Internet Engineering Task Force (IETF)
Request for Comments: 8176
Category: Standards Track
ISSN: 2070-1721

M. Jones
Microsoft
P. Hunt
Oracle
A. Nadalin
Microsoft

June 2017

Authentication Method Reference Values

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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8176.

Table of Contents

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.

Typically, each "amr" value provides an identifier for a family of closely related authentication methods. For example, the "otp" identifier intentionally covers OTPs (One-Time Passwords) based on both time and HMAC (Hashed Message Authentication Code). Many relying parties will be content to know that an OTP has been used in addition to a password; the distinction between which kind of OTP was used is not useful to them. Thus, there’s a single identifier that can be satisfied in two or more nearly equivalent ways.

Similarly, there’s a whole range of nuances between different fingerprint-matching algorithms. They differ in false-positive and false-negative rates over different population samples and also differ based on the kind and model of fingerprint sensor used. Like the OTP case, many relying parties will be content to know that a fingerprint match was made, without delving into and differentiating based on every aspect of the implementation of fingerprint capture and match. The "fpt" identifier accomplishes this.

Ultimately, the relying party is depending upon the identity provider to do reasonable things. If it does not trust the identity provider to do so, it has no business using it. The "amr" value lets the identity provider signal to the relying party additional information about what it did, for the cases in which that information is useful to the relying party.

The "amr" values defined by this specification are 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 and are already actually being used in practice.

The values defined by this specification only make distinctions that are known to be useful to relying parties. Slicing things more finely than would be used in practice would actually hurt interoperability, rather than helping it, because it would force relying parties to recognize that several or many different values actually mean the same thing to them.

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 that enable 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 MODRNA Authentication Profile 1.0 [OpenID.MODRNA] 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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Terminology

This specification uses the terms defined by JSON Web Token (JWT) [RFC7519] 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
: Biometric authentication [RFC4949] using facial recognition.

fpt
: Biometric authentication [RFC4949] using a fingerprint.

geo
: Use of geolocation information for authentication, such as that provided by [W3C.REC-geolocation-API-20161108].

hwk
: Proof-of-Possession (PoP) of a hardware-secured key. See Appendix C of [RFC4211] for a discussion on PoP.

iris
: Biometric authentication [RFC4949] using an iris scan.

kba
: Knowledge-based authentication [NIST.800-63-2] [ISO29115].

mca
: Multiple-channel authentication [MCA]. 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 [RFC4949]. One-time password specifications that this authentication method applies to include [RFC4226] and [RFC6238].

pin
: Personal Identification Number (PIN) [RFC4949] 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 [RFC4949].

rba
: Risk-based authentication [JECM].

retina
: Biometric authentication [RFC4949] using a retina scan.

sc
: Smart card [RFC4949].

sms
: Confirmation using SMS [SMS] text 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. This authentication technique is sometimes also referred to as "call back" [RFC4949].

user
: User presence test. Evidence that the end user is present and interacting with the device. This is sometimes also referred to as "test of user presence" [W3C.WD-webauthn-20170216].

vbm
: Biometric authentication [RFC4949] using a voiceprint.

wia
: Windows integrated authentication [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], OAuth 2.0 [RFC6749], and the entire 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.

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 Designated 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.

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].

Criteria that should be applied by the Designated Experts include 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.

6.1.1. Registration Template

Authentication Method Reference Name:
: The name requested (e.g., "otp") for the authentication method or family of closely related authentication methods. 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. To facilitate interoperability, the name must 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). 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

- Authentication Method Reference Name: "face"
- Authentication Method Reference Description: Facial recognition
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "fpt"
- Authentication Method Reference Description: Fingerprint biometric
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "geo"
- Authentication Method Reference Description: Geolocation
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "hwk"
- Authentication Method Reference Description: Proof-of-possession of a hardware-secured key
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "iris"
- Authentication Method Reference Description: Iris scan biometric
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "kba"
- Authentication Method Reference Description: Knowledge-based authentication
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "mca"
- Authentication Method Reference Description: Multiple-channel authentication
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "mfa"
- Authentication Method Reference Description: Multiple-factor authentication
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "otp"
- Authentication Method Reference Description: One-time password
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "pin"
- Authentication Method Reference Description: Personal Identification Number or pattern
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "pwd"
- Authentication Method Reference Description: Password-based authentication
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "rba"
- Authentication Method Reference Description: Risk-based authentication
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "retina"
- Authentication Method Reference Description: Retina scan biometric
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "sc"
- Authentication Method Reference Description: Smart card
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "sms"
- Authentication Method Reference Description: Confirmation using SMS
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "swk"
- Authentication Method Reference Description: Proof-of-possession of a software-secured key
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "tel"
- Authentication Method Reference Description: Confirmation by telephone call
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "user"
- Authentication Method Reference Description: User presence test
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "vbm"
- Authentication Method Reference Description: Voice biometric
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

- Authentication Method Reference Name: "wia"
- Authentication Method Reference Description: Windows integrated authentication
- Change Controller: IESG
- Specification Document(s): Section 2 of [RFC8176]

7. References

7.1. Normative References

[IANA.JWT.Claims]
IANA, "JSON Web Token Claims", <http://www.iana.org/assignments/jwt>.

[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>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <http://www.rfc-editor.org/info/rfc7519>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <http://www.rfc-editor.org/info/rfc8174>.

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, <https://www.iso.org/standard/45138.html>.

[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>.

[MCA] ldapwiki.com, "Multiple-channel Authentication", August 2016, <https://www.ldapwiki.com/wiki/Multiple-channel%20Authentication>.

[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, DOI 10.6028/NIST.SP.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", March 2017, <http://openid.net/specs/openid-connect-modrna-authentication-1_0.html>.

[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>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <http://www.rfc-editor.org/info/rfc4949>.

[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>.

[SMS] 3GPP, "Technical realization of the Short Message Service (SMS)", 3GPP Technical Specification (TS) 03.40 Version 7.5.0 (2001-12), January 2002, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=141>.

[W3C.REC-geolocation-API-20161108] Popescu, A., "Geolocation API Specification 2nd Edition", World Wide Web Consortium Recommendation REC-geolocation-API-20161108, November 2016, <https://www.w3.org/TR/2016/REC-geolocation-API-20161108>.

[W3C.WD-webauthn-20170216] Bharadwaj, V., Le Van Gong, H., Balfanz, D., Czeskis, A., Birgisson, A., Hodges, J., Jones, M., Lindemann, R., and J. Jones, "Web Authentication: An API for accessing Scoped Credentials", World Wide Web Consortium Working Draft WD-webauthn-20170216, February 2017, <http://www.w3.org/TR/2017/WD-webauthn-20170216/>.

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"]
```

Acknowledgements

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

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: tonynad@microsoft.com