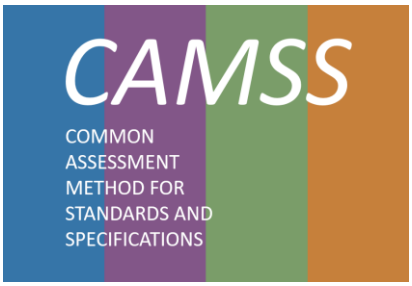

ASSESSMENT SUMMARY

Security Assertion Markup Language (SAML 2.0)

Organization for the Advancement of Structured Information Standards (OASIS)

TABLE OF CONTENTS

1. INTRODUCTION

The present document is a summary of the assessment of SAML 2.0 carried out by the CAMSS Team using the CAMSS EIF assessment scenario. The purpose of this scenario is assessing the compliance of a standard or specification with the European Interoperability Framework (EIF)[1].

2. ASSESSMENT SUMMARY

Security Assertion Markup Language (SAML)[2] is a standard to allow users to login into application using their session from other contexts, it is a single sign-on (SSO). It is developed and maintained by **OASIS[3]**. And its main advantages are: there is no need to type in credentials, no need to remember and review passwords and fosters having strong passwords.

2.1. Interoperability principles

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

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

- **Subsidiarity and proportionality**
  SAML 2.0 is included in the Slovakian national catalogue of recommended specifications. The National Interoperability Framework (NIF) of Slovakia is fully aligned with at least 4 out of 5 sections of the European Interoperability Framework (EIF) according to the National Interoperability Framework Observatory (NIFO)[4] factsheets

The specification partially 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 Open Data. Therefore, this criterion is not applicable to this specification. However, in OASIS, all the stakeholders have the opportunity to contribute to the development of SAML 2.0 and the decision making process includes a public review. Additionally, SAML 2.0 is widely implemented for the exchange of data. It has a significant market acceptance that demonstrates that it is mature enough for the development of products and services, including for the creation of innovative solutions.

[1] https://ec.europa.eu/isa2/eif_en

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

[3] https://www.oasis-open.org/

[4] https://joinup.ec.europa.eu/collection/national-interoperability-framework-observatory-nifo/nifo-factsheets

- **Transparency**
  SAML 2.0 fosters the visibility and comprehensibility of administrative rules, processes, data, services and decision-making of a public administration. In addition, it helps ensuring the availability of interfaces with internal information systems of a public administration.

- **Reusability**
  SAML 2.0 has been made available for its reuse by the by PHP, Python, Ruby, Java and .NET and is a sector agnostic specification.

- **Technological neutrality and data portability**
  SAML 2.0 is independent from any specific technology and/or platform and is designed to foster data portability between systems and applications. In addition, the technology helps to accomplish users' needs.

The Technical Specification partially supports the principles related to generic user needs and expectations:

- **User-centricity**
  SAML 2.0 eases the implementation of the once-only principle by allowing the exchange and reuse of data by public administrations across borders.

- **Inclusion and accessibility**
  SAML 2.0 does not foster e-accessibility. The purpose of the specification is not related e-accessibility.

- **Security and privacy**
  SAML 2.0 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. This profile was specified to promote interoperability by allowing the authentication to service providers through external identity providers. This fact foster security and privacy.

- **Multilingualism**
  SAML 2.0 does not foster the delivery of multilingual European public services. The purpose of the specification is not related multilingualism.

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

- **Administrative Simplification**
  SAML 2.0 allows cross-domain single sign-on, which reduces the administrative burden of the system administrators and the users. The system administrator is prevented from providing several authentication tokens and, the user does not have to deal with several credentials.

- **Preservation of information**
  SAML 2.0 does not foster the long-term preservation of electronic records and other kinds of information. The purpose of the specification is not related the preservation of information.

- **Assessment of effectiveness and efficiency**
  There are several existing documents and studies assessing SAML 2.0 features and capabilities and efficiency[5].

2.2. Interoperability layers

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

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

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

- **Interoperability governance**
  SAML 2.0 is not included in any catalogue of standards at supra-national level. Additionally, the specification is already associated to the European Interoperability Reference Architecture (EIRA) ABBs in the European Library of Specifications (ELIS). More specifically, SAML 2.0 can define the interoperability aspects of the "Identity management Component", "Identity Management Service", "Access Management Component", and "Access Management Service" ABBs of the EIRA Technical View.

- **Integrated public service governance & Legal interoperability**
  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. In addition, 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.

- **Organisational interoperability**

[5] https://www.researchgate.net/publication/221609828_Formal_analysis_of_SAML_20_web_browser_single_sign-on

https://www.researchgate.net/publication/45872317_Web_single_sign-on_authentication_using_SAML

SAML 2.0 is not a business process modelling standard or specification and does not define organisational interoperability aspects. The purpose of the specification is not related to organisational Interoperability.

- **Semantic interoperability**
  SAML 2.0 is not defining a cross-sector reusable data model. The specification defines a schema for the assertions that are involved in SAML performance but it cannot be considered as a data model. In addition, the technology is available for free on OASIS. Finally, 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.

- **Technical interoperability**
  SAML 2.0 is an open specification that is widely used for secure and authenticated access to platform and services.

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 are used to calculate the "Automated Score" per category and an "Overall Score".

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

Category	Automated Score	CAMSS Strength	Favourable	Unfavourable	Not Applicable
Principle setting the context for EU actions on interoperability	100%	100%	1	0	0
Core Interoperability principles	100%	94%	15	0	1
Principles related to generic user needs and expectations	100%	50%	2	0	2
Foundation principles for cooperation among public administrations	100%	67%	2	0	1
Interoperability layers	89%	82%	16*	2	4
Overall Score	**93%**	**81%**	**28**	**2**	**7**

With an 81% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 93% demonstrates that SAML 2.0 highly supports the European Interoperability Framework in the domains where it applies.

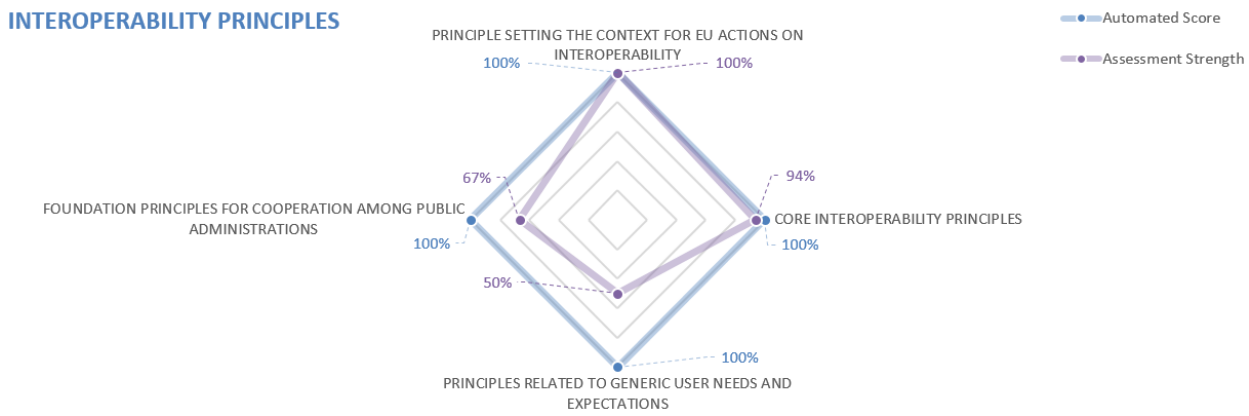

Figure 1 Assessment Results - Interoperability Principles

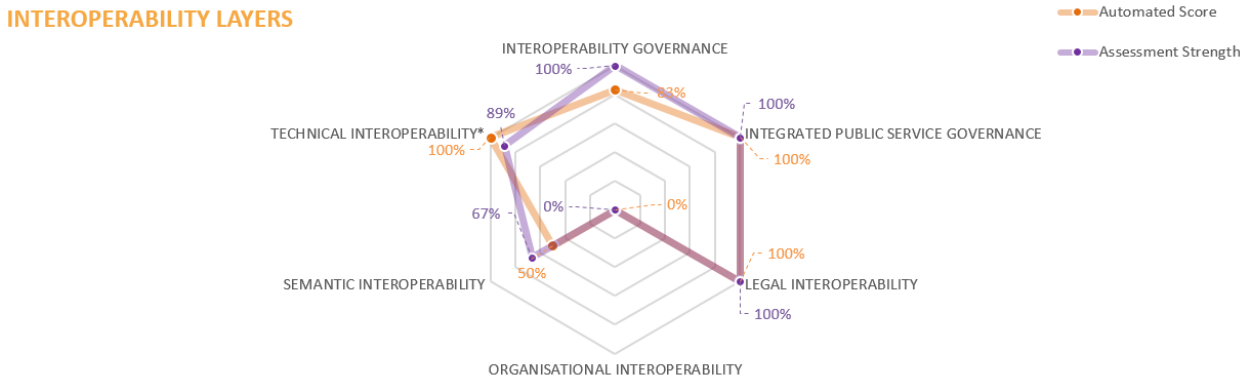

Figure 2 Assessment Results - Interoperability Layers