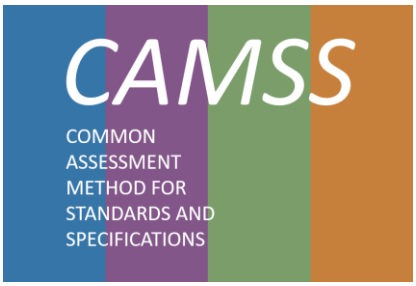

ASSESSMENT SUMMARY

Security Assertion Markup Language 2.0 - SAML 2.0 (OASIS)

TABLE OF CONTENTS

TABLE OF FIGURES

1. INTRODUCTION

This assessment has been carried out by the CAMSS Team using the CAMSS MSP scenario which is in full compliance with Annex II criteria set out in the Regulation 1025/2012[1], on European standardisation.

2. ASSESSMENT SUMMARY

Security Assertion Markup Language 2.0 (SAML 2.0) is the latest version of the SAML standard. It is used for exchanging authentication and authorization data between security domains. SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about an agent (usually an end user) between a SAML authority (named an Identity Provider) and a SAML consumer (named a Service Provider).

MARKET ACCEPTANCE

The market acceptance of SAML 2.0 is evidenced by the several implementations carried out by different vendors having a dominance over their market. For instance, the specification is implemented by Microsoft for the Microsoft Azure Active Directory[1]; and by Amazon for Amazon Web Services[2].

- **Coherence**

The coherence of the specification is evidenced by the absence of known existing conflicts with EU standards. Moreover, no existing or to-be-adopted European standards covering the same area as SAML 2.0, the exchange of authentication and authorisation data, have been found.

- **OASIS is a non-profit organisation[3] which follows an open process**. The MSP has already identified several OASIS specifications in the past, and has positively evaluated the compliance of its process for the development of specifications with Annex II criteria:

    - **Openness** of the specification is evidenced by the fact that OASIS offers membership[4] to all stakeholders affected by the developed open specifications so that they have a voice in their creation

    - **Consensus** is promoted by OASIS. It is evidenced by a clearly defined decision making[5] process based on votes requiring a majority

[1] https://docs.microsoft.com/en-us/azure/active-directory/develop/single-sign-on-saml-protocol

[2] https://aws.amazon.com/identity/saml/

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

[4] https://www.oasis-open.org/join/categories-dues

[5] https://www.oasis-open.org/policies-guidelines/tc-process-2017-05-26#voting

- **Transparency** of the specification is evidenced by the public availability of the information[6] related development and support process.

- **The specification meets adequately the requirements** set out in Annex II §4:

  - **Maintenance:** Although the Security Services Technical Committee is in charge of the development and maintenance of the specification, the maintenance and support process if not clearly defined.

  - **Availability:** SAML 2.0 is publicly available[7] for implementation and use for free on the website of OASIS.

  - **Intellectual Property Rights (IPR):** The OASIS Security Services Technical Committee in charge of the development of SAML operates under RF on RAND Mode of the OASIS IPR Policy[8].

  - **Relevance:** SAML 2.0 fosters cross-border interoperability between systems. It allows the extension of "single sign-on" across security domains. Thus, it reduces administrative burden of system administrators and users.

  - **Neutrality and stability:** SAML 2.0 has been developed by OASIS independently from any vendor product. OASIS is vendor neutral.

  - **Quality** is evidenced by the sufficient detail, consistency and completeness for its use by products and services. As the third stable version of the specification, SAML 2.0 is a very mature technical specification.

[6] http://saml.xml.org/saml-specifications

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

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

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".

Category	Automated Score	CAMSS Strength	# Favourable	# Unfavourable	# Not Applicable
Market acceptance	100%	100%	3	0	0
Coherence principle	100%	100%	3	0	0
Attributes	100%	100%	6	0	0
Requirements	88.89%	100%	8	1	**0**
Overall Score	**97.22%**	**100%**	**20**	**1**	**0**

The results of the CAMSS assessment, with a 100% CAMSS Strength, can be considered as truly representative of the specification attributes. Furthermore, a 97.22% Automated Score demonstrates that the technical specification is fully compliant with the CAMSS MSP scenario assessment criteria and therefore with standardisation regulation Annex II. It reflects the fact that SAML 2.0 fully meets the criteria regarding Market Acceptance, Coherence, and Attributes. The automated score of 88.89 for the requirements category is explained by the fact that SAML 2.0 does not meet the requirements related to the maintenance and support process.

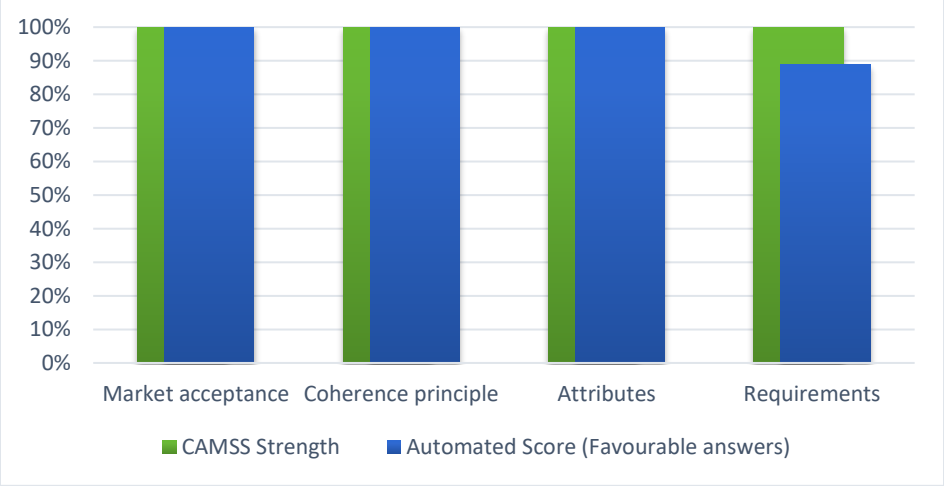

Figure 1 Assessment Results