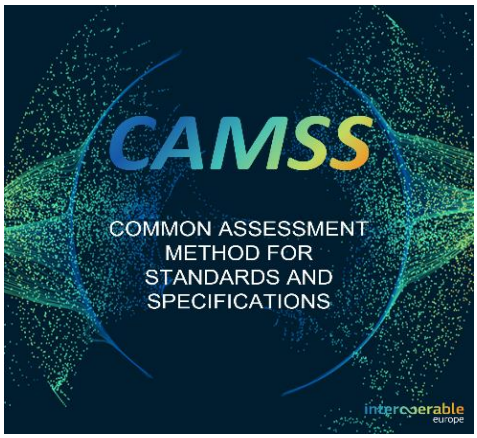

ASSESSMENT SUMMARY v1.0.0

Security Assertion Markup Language (SAML)[1]

OASIS[2]

[1] SAML 2.0 Reference: docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

[2] OASIS Website: https://www.oasis-open.org/

Change Control

Modification	Details
Version 1.0.0	
Initial version	

TABLE OF CONTENT

1. INTRODUCTION **4**

2. ASSESSMENT SUMMARY **4**

2.1. EIF Interoperability Principles 4

2.2. EIF Interoperability Layers 8

3. ASSESSMENT RESULTS **9**

1. INTRODUCTION

The present document is a summary of the assessment of **SAML 2.0** carried out by CAMSS using the CAMSS Assessment EIF scenario[3]. The purpose of this scenario is to assess the compliance of a standard or specification with the European Interoperability Framework (EIF)[4].

2. ASSESSMENT SUMMARY

The Security Assertion Markup Language (SAML) standard defines a framework for exchanging security information between online business partners. It was developed by the Security Services Technical Committee (SSTC)[5] of the standards organization OASIS.

SAML streamlines user access across various platforms by enabling Single Sign-On (SSO), allowing businesses to reduce authentication overhead, enhance security, and provide a seamless user experience regardless of their specific industry or function.

SAML plays a pivotal role in European initiatives like eIDAS[6], facilitating cross-border electronic identification among EU nations. The specification was developed and is maintained by OASIS, an international nonprofit consortium dedicated to advancing open standards for the global information society.

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

- **Subsidiarity and proportionality**
  SAML 2.0 is included in Portugal and Slovakian national catalogues of recommended specifications. The National Interoperability Framework (NIF) of Slovakia and Portugal is fully aligned with at least 2 out of 3 sections of the European Interoperability Framework (EIF) according to the National Interoperability Framework Observatory (NIFO) factsheets[7].

[3] CAMSS Assessment EIF Scenario 6.0: https://ec.europa.eu/eusurvey/runner/CAMSSAssessmentEIFScenario6

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

[5] SSTC: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[6] eIDAS Reference: https://digital-strategy.ec.europa.eu/es/policies/eidas-regulation

[7] NIFO Factsheets Reference: https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets-2022

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

- **Openness**

  The purpose of SAML 2.0 is not related to the publication of data as Linked Open Data.

  OASIS has defined a clear Technical Committee (hereby TC) process where all the stakeholders involved can participate in the development of the specification development process. All the information related to a TC activity is hosted and can be consulted. All details pertaining to TC activities are hosted and are readily accessible for reference.

  The OASIS Security Services Technical Committee, responsible for the development of SAML 2.0, operates under the RF on RAND Mode of the OASIS IPR Policy[8]. As a result, the specification is licensed on a Royalty-free and (F)RAND basis. This licensing approach, combined with the widespread adoption of SAML 2.0 in both public and private sectors, attests to its efficacy and reliability. Its integration into major European projects, bolstered by a transparent development process through OASIS, only strengthens its market credibility and drives increased adoption across diverse industries.

- **Transparency**

  By allowing the authentication for using services SAML 2.0 can contribute and promote the visibility of administrations by simplifying access to administrations' services, enable the exposure of interfaces to access the public administrations services and promote the comprehensibly of administrations by simplifying access to mentioned services. Moreover, the specification can be used internally by public officers which enhances the decision-making process, but it is not its main purpose.

- **Reusability**

  The SAML 2.0 specification is a business domain agnostic specification, designed to be implemented and/or used in any domain.

- **Technological neutrality and data portability**

  SAML 2.0 can be used independently from any other technical specifications or operating system. The specification has been developed by OASIS Security Services Technical Committee[9] independently from any specific platforms or technologies. Even though SAML 2.0 is XML based specifications, as XML is a well-known specification it does not cause technological dependency.

  Moreover, SAML 2.0 is a modular and extensive specification that accommodates a variety of use cases across diverse domains. The specification consists of various components and flows, meaning that implementers can choose to support certain parts of the standard based on their needs. On the other side, the specification allows for customization to a certain extent, and this

[8] OASIS Policies Guidelines: https://www.oasis-open.org/policies-guidelines/ipr

[9] Overview of SAML Reference: https://developers.onelogin.com/saml

flexibility is one of the reasons for its widespread adoption. However, there are boundaries to ensure interoperability and security.

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

- **User-centricity**
  The application of the once-only principle in all EU Member States public administrations aims at reducing the administrative burden. To achieve this, interoperability between public administrations is a sine qua non condition.

  The specification allows cross-domain single sign-on, which reduces the administrative burden of the system administrators and the users. By using SAML 2.0, the user will not have to deal with several credentials nor provide information twice.

- **Inclusion and accessibility**
  The purpose of SAML 2.0 is not related to e-accessibility. Therefore, this criterion is not applicable to the specification.

- **Security**
  The specification allows the exchange of authentication and authorization data between parties. It is mainly used to ensure single sign-on (SSO). It extends SSO across security domains independently from any platform which prevents non-interoperable proprietary technologies. For instance, a relevant implementation of SAML 2.0 is SAML Web Browser SSO profile[10] and this profile was specified to promote interoperability by allowing the authentication to service providers through external identity providers.

  SAML offers multiple protective measures against unauthorized changes. It utilizes XML Digital Signature to digitally sign assertions and protocol messages. Additionally, for added confidentiality and protection against tampering, SAML assertions can be encrypted using XML Encryption tailored for specific recipients. Moreover, the integrity and authenticity of SAML messages are further safeguarded through various binding profiles, such as the HTTP POST and Artifact bindings, among other robust security mechanisms in place.

- **Privacy**
  SAML 2.0 primarily focuses on the authentication and authorization aspects of user data exchange, rather than data protection *per se*. There are several features and best practices within the SAML specification can be leveraged to enhance the protection of personal data, especially when used by Public Administrations or other entities.

[10] SAML 2.0 Web Browser SSO Profile Reference: https://www.ibm.com/docs/en/was-liberty/core?topic=authentication-saml-20-web-browser-single-sign

The specification itself is primarily focused on authentication and expressing attributes and entitlements about subjects, rather than enforcing access controls on resources. Therefore, the specification neither addresses confidentiality nor prevents it.

The SAML 2.0 specification is recognized and integrated in several initiatives at both European and national levels, especially those concerning identity management, privacy, and electronic transactions such as eIDAS and more specifically, the CEF regulation[11].

- **Multilingualism**
  The purpose of SAML 2.0 is not related to the delivery of multilingual public services. Therefore, this criterion is not applicable to the specification.

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

- **Administrative Simplification**
  SAML 2.0 itself is a neutral, global standard that focuses on facilitating secure single sign-on and the exchange of authentication and authorization data. However, the features it offers can indeed simplify the delivery of public services, including those in the European context (CEF[12] and eID Building Block[13]) , when integrated appropriately. The specification provides the mechanisms that can enable digital service delivery channels, especially in scenarios requiring identity verification, single sign-on, and access control.

- **Preservation of information**
  The purpose of SAML 2.0 is not related to the long-term preservation of electronic records and other kinds of information. Therefore, this criterion is not applicable to the specification.

- **Assessment of effectiveness and efficiency**
  There are several existing documents and studies[14] assessing SAML 2.0 features and capabilities and effectiveness[15]. Broadly speaking, the studies are focused on the capability to enable Single Sign-on and its benefits.

[11] CEF regulation: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32021R1153

[12] CEF regulation: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32021R1153

[13] eID Building Block Reference: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eID

[14] ResearchGate analysis on SAML2.0 Reference: https://www.researchgate.net/publication/221609828_Formal_analysis_of_SAML_20_web_browser_single_sign-on

[15] ResearchGate on Single Sign-on Auth Reference: https://www.researchgate.net/publication/45872317_Web_single_sign-on_authentication_using_SAML

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

- **Interoperability governance**

  The specification is associated with EIRA[16] ABBs in the EIRA Library of Interoperability Specifications (ELIS)[17]. It is associated with Data Access Service, Access Management Component from Technical Infrastructure and Access Management Service, Authentication Service, Identification Component, Identity Management Service from the Technical View.

  There are existing mechanisms to carry out SAML 2.0 conformity. For instance, SAMLtool.com[18] provides a SAML Response XML validation on open source.

  Slovakia and Portugal are the only European Member States that recommend the specification in their ICT National Catalogues.

- **Legal Interoperability**

  The specification is not a European Standard.

- **Organisational interoperability**

  The SAML 2.0 specification primarily centres on authentication, authorization, and federated identity rather than directly addressing business process modelling. Nevertheless, by endorsing federated identity, which permits users to employ a single set of credentials for accessing numerous systems across various organizations, SAML can notably enhance and simplify business processes. As an example, it can be worth mentioning the eID Building Block[19].

- **Semantic Interoperability**

  The specification itself does not encourage the creation of communities at European platforms. It makes use of OASIS community to share data and results among their contributors.

[16] EIRA: https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira/release/v500

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

[18] SAML XML Validator Reference: https://www.samltool.com/validate_response.php

[19] eID Building Block Reference: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eID

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for **SAML 2.0**. 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	1540/1700 (91%)	94%	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*	840/1000 (84%)	80%	Seamless
Overall Score	3320/3800 (87%)[20]	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.

[20] 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