues of standards, specifications, and guidelines at national and EU level, in accordance with your NIF and relevant DIFs, when procuring and developing ICT solutions.

The European Commission set up a process for the identification and assessment of specifications for its use in the development of IT solutions and also when procuring them. Find here the commission implementing decisions that include the specifications identified by the European Commission: https://ec.europa.eu/growth/single-market/european-standards/ict-standardisation/ict-technical-specifications_en

Additionally, there could be other situations where a specification can be selected for European projects or initiatives out of the scope of the above-mentioned context. These specifications can be considered positively in this assessment.

○ Not Answered
○ Not Applicable
○ NO
● YES

* Justification

DNS Queries over HTTPS (DoH) is included in the second report of the observatory function on encryption by the Europol and Eurojust Public Information. Europol is the law enforcement agency of the European Union (EU) that aims to support its Member States in preventing and combating all forms of serious international and organised crime, cybercrime and terrorism. On the other hand, Eurojust is the European Union Agency for Criminal Justice Cooperation where national judicial authorities work closely together to fight serious organised cross-border crime.

Second report of the observatory function on encryption: https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2020-01_Joint-EP-EJ-Report_Observatory-Function-on-Encryption_EN.pdf

Europol: https://www.europol.europa.eu/

Eurojust Public Register: https://www.eurojust.europa.eu/public-register

*** A40 - Is the specification included in an open repository/catalogue of standards at national level?**

EIF Recommendation 23: Consult relevant catalogues of standards, specifications, and guidelines at the national and EU level, in accordance with your NIF and relevant DIFs, when procuring and developing ICT solutions.

EIF Recommendation 6: Reuse and share solutions, and cooperate in the development of joint solutions when implementing European public services.

- ○ Not Answered
- ○ Not Applicable
- ○ NO
- ● YES

* Justification

DNS Queries over HTTPS (DoH) is recommended by the Spanish Agency of Data Protection. According to this public institution, to provide confidentiality in DNS queries, different alternatives have been developed, including DNS over TLS (DoT) and DNS over HTTPS (DoH). Both solutions are designed to mitigate the risk that DNS queries can be intercepted, and if they are that the information is illegible, contributing to improve confidentiality.

AEPD Technical Note on DNS Privacy: https://www.aepd.es/guides/technical-note-dns-privacy.pdf

*** A41 - Is the specification included in an open repository/catalogue of standards at European level?**

EIF Recommendation 23: Consult relevant catalogues of standards, specifications, and guidelines at the national and EU level, in accordance with your NIF and relevant DIFs, when procuring and developing ICT solutions.

EIF Recommendation 6: Reuse and share solutions, and cooperate in the development of joint solutions when implementing European public services.

- ○ Not Answered
- ○ Not Applicable
- ○ NO
- ● YES

* Justification

DNS Queries over HTTPS (DoH) is included in the 2023 Rolling Plan for ICT standardisation, specifically the ePrivacy part of the plan. The ePrivacy Directive and the General Data Protection Regulation provide the legal framework to ensure digital privacy for EU citizens. DoH is presented as standardised encodings for DNS queries and responses that are suitable for use in HTTPS. This enables the domain name system to function over certain paths where existing DNS methods experience problems.

ePrivacy (RP2023): https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/eprivacy-rp2023

Legal Interoperability

*** A42 - Is the specification a European Standard?**

EIF Recommendation 27: Ensure that legislation is screened by means of ‘interoperability checks’, to identify any barriers to interoperability. When drafting legislation to establish a European public service, seek to make it consistent with relevant legislation, perform a ‘digital check’, and consider data protection requirements.

European Standards are those standards developed by certain organisations dedicated to this purpose. CEN, CENELEC, and ETSI are the principal organisations and all of them are developing their standards under the basis of meeting the requirements established within the European Standardisation Regulation. CEN-CENELEC homepage: https://www.cencenelec.eu/

○ Not Answered
○ Not Applicable
● NO
○ YES

* Justification

DNS queries over HTTPS (DoH) is developed by IETF, a standard development organisation based in the US. Moreover, the DNS queries over HTTPS (DoH) specification does not appear in any of the main European standard development bodies, therefore, the specification is not a European standard.

DoH specification: https://datatracker.ietf.org/doc/html/rfc8484

Organisational Interoperability

* **A43 - Does the specification facilitate the modelling of business processes?**

EIF Recommendation 28: Document your business processes using commonly accepted modelling techniques and agree on how these processes should be aligned to deliver a European public service.

○ Not Answered
● Not Applicable
○ NO
○ YES

* Justification

While DoH is not intended for modeling business processes, it is a low-level networking protocol that operates at the DNS layer. It focuses on securing the transmission of DNS-related information between clients and DNS resolvers. Modeling business processes typically involves higher-level concepts and frameworks that go beyond the scope of network protocols like DoH.

RFC 8484: https://datatracker.ietf.org/doc/html/rfc8484

* **A44 - To what extent does the specification facilitate organisational interoperability agreements?**

EIF Recommendation 29: Clarify and formalise your organisational relationships for establishing and operating European public services.

Relates to specifications' capacities to help and ease the creation and formalisation of Interoperability agreements. E.g. Memorandums of Understanding (MoUs), Services Level Agreements (SLAs).

○ Not Answered
○ Not Applicable
○ The specification's definition hinders the drafting of such agreements.
○ The specification makes no provisions that would facilitate the drafting of such agreements.

● The specification defines certain elements to facilitate such agreements.
○ The specification defines most elements to facilitate such agreements.
○ The specification explicitly identifies all elements to be used in drafting such agreements.

* Justification

DNS over HTTPS (DoH) is not inherently designed to facilitate organisational interoperability agreements. While DoH may not directly address organisational interoperability agreements, it can play a role in ensuring secure and private DNS communication between systems or entities that want to make an organisational interoperability agreements.

RFC 8484: https://datatracker.ietf.org/doc/html/rfc8484

Semantic Interoperability

*** A45 - Does the specification encourage the creation of communities along with the sharing of their data and results in national and/or European platforms?**

EIF Recommendation 32: Support the establishment of sector-specific and cross-sectoral communities that aim to create open information specifications and encourage relevant communities to share their results on national and European platforms.

Relates to specifications that are narrowly related to the data/information being exchanged, its format, and structure. It would allow a common method/mechanism to improve its reuse and exchange removing possible limitations. An example of it could be RDF, which is used to describe information and its metadata using specific syntax and serialisation.

○ Not Answered
○ Not Applicable
○ Yes, but at national or regional level.
● Yes, at European platforms.

* Justification

DNS queries over HTTPS (DoH) encourages collaboration as it was created by IETF, a non-profit and open organisation dedicated to standardisation. For instance, IETF has created discussions lists for their specifications that improve the development and specification of Internet technology through the general discussion of technical, procedural, operational, and other topics for which no dedicated mailing lists exist.

IETF Discussion Lists: https://www.ietf.org/how/lists/discussion

Useful links

CAMSS Joinup Page (https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss)

CAMSS Library of Assessments (https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-assessments-library)

CAMSS Assessment EIF Scenario - User Guide (https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/camss-assessment-eif-scenario/camss-assessment-eif-scenario-quick-user-guide)

Contact

CAMSS@everis.com

CAMSS Assessment EIF Scenario v6.0.0 - Results

CAMSS Assessment Result

Thank you for your contribution.

The score of the specification related to the scenario under which it is being evaluated depends on the scores achieved in each section of the survey. Please see the example below for guidance.

The following table shows the 'compliance levels' that a specification can reach depending on the assessment score.

EIF Scenario Compliance Level Conversion Table

			Compliance Level		
Section	**Ad-hoc**	**Opportunistic**	**Essential**	**Sustainable**	**Seamless**
Principles setting the context for EU Actions on Interoperability	20	40	50	80	90
EIF Core Interoperability Principles	0 to 340	341 to 681	681 to 1020	1021 to 1360	1361 to 1700
EIF Principles Related to generic user needs and expectations	0 to 240	241 to 480	481 to 720	721 to 960	961 to 1200

EIF Foundation principles for cooperation among public administrations	0 to 100	101 to 200	201 to 300	301 to 400	401 to 500
EIF Interoperability Layers	0 to 200	201 to 400	401 to 600	601 to 800	801 to 1000

The table below expresses the range of the score per section. When used in combination with the table above, the total score can be interpreted. See the example below for guidance.

Section Compliance Conversion Table

Compliance Level	Description
Ad-hoc	Poor level of conformance with the EIF - The specification does not cover the requirements and recommendations set out by the EIF in this area.
Opportunistic	Fair level of conformance with the EIF - The specification barely covers the requirements and recommendations set out by the European Interoperability Framework in this area.
Essential	Essential level of conformance with the EIF - The specification covers the basic aspects set out in the requirement and recommendations from the European Interoperability Framework.
Sustainable	Good level of conformance with the EIF scenario - The specification covers all the requirements and recommendations set out by the European Interoperability Framework in this area.
Seamless	Leading practice of conformance level with the EIF - The specification fully covers the requirements and recommendations set out by the European Interoperability Framework in this area.

Example – How to find the final Compliance Level

Using the score reached after the initial assessment, the interpretation can be made as follows.

1. In the summary table, observe the score for each section, e.g. EIF Core Interoperability Principles has 1800 points.

2. In the middle table – the Section Compliance Conversion Table – see that this number correlates to a column. In our example, the 1800 points of Core Interoperability Principles fall in the EIF Core Interoperability Principles row, and ‘1441 to 1800’ point range, placing it in the column 'Compliance **Seamless**'.

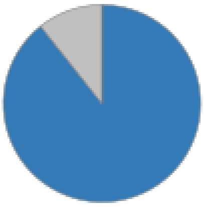
3. Next, in the top table – the EIF Scenario Compliance Level Conversion Table – we see Compliance Level "**Seamless**", and from its description that the specification for the EIF Core Interoperability Principles ‘fully covers the requirements and recommendations set out by the European Interoperability Framework in this area.’.

For additional calculation of the assessment strength, please follow the instruction provided in the User Guide, found here.

Summary

Your Score 4020

Maximum Score 4500



Section	Score for this Section	
EIF PRINCIPLES SETTING THE CONTEXT FOR EU ACTIONS ON INTEROPERABILITY	20/100	
EIF CORE INTEROPERABILITY PRINCIPLES	1640 /1700	
EIF PRINCIPLES RELATED TO GENERIC USER NEEDS AND EXPECTATIONS	1000 /1200	
EIF FOUNDATION PRINCIPLES FOR COOPERATION AMONG PUBLIC ADMINISTRATIONS	500 /500	
EIF INTEROPERABILITY LAYERS	860 /1000	

Scores by Question

EIF PRINCIPLES SETTING THE CONTEXT FOR EU ACTIONS ON INTEROPERABILITY

Score for this Section: 20/100

A1 - To what extent has the specification been included in a national catalogue from a Member State whose National Interoperability Framework has a high performance on interoperability according to National Interoperability Framework Observatory factsheets?

Your answer ✗ The specification has not been included within the catalogue of any Member State.

20 out of 100 points

EIF CORE INTEROPERABILITY PRINCIPLES

Score for this Section: 1640/1700

A2 - Does the specification facilitate the publication of data on the web?

Your answer ✓ Not Applicable

100 out of 100 points

A3 - To what extent do stakeholders have the opportunity to contribute to the development of the specification?

Your answer ✓ The working group is open to all without specific fees, registration, or other conditions.

100 out of 100 points

A4 - To what extent is a public review part of the release lifecycle?

Your answer ✓ All major and minor releases foresee a public review during which collected feedback is publicly visible.

100 out of 100 points

A5 - To what extent do restrictions and royalties apply to the specification's use?

Your answer ✓ Use of the specification is royalty-free and its Intellectual Property Right (IPR) policy or licence is aligned with Fair, Reasonable and Non-Discriminatory (F/RAND) principles.

100 out of 100 points

A6 - To what extent is the specification sufficiently mature for its use in the development of digital solutions/services?

Your answer	✓ The specification, in addition to having major releases available, has published documentation on its supporting processes (e.g. change management and release management).	100 out of 100 points

A7 - To what extent has the specification sufficient market acceptance for its use in the development of digital solutions/services?

Your answer	✓ The specification does not have market acceptance because it is directly used to create innovative solutions.	100 out of 100 points

A8 - To what extent has the specification support from at least one community?

Your answer	✓ There is a community tasked to provide public support linked to the specification and manage its maintenance.	100 out of 100 points

A9 - To what extent does the specification enable the visibility of administrative procedures, rules data, and services?

Your answer	✓ Not Applicable	100 out of 100 points

A10 - To what extent does the specification scope comprehensibly administrative procedures, rules data, and services?

Your answer	✓ Not Applicable	100 out of 100 points

A11 - To what extent does the specification enable the exposure of interfaces to access the public administration's services?

Your answer	✓ The specification can contribute to the exposure of interfaces, but it is not its main purpose.	60 out of 100 points

A12 - To what extent is the specification usable beyond the business-specific domain, allowing its usage across business domains?

Your answer ✓ The specification is domain-agnostic, designed to be implemented and/or used in any domain.

100 out of 100 points

A13 - Is the specification technology agnostic?

Your answer ✓ YES

100 out of 100 points

A14 - Is the specification platform agnostic?

Your answer ✓ YES

100 out of 100 points

A15 - To what extent does the specification allow for partial implementations?

Your answer ✓ The specification explicitly foresees sets of requirements that can be implemented incrementally or separately.

100 out of 100 points

A16 - Does the specification allow customisation?

Your answer ✓ YES

100 out of 100 points

A17 - Does the specification allow extension?

Your answer ✓ YES

100 out of 100 points

A18 - To what extent does the specification enable data portability between systems/applications supporting the implementation or evolution of European public services?

Your answer ✓ The specification introduces certain aspects that can contribute to enabling data portability.

80 out of 100 points

EIF PRINCIPLES RELATED TO GENERIC USER NEEDS AND EXPECTATIONS

Score for this Section: 1000/1200

A19 - To what extent does the specification allow relevant information to be reused when needed?

Your answer ✓ Provided information is reused, but not in all scenarios.

80 out of 100 points

A20 - To what extent does the specification enable the e-accessibility?

Your answer ✓ Not Applicable

100 out of 100 points

A21 - To what extent does the specification ensure the protection of personal data managed by Public Administrations?

Your answer ✓ The specification explicitly addresses data protection but without referring to relevant regulations.

80 out of 100 points

A22 - Does the specification provide means for restriction of access to information/data?

Your answer ✓ The specification explicitly addresses and enables the implementation of features to guarantee confidentiality.

100 out of 100 points

A23 - Is the specification included in any initiative at European or National level covering privacy aspects?

Your answer ✓ Yes, at European level.

100 out of 100 points

A24 - To what extent does the specification enable the secure exchange of data?

Your answer ✓ The specification explicitly addresses and enables the secure and trustworthy exchange of data.

100 out of 100 points

A25 - To what extent does the specification enable the secure processing of data?

Your answer ✓ The specification addresses data security and trustworthy data processing but does not foresee specific provisions to enable them. 60 out of 100 points

A26 - To what extent the specification guarantees the authenticity and authentication of the roles agents involved in the data transactions?

Your answer ✓ The specification introduces certain aspects that can contribute to enabling authenticity features. 80 out of 100 points

A27 - To what extent information is protected against unauthorised changes?

Your answer ✓ The specification explicitly addresses and enables the implementation of features to guarantee data integrity. 100 out of 100 points

A28 - To what extent does the specification ensure and enable data processing accuracy?

Your answer ✓ The specification addresses data accuracy but without specific provisions to enable it. 60 out of 100 points

A29 - To what extent does the specification provide an access control mechanism?

Your answer ✓ The specification introduces certain aspects that can contribute to enabling access control mechanisms. 80 out of 100 points

A30 - To what extent could the specification be used in a multilingual context?

Your answer ✓ The specification foresees limited support for multilingualism. 60 out of 100 points

EIF FOUNDATION PRINCIPLES FOR COOPERATION AMONG PUBLIC ADMINISTRATIONS

Score for this Section: 500/500

A31 - Does the specification simplify the delivery of European public services?

Your answer ✓ YES

100 out of 100 points

A32 - Does the specification enable digital service delivery channels?

Your answer ✓ Not Applicable

100 out of 100 points

A33 - To what extent does the specification enable the long-term preservation of data/information /knowledge (electronic records included)?

Your answer ✓ Not Applicable

100 out of 100 points

A34 - To what extent are there assessments of the specification's effectiveness?

Your answer ✓ There are such assessments directly addressing the specification.

100 out of 100 points

A35 - To what extent are there assessments of the specification's efficiency?

Your answer ✓ There are such assessments directly addressing the specification.

100 out of 100 points

EIF INTEROPERABILITY LAYERS

Score for this Section: 860/1000

A36 - Is the (or could it be) specification mapped to the European Interoperability Architecture (EIRA)?

Your answer ✓ YES

100 out of 100 points

A37 - To what extent can the conformance of the specification's implementations be assessed?

Your answer ✓ The specification defines conformance as requirements with resources to enable automated measurement.

80 out of 100 points

A38 - Is the specification recommended by a European Member State?

Your answer ✓ YES

100 out of 100 points

A39 - Is the specification selected for its use in a European Cross-border project/initiative?

Your answer ✓ YES

100 out of 100 points

A40 - Is the specification included in an open repository/catalogue of standards at national level?

Your answer ✓ YES

100 out of 100 points

A41 - Is the specification included in an open repository/catalogue of standards at European level?

Your answer ✓ YES

100 out of 100 points

A42 - Is the specification a European Standard?

Your answer ✗ NO

20 out of 100 points

A43 - Does the specification facilitate the modelling of business processes?

Your answer ✓ Not Applicable

100 out of 100 points

A44 - To what extent does the specification facilitate organisational interoperability agreements?

Your answer ✓ The specification defines certain elements to facilitate such agreements.

60 out of 100 points

A45 - Does the specification encourage the creation of communities along with the sharing of their data and results in national and/or European platforms?

Your answer	✓ Yes, at European platforms.	100 out of 100 points

Contact	CAMSS@everis.com
Useful links	CAMSS Joinup Page CAMSS Library of Assessments CAMSS Assessment EIF Scenario - User Guide
Contribution ID	52caefa1-053d-4983-ad21-6cca8bf3b5ec
Completed at	05/04/2024 11:55:28
Completion time	-