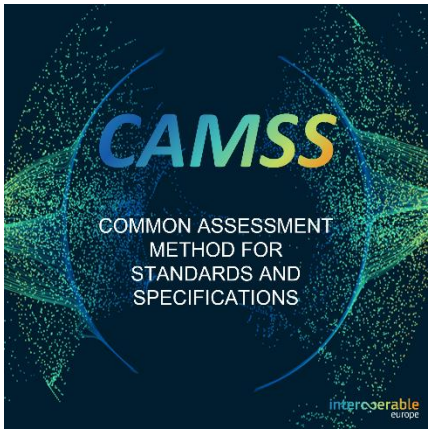

ASSESSMENT SUMMARY v1.0.0

HTTP over SSL/TLS (HTTPS)[1]

IETF[2]

[1] HTPPS specification: https://datatracker.ietf.org/doc/html/rfc2818

[2] IETF website: 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 **HTTPS** carried out by CAMSS using the CAMSS Assessment EIF scenario[3]. The purpose of this scenario is to assess the compliance of a standard or specification with the European Interoperability Framework (EIF)[4].

2. ASSESSMENT SUMMARY

HTTP over SSL/TLS also known as HTTPS is a secure version of the HTTP[5] protocol, which is the standard protocol for communication on the internet. HTTPS uses encryption to ensure that the data transmitted between a user's web browser and a website remains private and cannot be intercepted or tampered with by malicious attackers.

By using HTTPS, sensitive information such as passwords, credit card details, and personal data can be securely transmitted over the internet. It provides protection against various security threats, including eavesdropping, data tampering, and identity theft.

HTTPS has been developed by the Internet Engineering Task Force (IETF), global open community of network designers, engineers, researchers, and other experts who work together to develop and maintain the standards and protocols that shape the internet's operation and evolution.

2.1. EIF Interoperability Principles

Interoperability principles are fundamental behavioural aspects that drive interoperability actions. They are relevant to the process of establishing interoperable European public services. They describe the context in which European public services are designed and implemented.

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

- **Subsidiarity and proportionality**
  HTTPS is included in 7 national catalogues of recommended specifications. They belong to Croatia, Cyprus, France, Germany, Greece, Portugal, and Sweden. The National Interoperability Framework (NIF) of France and Germany is fully alignes with at least 2 out of 3 sections of the European Interoperability Framework (EIF) according to the National Interoperability Framework Observatory (NIFO) factsheets[6].

[3] CAMSS Assessment EIF Scenario 6.0.0: https://ec.europa.eu/eusurvey/runner/CAMSSAssessmentEIFScenario6

[4] ISA[2] programme: https://ec.europa.eu/isa2/eif_en

[5] HTTP specification: https://www.ietf.org/rfc/rfc2616.txt

[6] NIFO factsheets: https://joinup.ec.europa.eu/collection/nifo-national-interoperabilityframeworkobservatory/digital-public-administration-factsheets-2022

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

- **Openness**

  HTTPS can be an enabler for the secure publication of data on the web given that it ensures that data and any resource published on the web can be safely transmitted to the users. Like all IETF standards, HTTPS is a free and open technical specification, licensed on a Royalty-free basis. Stakeholdes contrbutions are at the core of Its standard development process, and evolves through an iterative process where draft versions of the specification are made available for public review and feedback comments.

  Its maturity and popularity is evident, since HTTPS has become the standard protocol for transmitting sensitive data over the internet, and it is widely supported by web browsers, web servers, and other software applications. The majority of websites that handle user data, especially those involving e-commerce, online banking, and user accounts, use HTTPS to ensure the security and privacy of their users.

- **Transparency**

  HTTPS security features can indirectly contribute to building trust, thus enhancing the visibility and accessibility of services on the web. Nonetheless, it does not comprehensively address the overall management, visibility, or control of administrative procedures, rules, data, and services. Moreover, The use of HTTPS not only ensures that the communication between the user and the service is protected, but also provides the exposure interface of the message that will be sent to the requester.

- **Reusability**

  HTTPS is domain-agnostic, meaning it can be used with any domain or website. It is not specific to any particular domain or type of website. HTTPS can be implemented on various types of domains, including government websites, e-commerce platforms, social media platforms, news websites, and more.

- **Technological neutrality and data portability**

  While HTTPS is platform-agnostic, it still has dependency on the HTTP protocol, given that it is a specific implementation of the HTTP protocol that adds security features through the use of SSL/TLS encryption. Neither does HTTPS allow for partial implementations, as it is a holistic security protocol that has to be applied to the website or application as a whole. Moreover, it can be customised and extended through the addition of new features to enhance its capabilities and address specific requirements.

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

- **User-centricity**

  Although HTTPS is not directly related to the reuse of information, in some cases, cache content over HTTPS can provide a mean to reuse information, but not in a consitent manner.

- **Inclusion and accessibility**
  HTTPS itself does not directly address the specific accessibility needs of users with disabilities, it is anessential component for providing secure and accessible online services. Nonetheless, it can contribute to the enabling of e-accessibility. By establishing a secure foundation upon which they can build and ensure inclusive e-accessibility for all users, regardless of their abilities.

- **Privacy**
  HTTPS plays a crucial role in ensuring the protection of personal data transmitted over the internet. It provides several key mechanisms that enhance the security and privacy of user that range from encryption to authentication mechanisms in order to prevent data interception and enhance user privacy, in the same way, it is also a goof enabler for information confidentiality through the use of SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols, which encrypt the data exchanged between the client and server. Moreover, HTTPS is currently being used y many projects among which we can find TESTA[7] network service, a cross border project that provides a European backbone network for data exchange between a wide variety of public administrations.

- **Security**
  The primary purpose of HTTPS is to establish a secure and encrypted connection between a client (such as a web browser) and a server. This secure connection ensures that data exchanged between the client and server remains protected and cannot be intercepted or tampered with by unauthorized parties, and also shields the confidentiality and authenticity of data during transit.

- **Multilingualism**
  The purpose of HTTPS is not related to the delivery of multilingual European public services. Therefore this criterion is considered not applicable to the specification.

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

- **Administrative Simplification**
  HTTPS can enable digital service delivery channels by providing a secure and encrypted communication channel between clients and servers. It forms the foundation for secure and reliable online interactions, allowing organizations to deliver their services through digital channels such as websites, web applications, and APIs.

- **Preservation of information**
  The purpose of HTTPS is not related to the long-term preservation of electronic records and other kinds of information. Therefore, this criterion is not applicable to this specification.

[7] TESTA project: https://ec.europa.eu/isa2/solutions/testa_en

- **Assessment of effectiveness and efficiency**
  There are existing studies assessing HTTPS in terms of effectiveness and efficiency. Among some of the studies found assessing the effectiveness, it can be mentioned an empirical study of the cost of DNS-over-HTTPS[8]. Regarding efficiency, an interesting study to mention is a comparison between HTTP and HTTPS performance[9].

2.2. EIF Interoperability Layers

The interoperability model which is applicable to all digital public services includes:
- Four layers of interoperability: legal, organisational, semantic and technical;
- A cross-cutting component of the four layers, 'integrated public service governance';
- A background layer, 'interoperability governance'.

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

- **Interoperability governance**
  HTTPS is associated with EIRA[10] ABBs in the EIRA Library of Specifications (ELIS)[11]. More specifically, HTTPS is already associated with the "Data Exchange Component" and "Data Exchange Services" ABBs of the EIRA Technical View. It is worth to note that there is not a validator or conformance-checking tool associated with it. However, there are several tools and practices available to assess the implementation and conformance of HTTPS in a web application or server configuration such as the SSL/TLS Certificate Validation[12]. Moreover, HTTPS is included in the national catalogue of 7 Member States, and it is currently being implemented in may European cross-border projects, such as the TESTA[13] network service.

- **Legal Interoperability**
  HTTPS is not a European Standard in the sense of a formal standard developed and recognized by the European standards organizations.

[8] An Empirical Study of the Cost of DNS-over-HTTPS: https://dl.acm.org/doi/abs/10.1145/3355369.3355575

[9] A comparison of HTTP and HTTPS performance: https://citeseerx.ist.psu.edu/documentrepid=rep1&type=pdf&doi=1cd89de5cf0e618924c73ac2b060104b7076f0b7

[10] EIRA: https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira/release/600

[11] ELIS: https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elis/elis-dashboard

[12] Validation methods for TLS/SSL certificates: https://www.digicert.com/faq/public-trust-and-certificates/what-are-the-validation-methods-for-tls-sslcertificates

[13] TESTA project: https://ec.europa.eu/isa2/solutions/testa_en

- **Organisational interoperability**
  Although the purpose of HTTPS is not related to the modelling of business processes, it may indirectly facilitate organisational interoperability agreements on the basis that its standardized communication channel can support interoperability efforts by securing data transmission, and authentication.

- **Semantic Interoperability**
  HTTPS is at the center of many debates in the Joinup platform[14], where there can be found many forums with discussions on its implementation.

[14] Joinup platform HTTPS discussions:

https://joinup.ec.europa.eu/search?keys=https+&sort_by=creation-date&f%5B0%5D=type%3Adiscussion

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for **HTTPS** 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
Principle setting the context for EU actions on interoperability	100/100 (100%)	100%	Seamless
Core interoperability principles	1420/1700 (84%)	100%	Seamless
Principles related to generic user needs and expectations	1040/1200 (87%)	75%	Seamless
Foundation principles for cooperation among public administrations	500/500 (100%)	80%	Seamless
Interoperability layers*	940/1000 (94%)	90%	Seamless
Overall Score	3500/4000 (88%)[15]	89%	

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

With an 89% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 88% (3500/4000) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.

[15] 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