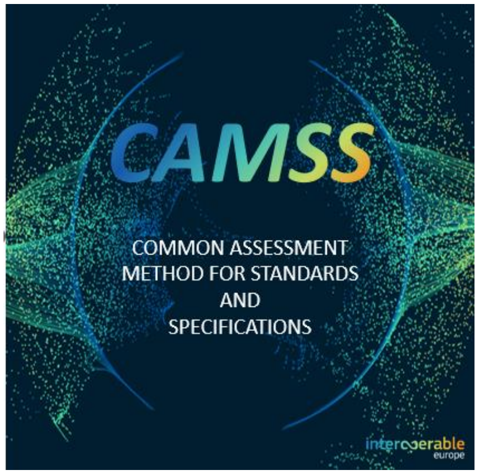

ASSESSMENT SUMMARY v1.0.0

DNS Queries over HTTPS (DoH)[1]

Internet Engineering Task Force (IETF)[2]

[1] DoH: https://datatracker.ietf.org/doc/html/rfc8484

[2] IETF: https://www.ietf.org/

Change Control

Modification	Details
Version 1.0.0	
Initial version	

TABLE OF CONTENT

1. Introduction

The present document is a summary of the assessment of **DNS Queries over HTTPS (DoH)** carried out by CAMSS using the CAMSS EIF assessment scenario. The purpose of this scenario is assessing the compliance of a standard orspecification with the European Interoperability Framework (EIF)[3].

2. Assessment Summary

DNS Queries over HTTPS (DoH) is a 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.

This specification is developed by the IETF, which was founded in 1986, and aims to be the premiere standards development organization (SDO) for the Internet. The IETF makes voluntary standards that are often adopted by Internet users, network operators, and equipment vendors, and it thus helps shape the trajectory of the development of the Internet. Thanks to this specification, logs can then be accessed by analysis and reporting software to perform audits, monitoring, troubleshooting, and other essential IT operational tasks, which can enhance interoperability and eGovernment.

2.1 Interoperability Principles

Interoperability principles are fundamental behavioural aspects that drive interoperability actions. They are relevant to the process of establishing interoperable European public services. They describe the context in which European public services are designed and implemented. The specification specifically addresses interoperability in cloud computing, which can be extremely useful in eGovernment by enhancing data portability, increased efficiency, and integrity.

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

- **Subsidiarity and proportionality**

  DNS Queries over HTTPS (DoH) is not included within the ICT catalogue of any Member State.

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

- **Openness**
- DNS over HTTPS (DoH) is maintained by the Internet Engineering Steering Group (IESG)[4], who irresponsible for technical management of IETF activities and the Internet standards process. This specification is currently on its 15th version, published in 2018 and has a public document history[5] where any action related to the specification's content is reported.

[3] European Interoperability Framework (EIF): https://ec.europa.eu/isa2/eif_en
[4] IESG IETF: https://www.ietf.org/about/groups/iesg/
[5] RFC 8484 History: https://datatracker.ietf.org/doc/rfc8484/history/

IESG welcomes the critical evaluation of protocols and has provided guidance for it. For instance, there is a section in the RFC Editor[6] where any user can report doubts or comments regarding RFC 8484. In addition, this specification is the foundation for many different innovative solutions. BIND 9[7] by the Internet Systems Consortium (ISC) comes with initial support for DNS-over-HTTPS (DoH) as DoH is 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.

- **Transparency**

  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.

- **Reusability**

  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.

- **Technological neutrality and data portability**

  DNS over HTTPS (DoH) is designed to be technology and platform agnostic, meaning that it operates at the application layer of the networking stack and can be implemented across different platforms and technologies.

  As 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. In addition, DNS over HTTPS (DoH) allows for customisation and extensions but the extent of it may vary depending on the DNS resolver or client software being used. For instance, users can specify the URLs of the DoH servers they want to use and use option codes to enable the inclusion of additional parameters or features in DNS queries and responses.

  DNS over HTTPS (DoH) can contribute to data portability between systems and applications as it secures DNS 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.

[6] RFC 8484 Editor Errata: https://www.rfc-editor.org/errata/rfc8484
[7] ISC DoH in BIND 9: https://www.isc.org/blogs/bind-implements-doh-2021/

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

- **User-centricity**

  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.

- **Inclusion and accessibility**

  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.

- **Privacy**

  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. Even so, it does not extend its protection to other layers of the communication stack or to the handling of personal data within applications or services. Security and privacy considerations are based on RFC 8446[8], IETF's Transport Layer Security (TLS) Protocol. The standard defines confidentiality and how AEAD encryption provides confidentiality and integrity for the data. In addition, DoH is included in the EU-funded SAPPAN project[9], which seeks to introduce a privacy-preserving sharing and automation platform to facilitate efficient response to and recovery from cyberattacks.

- **Security**

  DNS over HTTPS (DoH) enhances the security of data exchange and processing at the DNS layer by encrypting DNS queries and responses. It DoH significantly improves online security and privacy by securing DNS queries and minimizing exposure of sensitive information during resolution processes. For that reason, DoH encrypts DNS traffic and requires authentication of the server, thus preventing certain types of cyber-attacks and ensuring that the communication has not been tampered with.

  DoH provides protection against unauthorised 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. While it ensures the confidentiality and integrity of DNS transactions, it does not directly address data processing accuracy beyond the DNS layer nor defines access control mechanisms in the traditional sense, as it relies on the existing security mechanisms of the HTTPS protocol, including server authentication through digital certificates.

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

[9] SAPPAN Project: https://sappan-project.eu

- **Multilingualism**
  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.

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

- **Administrative Simplification**
  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.

- **Preservation of information**
  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.

- **Assessment of effectiveness and efficiency**
  The effectiveness and efficiency of DNS over HTTPS (DoH) is often evaluated through various means, including practical implementation and scalability. For instance, A 2019-paper[10] 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. Another 2020-paper[11] related to the 3rd International Conference on Information and Computer Technologies (ICICT) describes the impact of DoH on cyber systems as one of the latest enhancements implemented to address security against malware and other vulnerabilities, which proves the specification's efficiency.

2.2 Interoperability Layers

The interoperability model which is applicable to all digital public services includes:

- Four layers of interoperability: legal, organisational, semantic, and technical.
- A cross-cutting component of the four layers “integrated public service governance”.
- A background layer, “interoperability governance”.

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

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

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

- **Interoperability Governance**

  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. As for conformance requirements of DNS queries over HTTPS (DoH), they are expressed with a combination of descriptive assertions to be interpreted as described in BP14[12].

  DNS Queries over HTTPS (DoH) is included in the second report of the observatory function on encryption[13] by the Europol[14] and Eurojust Public Information[15]. In addition, the specification is recommended by the Spanish Agency of Data Protection to provide confidentiality in DNS queries[16]. In fact, DoH is included in the 2023 Rolling Plan for ICT standardisation, specifically the ePrivacy[17] part of the plan.

- **Legal interoperability**

  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.

- **Organisational interoperability**

  While DoH is not intended for modelling business processes nor facilitating 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.

- **Semantic Interoperability**

  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[18] 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.

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

[13] 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

[14] Europol: https://www.europol.europa.eu

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

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

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

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

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for the **DNS queries over HTTPS (DoH).** The CAMSS "Strength" indicator measures the reliability of the assessment by calculating the number of answered (applicable) criteria. On the other hand, the number of favourable answers and the number of unfavourable ones is used to calculate the "Automated Score" per category and an "Overall Score".

Category	Automated Score	Assessment Strength	Compliance Level
Principles setting the context for EU actions on interoperability	20/100 (20%)	100%	Ad-hoc
Core interoperability principles	1640/1700 (96%)	82%	Seamless
Principles related to generic user needs and expectations	1000/1200 (83%)	92%	Seamless
Foundation principles for cooperation among public administrations	500/500 (100%)	60%	Seamless
Interoperability layers*	860/1000 (86%)	90%	Seamless
Overall Score	3320/3800 (87%)[19]	84%	

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

With an 84% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 87% (3320/3800) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.

[19] See the "results interpretation" section of the CAMSS Assessment EIF Scenario Quick User Guide: https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/camss-assessment-eif-scenario/results-visualisation-and-interpretation