ASSESSMENT SUMMARY

OAuth 2.0 (IETF)

TABLE OF CONTENTS

TABLE OF FIGURES

No table of figures entries found.

1. INTRODUCTION

This document reports to the European Multi-Stakeholder Platform on ICT Standardisation, hereafter 'the MSP', on the assessment of a technical specification (TS), **OAuth 2.0** from **IETF.** This assessment has been performed by the CAMSS Team following the CAMSS MSP scenario assessment criteria which is in full compliance with Annex II criteria set out in the Regulation 1025/2012[1], on European standardisation.

2. ASSESSMENT SUMMARY

The *OAuth 2.0* authorization *framework* is an open technical specification for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites without sharing their data.

During the assessment, evidence was found of the technical specification, OAuth 2.0, being satisfactorily compliant with the standardisation regulation Annex II criteria.

- **Market acceptance** of the technical specification is evidenced by the wide adoption of the TS by different suppliers and vendors.

  OAuth 2.0 is used as a way for Internet users and developers to grant websites or applications access to their information on other HTTP applications without exposing their credentials.

  This mechanism is used extensively by companies with an international market dominance such as Amazon, Google, Facebook, Microsoft and Twitter to allow the users to share information about their accounts with third party applications.

- **Coherence** of the TS is evidenced by the fact that there is no existing European standard or technical specifications being under consideration to become a European standard that has the same area of application as OAuth 2.0.

- **IETF is a non-profit organisation which follows an open process.** The MSP has already identified TS of IETF in the past, and positively evaluated the compliance of its process with Annex II criteria.

  a) Openness of the TS is evidenced by the openness of IETF to newcomers. There is no formal membership.

  b) Consensus and continuous consent of the community is required during the several iterations carried out during the development of the TS, as all IETF technical specifications.

  c) Transparency is evidenced by the availability of the documentation during the development period of the TS**.** The IETF Datatracker is the day-to-day front-end to the

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1025&from=EN

IETF database for people working on IETF standards. It contains data about the documents, working groups, meetings, agendas, presentations and more, of the IETF.

- **The TS meets adequate requirements** set out in Annex II §4

a) Maintenance

OAuth is an IETF standard, and as such it follows the defined and publicly available set of processes for the modification and revocation of standards defined in sections 6.3 and 6.4 of its Internet Standards Process[2].

b) Availability

As all the IETF standards, OAuth 2.0 is a free and open TS, and it is available for use at the corresponding IETF repository[3].

c) Intellectual Property Rights (IPR)

OAuth 2.0 is licensed by the IETF Trust. It is subject to BCP 78[4] and the Trust Legal Provisions in force on the date of TS publication[5]. IPR claims relating to the TS are available from the IETF Datatracker IPR Search tool[6]. It is therefore licensed on a royalty-free basis.

d) Relevance

OAuth 2.0 contributes to interoperability between public administrations by enabling the delegation of access to protected resources for client applications between them, which is evidenced by several existing implementations and references. Therefore it addresses public policy objectives, and example of which would be the NIS Directive[7]. Regarding societal needs, it tackles the increasing need for security in some of the most breaking-edge technologies at the moment, like it is the case of IoT[8].

e) Neutrality and stability

[2] https://www.rfc-editor.org/rfc/rfc2026.txt

[3] https://tools.ietf.org/html/rfc6749

[4] https://www.rfc-editor.org/rfc/rfc5378.txt

[5] http://trustee.ietf.org/license-info/IETF-TLP-4.pdf

[6] https://datatracker.ietf.org/ipr/search/?rfc=6749&submit=rfc

[7] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[8] https://nordicapis.com/why-oauth-2-0-is-vital-to-iot-security/

OAuth 2.0 keeps no dependencies on other specific products, platforms or technologies; and has reached maturity and stability.

f) Quality

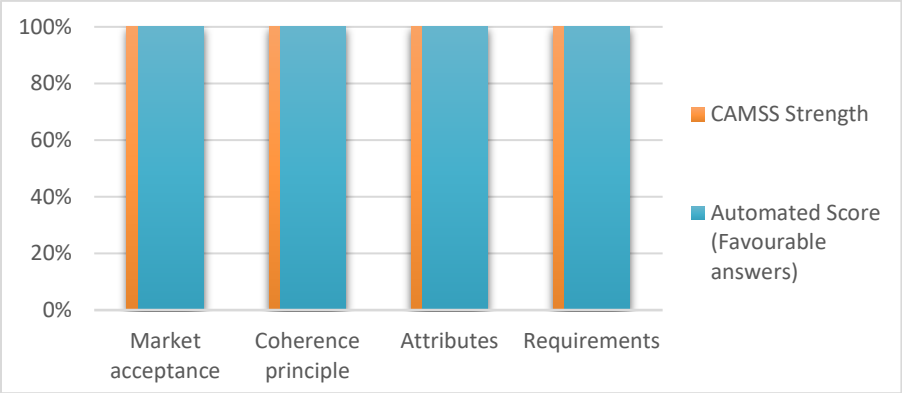
OAuth 2.0 has sufficient detail, consistency and completeness for the use and development of products and services. It is evidenced by its wide use as a security TS for phones, tablets, wearables, and internet of things devices.

3. Assessment Results

This section presents an overview of the results of the CAMSS assessments for OAuth 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	100 %	100 %	9	0	0
Overall Score:	**100%**	**100 %**	**21**	**0**	**0**

The results of the CAMSS assessment, with a 100% CAMSS Strength, can be considered as truly representative of the specification attributes. Furthermore, a 100% Automated Score demonstrates that the technical specification is fully compliant with the CAMSS MSP scenario assessment criteria and therefore with standardisation regulation Annex II. The Overall Score is 100%, so it reflects that OAuth 2.0 fully meets the criteria regarding Market Acceptance, Coherence, Attributes and Requirements.



IV. Assessment Observations

During our assessment, the observation has been made that OAuth 2.0 has been particularly criticized due to the huge difference with its first version. OAuth 2.0 is less secure than its predecessor OAuth 1.0. This is because version 2.0 creators deliberately focused on making the technical specification more flexible between sites and devices. The changes are so significant that OAuth 2.0 is not backward compatible.

Due to the aforementioned intention to make OAuth 2.0 a rich and highly extensible framework with many optional components, an OAuth 2.0 implementation might be non-interoperable with another. Additional agreements like profiles prevent different implementations and thus improve interoperability. Large players like Facebook and Google create these profiles through their market dominance. When no

single dominant party is available, other means such as standardisation by consensus are used to create profiles for particular application areas. As a conclusion, many decisions are taken in order to come up with secure and interoperable implementations of OAuth 2.0.

Also, OAuth 2.0 does not directly support encryption, signature or client verification. Instead, OAuth 2.0 expects implementers to use an outside protection protocol, which caused security vulnerabilities. However, the aforementioned issues did not prevent OAuth 2.0 from imposing itself since several years as a standard security framework for transmitting authorization decisions across a network of web applications and APIs. The version 2.0 of the technical specification is today widely adopted, notably by Facebook and Google.