CAMSS Assessment EIF Scenario v6.0.0

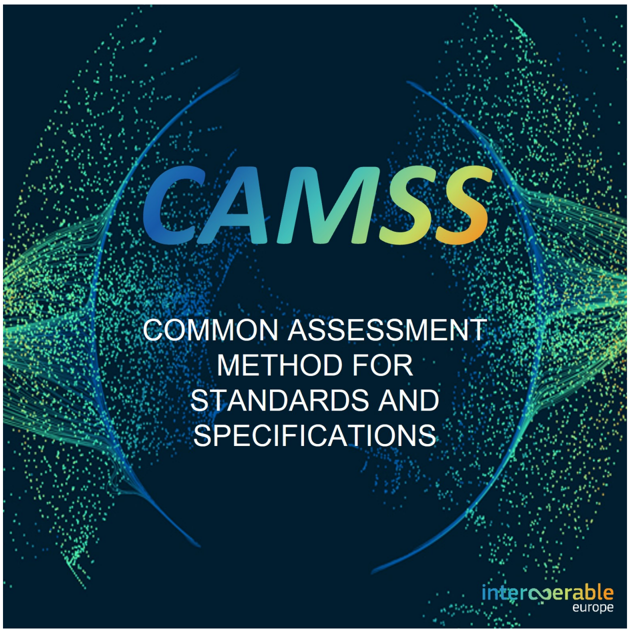
Fields marked with * are mandatory.

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

CAMSS Team

Your First Name

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

SAML 2.0 - Security Assertion Markup Language

* Version of the specification

2.0

* Description of the specification

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) of the standards organization OASIS.

* URL from where the specification is distributed

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

* 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

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

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.

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

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

Slovakia NIFO Factsheet:
https://joinup.ec.europa.eu/sites/default/files/inline-files/NIFO%20-%20Factsheet%20Slovakia_2016_v1_0.pdf

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

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

The purpose of SAML 2.0 is not related to the publication of data as Linked Open Data. Therefore, this criterion is not applicable to this specification.

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

*** 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

OASIS has defined a clear Technical Committee (hereby TC) process where all the stakeholders involved have the opportunity to participate in the development of the specification development process.
All the information related to a TC activity is hosted and can be consulted.

OASIS Policies Guidelines:
https://www.oasis-open.org/policies-guidelines/tc-process-2017-05-26

* 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

OASIS has established a comprehensive Technical Committee (TC) process that invites participation from all relevant stakeholders during the specification development journey. For every major and minor release, a public review phase is incorporated, and during this period, feedback from the community is collected and made transparently available for everyone to view and consult. All details pertaining to TC activities are hosted and are readily accessible for reference.

OASIS Policies Guidelines:
https://www.oasis-open.org/policies-guidelines/tc-process-2017-05-26

* **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

The OASIS Security Services Technical Committee, in charge of the development of SAML 2.0, operates under RF on RAND Mode of the OASIS IPR Policy. The specification is licensed on a Royalty-free and (F) RAND basis.

OASIS Commitee Referenece:
https://www.oasis-open.org/committees/security/ipr.php

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

* **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

The specification was carried out in 2001 and has been developed and maintained by OASIS. It has suffered 1 minor update (SAML 1.1) and a major one (SAML 2.0). This fact demonstrates the maturity of the specification that is being assessed. Moreover, it is also implemented by IT vendors and suppliers having a market dominance. For instance, SAML 2.0 is implemented by Microsoft for the Microsoft Azure Active Directory and by Amazon for Amazon Web Services. Therefore, it is demonstrated that SAML 2.0 has enough maturity and market acceptance for its use in the development of products and services.

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

Microsoft Azure Active using SAML 2.0 Reference:
https://learn.microsoft.com/en-us/azure/active-directory/develop/single-sign-on-saml-protocol

* **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

At the moment of performing the assessment, SAML 2.0 is widely used to secure and authenticate access to the internal and external platforms as eases the single sign-on (SSO) processes. These types of SSO's are included in the development of platforms and services, including innovative solutions.

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

* **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

OASIS is a non-profit consortium that drives the development, convergence and adoption of open standards for the global information society. SAML 2.0 is developed and maintained by OASIS. It also has the support from CEF eID Services and the Connecting Europe Facility (CEF).

OASIS Reference:
https://www.oasis-open.org/org

Connecting Europe Facility (CEF) Community:
https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/connecting-europe-facility_en

CEF eID Services
https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+eID+Profile

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

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

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

*

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

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

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

* **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

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

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

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

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

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

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

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 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.

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

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

*** 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

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 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.

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

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

*** 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

> 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.
>
> SAML 2.0 Reference:
> http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

*** 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

> The SAML 2.0 specification allows for customization to a certain extent, and this flexibility is one of the reasons for its widespread adoption. However, there are boundaries to ensure interoperability and security.
>
> SAML 2.0 Reference:
> http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

*** 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

The SAML 2.0 specification is designed with extensibility in mind. Extensibility in SAML allows for the addition of new elements and attributes within the confines of the existing XML schema to accommodate specific use cases, environments, or new functionalities without altering the core specification.

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

* **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

SAML 2.0 is a format that allows seamless cross-border interoperability between systems, regardless of its implementation.

The specification allows cross-domain single sign-on, which reduces the administrative burden of the system administrators and the users. As well, providing authentication across sectors and platforms allows administrations and stakeholders to exchange and reuse data fostering the data portability across borders.

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

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

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, avoid the user to deal with several credentials nor provide information twice.

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

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 SAML 2.0 is not related to e-accessibility. Therefore, this criterion is not applicable to the specification.

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

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

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.

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

* **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

SAML 2.0 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.

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

* **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

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.

eIDAS Reference:

https://digital-strategy.ec.europa.eu/es/policies/eidas-regulation

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

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

The specification allows the exchange of authentication and authorization data between parties. It is mainly used to ensure single sign-on (SSO) and by doing so, it secures the exchange of data. 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.

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

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

*** 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

The specification allows the secure processing of data between parties. It is mainly used to ensure single sign-on (SSO) and by doing so, it secures the processing of data. 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. This profile was specified to promote interoperability by allowing the authentication to service providers through external identity providers.

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

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

SAML 2.0 is specifically designed to address issues related to the authenticity and authentication of agents (users or systems) involved in data transactions. The specification provides a structured means for an Identity Provider (IdP) to assert claims about a subject (typically a user) to a Service Provider (SP), especially concerning the subject's authentication status and associated attributes.

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

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

The specification has multiple methods to protect the information against unauthorised changes such as:
-Digital Signatures: SAML assertions and protocol messages can be digitally signed using XML Digital Signature.
-Message Encryption: SAML assertions can be encrypted for a specific recipient using XML Encryption. While encryption primarily ensures confidentiality, it also adds an additional layer of protection against tampering.
-Binding Profiles: Various SAML binding profiles, like the HTTP POST and Artifact bindings, have specific mechanisms to ensure the integrity and authenticity of the SAML messages transported using those bindings.
And more to be described.

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

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

The purpose of SAML 2.0 is not related to ensuring and enabling data processing accuracy. Therefore, this criterion is not applicable to the specification.

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

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

SAML 2.0 primarily facilitates authentication through Single Sign-On (SSO). However, its assertions can include user attributes and roles, which Service Providers can leverage for access control decisions. Thus, while SSO simplifies the login process, SAML 2.0 also indirectly aids in implementing access control mechanisms.

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

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

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

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

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, when integrated appropriately.

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

* **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

The SAML 2.0 specification provides the mechanisms that can enable digital service delivery channels, especially in scenarios requiring identity verification, single sign-on, and access control.

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

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

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.

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

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

There are several existing documents and studies assessing SAML 2.0 features and capabilities and effectiveness. Broadly speaking, the studies are focused on the capability to enable Single Sign-on and its benefits.

Researchgate analysis on SAML2.0 Reference:
https://www.researchgate.net/publication
/221609828_Formal_analysis_of_SAML_20_web_browser_single_sign-on

Researchgate on Single Sign-on Auth Reference:
https://www.researchgate.net/publication/45872317_Web_single_sign-on_authentication_using_SAML

* **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

There are several existing documents and studies assessing SAML 2.0 features and capabilities and efficiency. Broadly speaking, the studies are focused on the capability to enable Single Sign-on and its benefits.

Researchgate analysis on SAML2.0 Reference:
https://www.researchgate.net/publication/221609828_Formal_analysis_of_SAML_20_web_browser_single_sign-on

Researchgate on Single Sign-on Auth Reference:
https://www.researchgate.net/publication/45872317_Web_single_sign-on_authentication_using_SAML

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

The specification is associated with EIRA ABB's in the EIRA Library of Interoperability Specifications (ELIS). 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 Technical Application.

ELIS link:
https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elis/release/v501

*** 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

There are existing mechanisms to carry out SAML 2.0 conformity. For instance, SAMLtool.com provides a SAML Response XML validation on open source that can be found at their Github.

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

*** 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

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

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

*** 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

SAML 2.0 is a format that allows seamless cross-border interoperability between systems, independently of existing implementations.

To demonstrate this fact is worth to take into account that in the context of Connecting Europe Facility (CEF), the CEF eID Building Block has been developed to support the (eiDAS) regulation. This building block includes technical specifications composing the “eiDAS eiD profile”. Among these specifications, the eiDAS SAML Attribute Profile defines the SAML 2.0 attributes to be used for the assertion of natural and legal person identity between eIDAS nodes.

Regulation (EU) No 2021/1153 Reference:

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

eID Building Block Reference:
https://hadea.ec.europa.eu/news/eid-discover-one-cef-building-blocks-2022-06-27_en

* **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

SAML 2.0 is not included in any catalogue of standards at supra-national level.

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

* **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

SAML 2.0 is recognized at the European level as part of various initiatives and repositories of standards, most notably within the context of eIDAS.

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

CEF eID Services:
https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+eID+Profile

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

SAML 2.0 is not a European Standard.

SAML2.0 Reference:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

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

The SAML 2.0 specification itself is focused on authentication, authorization, and federated identity, not directly on modelling business processes. However, federated identity, which SAML supports, can significantly streamline business processes:
Federated identity allows users to use a single set of credentials to access multiple systems or applications across different organizations.

SAML2.0 Reference:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

*** 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

The purpose of SAML 2.0 is not related to organisational interoperability. Therefore, this criterion is not applicable to the specification.

SAML2.0 Reference:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

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

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.

SAML2.0 Reference:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

OASIS Members Reference:
https://www.oasis-open.org/members/

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