

OAuth Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 28, 2017

M. Jones
Microsoft
P. Hunt
Oracle
A. Nadalin
Microsoft
January 24, 2017

Authentication Method Reference Values
draft-ietf-oauth-amr-values-05

Abstract

The "amr" (Authentication Methods References) claim is defined and registered in the IANA "JSON Web Token Claims" registry but no standard Authentication Method Reference values are currently defined. This specification establishes a registry for Authentication Method Reference values and defines an initial set of Authentication Method Reference values.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 28, 2017.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
1.1.	Requirements Notation and Conventions	3
1.2.	Terminology	3
2.	Authentication Method Reference Values	3
3.	Relationship to "acr" (Authentication Context Class Reference)	5
4.	Privacy Considerations	6
5.	Security Considerations	6
6.	IANA Considerations	6
6.1.	Authentication Method Reference Values Registry	6
6.1.1.	Registration Template	7
6.1.2.	Initial Registry Contents	8
7.	References	10
7.1.	Normative References	10
7.2.	Informative References	11
Appendix A.	Examples	12
Appendix B.	Acknowledgements	12
Appendix C.	Document History	13
	Authors' Addresses	13

[1.](#) Introduction

The "amr" (Authentication Methods References) claim is defined and registered in the IANA "JSON Web Token Claims" registry [[IANA.JWT.Claims](#)] but no standard Authentication Method Reference values are currently defined. This specification establishes a registry for Authentication Method Reference values and defines an initial set of Authentication Method Reference values.

For context, the "amr" (Authentication Methods References) claim is defined by [Section 2](#) of the OpenID Connect Core 1.0 specification [[OpenID.Core](#)] as follows:

amr

OPTIONAL. Authentication Methods References. JSON array of strings that are identifiers for authentication methods used in the authentication. For instance, values might indicate that both password and OTP authentication methods were used. The definition of particular values to be used in the "amr" Claim is beyond the scope of this specification. Parties using this claim will need to agree upon the meanings of the values used, which may be

context-specific. The "amr" value is an array of case sensitive strings.

The "amr" values defined by this specification is not intended to be an exhaustive set covering all use cases. Additional values can and will be added to the registry by other specifications. Rather, the values defined herein are an intentionally small set that are already actually being used in practice.

For context, while the claim values registered pertain to authentication, note that OAuth 2.0 [[RFC6749](#)] is designed for resource authorization and cannot be used for authentication without employing appropriate extensions, such as those defined by OpenID Connect Core 1.0 [[OpenID.Core](#)]. The existence of the "amr" claim and values for it should not be taken as encouragement to try to use OAuth 2.0 for authentication without employing extensions enabling secure authentication to be performed.

When used with OpenID Connect, if the identity provider supplies an "amr" claim in the ID Token resulting from a successful authentication, the relying party can inspect the values returned and thereby learn details about how the authentication was performed. For instance, the relying party might learn that only a password was used or it might learn that iris recognition was used in combination with a hardware-secured key. Whether "amr" values are provided and which values are understood by what parties are both beyond the scope of this specification. The OpenID Connect MODRMA Authentication Profile 1.0 [[OpenID.MODRMA](#)] is one example of an application context that uses "amr" values defined by this specification.

1.1. Requirements Notation and Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [[RFC2119](#)].

1.2. Terminology

This specification uses the terms defined by JSON Web Token (JWT) [[JWT](#)] and OpenID Connect Core 1.0 [[OpenID.Core](#)].

2. Authentication Method Reference Values

The following is a list of Authentication Method Reference values defined by this specification:

face

Facial recognition

fpt

Fingerprint biometric

geo

Use of geolocation information

hwk

Proof-of-possession (PoP) of a hardware-secured key. See [Appendix C of \[RFC4211\]](#) for a discussion on PoP.

iris

Iris scan biometric

kba

Knowledge-based authentication [[NIST.800-63-2](#)] [[ISO29115](#)]

mca

Multiple-channel authentication. The authentication involves communication over more than one distinct communication channel. For instance, a multiple-channel authentication might involve both entering information into a workstation's browser and providing information on a telephone call to a pre-registered number.

mfa

Multiple-factor authentication [[NIST.800-63-2](#)] [[ISO29115](#)]. When this is present, specific authentication methods used may also be included.

otp

One-time password. One-time password specifications that this authentication method applies to include [[RFC4226](#)] and [[RFC6238](#)].

pin

Personal Identification Number or pattern (not restricted to containing only numbers) that a user enters to unlock a key on the device. This mechanism should have a way to deter an attacker from obtaining the PIN by trying repeated guesses.

pwd

Password-based authentication

rba

Risk-based authentication [[JECM](#)]

retina

Retina scan biometric

sc

Smart card

sms

Confirmation using SMS message to the user at a registered number

swk

Proof-of-possession (PoP) of a software-secured key. See [Appendix C of \[RFC4211\]](#) for a discussion on PoP.

tel

Confirmation by telephone call to the user at a registered number

user

User presence test

vbm

Voice biometric

wia

Windows integrated authentication, as described in [\[MSDN\]](#)

3. Relationship to "acr" (Authentication Context Class Reference)

The "acr" (Authentication Context Class Reference) claim and "acr_values" request parameter are related to the "amr" (Authentication Methods References) claim, but with important differences. An Authentication Context Class specifies a set of business rules that authentications are being requested to satisfy. These rules can often be satisfied by using a number of different specific authentication methods, either singly or in combination. Interactions using "acr_values" request that the specified Authentication Context Classes be used and that the result should contain an "acr" claim saying which Authentication Context Class was satisfied. The "acr" claim in the reply states that the business rules for the class were satisfied -- not how they were satisfied.

In contrast, interactions using the "amr" claim make statements about the particular authentication methods that were used. This tends to be more brittle than using "acr", since the authentication methods that may be appropriate for a given authentication will vary over time, both because of the evolution of attacks on existing methods and the deployment of new authentication methods.

4. Privacy Considerations

The list of "amr" claim values returned in an ID Token reveals information about the way that the end-user authenticated to the identity provider. In some cases, this information may have privacy implications.

While this specification defines identifiers for particular kinds of credentials, it does not define how these credentials are stored or protected. For instance, ensuring the security and privacy of biometric credentials that are referenced by some of the defined Authentication Method Reference values is beyond the scope of this specification.

5. Security Considerations

The security considerations in OpenID Connect Core 1.0 [[OpenID.Core](#)] and OAuth 2.0 [[RFC6749](#)] and the OAuth 2.0 Threat Model [[RFC6819](#)] apply to applications using this specification.

As described in [Section 3](#), taking a dependence upon particular authentication methods may result in brittle systems, since the authentication methods that may be appropriate for a given authentication will vary over time.

6. IANA Considerations

6.1. Authentication Method Reference Values Registry

This specification establishes the IANA "Authentication Method Reference Values" registry for "amr" claim array element values. The registry records the Authentication Method Reference value and a reference to the specification that defines it. This specification registers the Authentication Method Reference values defined in [Section 2](#).

To facilitate interoperability, the Designated Experts must either:

- a. require that Authentication Method Reference values being registered use only printable ASCII characters excluding double quote ('"') and backslash ('\') (the Unicode characters with code points U+0021, U+0023 through U+005B, and U+005D through U+007E), or
- b. if new Authentication Method Reference values are defined that use other code points, require that their definitions specify the exact Unicode code point sequences used to represent them.
Furthermore, proposed registrations that use Unicode code points

that can only be represented in JSON strings as escaped characters must not be accepted.

Values are registered on an Expert Review [[RFC5226](#)] basis after a three-week review period on the `jwt-reg-review@ietf.org` mailing list, on the advice of one or more Designated Experts. To increase potential interoperability, the experts are requested to encourage registrants to provide the location of a publicly-accessible specification defining the values being registered, so that their intended usage can be more easily understood.

Registration requests sent to the mailing list for review should use an appropriate subject (e.g., "Request to register Authentication Method Reference value: otp").

Within the review period, the Designated Experts will either approve or deny the registration request, communicating this decision to the review list and IANA. Denials should include an explanation and, if applicable, suggestions as to how to make the request successful. Registration requests that are undetermined for a period longer than 21 days can be brought to the IESG's attention (using the `iesg@ietf.org` mailing list) for resolution.

Criteria that should be applied by the Designated Experts includes determining whether the proposed registration duplicates existing functionality, whether it is likely to be of general applicability or whether it is useful only for a single application, whether the value is actually being used, and whether the registration description is clear.

IANA must only accept registry updates from the Designated Experts and should direct all requests for registration to the review mailing list.

It is suggested that the same Designated Experts evaluate these registration requests as those who evaluate registration requests for the IANA "JSON Web Token Claims" registry [[IANA.JWT.Claims](#)].

6.1.1. Registration Template

Authentication Method Reference Name:

The name requested (e.g., "otp"). Because a core goal of this specification is for the resulting representations to be compact, it is RECOMMENDED that the name be short -- that is, not to exceed 8 characters without a compelling reason to do so. This name is case sensitive. Names may not match other registered names in a case-insensitive manner unless the Designated Experts state that there is a compelling reason to allow an exception.

Authentication Method Reference Description:

Brief description of the Authentication Method Reference (e.g., "One-time password").

Change Controller:

For Standards Track RFCs, state "IESG". For others, give the name of the responsible party. Other details (e.g., postal address, email address, home page URI) may also be included.

Specification Document(s):

Reference to the document or documents that specify the parameter, preferably including URIs that can be used to retrieve copies of the documents. An indication of the relevant sections may also be included but is not required.

6.1.2. Initial Registry Contents

- o Authentication Method Reference Name: "face"
- o Authentication Method Reference Description: Facial recognition
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]

- o Authentication Method Reference Name: "fpt"
- o Authentication Method Reference Description: Fingerprint biometric
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]

- o Authentication Method Reference Name: "geo"
- o Authentication Method Reference Description: Geolocation
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]

- o Authentication Method Reference Name: "hwk"
- o Authentication Method Reference Description: Proof-of-possession of a hardware-secured key
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]

- o Authentication Method Reference Name: "iris"
- o Authentication Method Reference Description: Iris scan biometric
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]

- o Authentication Method Reference Name: "kba"
- o Authentication Method Reference Description: Knowledge-based authentication
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]

- o Authentication Method Reference Name: "mca"
- o Authentication Method Reference Description: Multiple-channel authentication
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]
- o Authentication Method Reference Name: "mfa"
- o Authentication Method Reference Description: Multiple-factor authentication
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]
- o Authentication Method Reference Name: "otp"
- o Authentication Method Reference Description: One-time password
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]
- o Authentication Method Reference Name: "pin"
- o Authentication Method Reference Description: Personal Identification Number or pattern
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]
- o Authentication Method Reference Name: "pwd"
- o Authentication Method Reference Description: Password-based authentication
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]
- o Authentication Method Reference Name: "rba"
- o Authentication Method Reference Description: Risk-based authentication
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]
- o Authentication Method Reference Name: "retina"
- o Authentication Method Reference Description: Retina scan biometric
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]
- o Authentication Method Reference Name: "sc"
- o Authentication Method Reference Description: Smart card
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]
- o Authentication Method Reference Name: "sms"
- o Authentication Method Reference Description: Confirmation using SMS

- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]

- o Authentication Method Reference Name: "swk"
- o Authentication Method Reference Description: Proof-of-possession of a software-secured key
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]

- o Authentication Method Reference Name: "tel"
- o Authentication Method Reference Description: Confirmation by telephone call
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]

- o Authentication Method Reference Name: "user"
- o Authentication Method Reference Description: User presence test
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]

- o Authentication Method Reference Name: "vbm"
- o Authentication Method Reference Description: Voice biometric
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]

- o Authentication Method Reference Name: "wia"
- o Authentication Method Reference Description: Windows integrated authentication
- o Change Controller: IESG
- o Specification Document(s): [Section 2](#) of [[this specification]]

7. References

7.1. Normative References

- [IANA.JWT.Claims]
IANA, "JSON Web Token Claims",
<<http://www.iana.org/assignments/jwt>>.
- [JWT]
Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", [RFC 7519](#), May 2015,
<<http://www.rfc-editor.org/info/rfc7519>>.
- [OpenID.Core]
Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, "OpenID Connect Core 1.0", November 2014,
<http://openid.net/specs/openid-connect-core-1_0.html>.

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 5226](#), DOI 10.17487/RFC5226, May 2008, <<http://www.rfc-editor.org/info/rfc5226>>.
- [RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", [RFC 6749](#), DOI 10.17487/RFC6749, October 2012, <<http://www.rfc-editor.org/info/rfc6749>>.

7.2. Informative References

- [ISO29115] International Organization for Standardization, "ISO/IEC 29115:2013 -- Information technology - Security techniques - Entity authentication assurance framework", ISO/IEC 29115:2013, April 2013, <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45138>.
- [JECM] Williamson, G., "Enhanced Authentication In Online Banking", Journal of Economic Crime Management 4.2: 18-19, 2006, <<http://utica.edu/academic/institutes/ecii/publications/articles/51D6D996-90F2-F468-AC09C4E8071575AE.pdf>>.
- [MSDN] Microsoft, "Integrated Windows Authentication with Negotiate", September 2011, <<http://blogs.msdn.com/b/benjaminperkins/archive/2011/09/14/iis-integrated-windows-authentication-with-negotiate.aspx>>.
- [NIST.800-63-2] National Institute of Standards and Technology (NIST), "Electronic Authentication Guideline", NIST Special Publication 800-63-2, August 2013, <<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>>.
- [OpenID.MODRNA] Connotte, J. and J. Bradley, "OpenID Connect MODRNA Authentication Profile 1.0", September 2016, <<https://bitbucket.org/openid/mobile/raw/default/draft-mobile-authentication-01.txt>>.

- [RFC4211] Schaad, J., "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)", [RFC 4211](#), DOI 10.17487/RFC4211, September 2005, <<http://www.rfc-editor.org/info/rfc4211>>.
- [RFC4226] M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm", [RFC 4226](#), DOI 10.17487/RFC4226, December 2005, <<http://www.rfc-editor.org/info/rfc4226>>.
- [RFC6238] M'Raihi, D., Machani, S., Pei, M., and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm", [RFC 6238](#), DOI 10.17487/RFC6238, May 2011, <<http://www.rfc-editor.org/info/rfc6238>>.
- [RFC6819] Lodderstedt, T., Ed., McGloin, M., and P. Hunt, "OAuth 2.0 Threat Model and Security Considerations", [RFC 6819](#), DOI 10.17487/RFC6819, January 2013, <<http://www.rfc-editor.org/info/rfc6819>>.

[Appendix A](#). Examples

In some cases, the "amr" claim value returned may contain a single Authentication Method Reference value. For example, the following "amr" claim value indicates that the authentication performed used an iris scan biometric:

```
"amr": ["iris"]
```

In other cases, the "amr" claim value returned may contain multiple Authentication Method Reference values. For example, the following "amr" claim value indicates that the authentication performed used a password and knowledge-based authentication:

```
"amr": ["pwd", "kba"]
```

[Appendix B](#). Acknowledgements

Caleb Baker participated in specifying the original set of "amr" values. John Bradley, Brian Campbell, William Denniss, Linda Dunbar, Paul Kyzivat, Elaine Newton, James Manger, Catherine Meadows, Kathleen Moriarty, Nat Sakimura, and Mike Schwartz provided reviews of the specification.

[Appendix C](#). Document History

[[to be removed by the RFC editor before publication as an RFC]]

-05

- o Specified characters allowed in "amr" values, reusing the IANA Considerations language on this topic from [RFC 7638](#).

-04

- o Added examples with single and multiple values.
- o Clarified that the actual credentials referenced are not part of this specification to avoid additional privacy concerns for biometric data.
- o Clarified that the OAuth 2.0 Threat Model [[RFC6819](#)] applies to applications using this specification.

-03

- o Addressed shepherd comments.

-02

- o Addressed working group last call comments.

-01

- o Distinguished between retina and iris biometrics.
- o Expanded the introduction to provide additional context to readers.
- o Referenced the OpenID Connect MODRMA Authentication Profile 1.0 specification, which uses "amr" values defined by this specification.

-00

- o Created the initial working group draft from [draft-jones-oauth-amr-values-05](#) with no normative changes.

Authors' Addresses

Michael B. Jones
Microsoft

Email: mbj@microsoft.com

URI: <http://self-issued.info/>

Phil Hunt
Oracle

Email: phil.hunt@yahoo.com

Anthony Nadalin
Microsoft

Email: tonymad@microsoft.com