WebAuthn Working Group
Internet-Draft
Intended status: Informational
Expires: November 3, 2018

M. Jones
Microsoft

May 2, 2018

COSE Algorithms for Web Authentication (WebAuthn)
draft-jones-webauthn-cose-algorithms-01

Abstract

The W3C Web Authentication (WebAuthn) specification uses COSE algorithm identifiers. This specification registers algorithms in the IANA "COSE Algorithms" registry that are used by WebAuthn that are not already registered. Also, they are registered in the IANA "JSON Web Signature and Encryption Algorithms" registry, when not already registered there.

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 https://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 November 3, 2018.

Table of Contents

1. Introduction

This specification defines how to use several algorithms with COSE [RFC8152] that are used by the W3C Web Authentication (WebAuthn) [WebAuthn] specification. These algorithms are registered in the IANA "COSE Algorithms" registry [IANA.COSE.Algorithms] and also in the IANA "JSON Web Signature and Encryption Algorithms" registry [IANA.JOSE.Algorithms], when not already registered there.

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.

2. RSASSA-PKCS1-v1_5 Signature Algorithm

The RSASSA-PKCS1-v1_5 signature algorithm is defined in [RFC8017]. The RSASSA-PKCS1-v1_5 signature algorithm is parameterized with a hash function (h).

A key of size 2048 bits or larger MUST be used with these algorithms. Implementations need to check that the key type is 'RSA' when creating or verifying a signature.

The RSASSA-PKCS1-v1_5 algorithms specified in this document are in the following table.

Name	Value	Hash	Description
RS256	TBD (requested assignment -257)	SHA-256	RSASSA-PKCS1-v1_5 w/ SHA-256
RS384	TBD (requested assignment -258)	SHA-384	RSASSA-PKCS1-v1_5 w/ SHA-384
RS512	TBD (requested assignment -259)	SHA-512	RSASSA-PKCS1-v1_5 w/ SHA-512
RS1	TBD (requested assignment -65535)	SHA-1	RSASSA-PKCS1-v1_5 w/ SHA-1

Table 1: RSASSA-PKCS1-v1_5 Algorithm Values

3. IANA Considerations

3.1. COSE Algorithms Registrations

This section registers the following values in the IANA "COSE Algorithms" registry [IANA.COSE.Algorithms].

- Name: RS256
- Value: TBD (requested assignment -257)
- Description: RSASSA-PKCS1-v1_5 w/ SHA-256
- Reference: Section 2 of this document
- Recommended: No

- Name: RS384
- Value: TBD (requested assignment -258)
- Description: RSASSA-PKCS1-v1_5 w/ SHA-384
- Reference: Section 2 of this document
- Recommended: No

- Name: RS512
- Value: TBD (requested assignment -259)
- Description: RSASSA-PKCS1-v1_5 w/ SHA-512
- Reference: Section 2 of this document
- Recommended: No

- Name: RS1
- Value: TBD (requested assignment -65535)
- Description: RSASSA-PKCS1-v1_5 w/ SHA-1
- Reference: Section 2 of this document
- Recommended: Deprecated

4. Security Considerations

4.1. RSA Key Size Security Considerations

The security considerations on key sizes for RSA algorithms from Section 6.1 of [RFC8230] also apply to the RSA algorithms in this specification.

4.2. RSASSA-PKCS1-v1_5 with SHA-2 Security Considerations

The security considerations on the use of RSASSA-PKCS1-v1_5 with SHA-2 hash functions from Section 8.3 of [RFC7518] also apply to their use in this specification. For that reason, these algorithms are registered as being "Not Recommended".

4.3. RSASSA-PKCS1-v1_5 with SHA-1 Security Considerations

The security considerations on the use of the SHA-1 hash function from [RFC6194] apply in this specification. For that reason, the "RS1" algorithm is registered as "Deprecated". It MUST NOT be used by COSE implementations.

A COSE algorithm identifier for this algorithm is nonetheless being registered because deployed TPMs continue to use it, and therefore WebAuthn implementations need a COSE algorithm identifier for "RS1" when TPM attestations using this algorithm are being represented.

5. References

5.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6194] Polk, T., Chen, L., Turner, S., and P. Hoffman, "Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms", RFC 6194, DOI 10.17487/RFC6194, March 2011, <https://www.rfc-editor.org/info/rfc6194>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.

[RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <https://www.rfc-editor.org/info/rfc7518>.

[RFC8017] Moriarty, K., Ed., Kaliski, B., Jonsson, J., and A. Rusch, "PKCS #1: RSA Cryptography Specifications Version 2.2", RFC 8017, DOI 10.17487/RFC8017, November 2016, <https://www.rfc-editor.org/info/rfc8017>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

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

[RFC8230] Jones, M., "Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages", RFC 8230, DOI 10.17487/RFC8230, September 2017, <https://www.rfc-editor.org/info/rfc8230>.

5.2. Informative References

[IANA.COSE.Algorithms]
IANA, "COSE Algorithms",
<https://www.iana.org/assignments/cose/cose.xhtml#algorithms>.

[IANA.JOSE.Algorithms]
IANA, "JSON Web Signature and Encryption Algorithms",
<https://www.iana.org/assignments/jose/jose.xhtml#web-signature-encryption-algorithms>.

[WebAuthn]
Balfanz, D., Czeskis, A., Hodges, J., Jones, J., Jones, M., Kumar, A., Liao, A., Lindemann, R., and E. Lundberg, "Web Authentication: An API for accessing Public Key Credentials", Candidate Recommendation, World Wide Web Consortium (W3C) Recommendation-track, March 2018,
<https://w3c.github.io/webauthn/>.

Acknowledgements

Thanks to John Fontana, Jeff Hodges, Tony Nadalin, Jim Schaad, Goeran Selander, Wendy Seltzer, Sean Turner, and Samuel Weiler for their roles in registering these algorithm identifiers.

Document History

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

-01

- Updated the requested RS1 value from -262 to -65535 to match the temporary registration made on 2018-04-19.
- Populated the Acknowledgements section.

-00

- Initial version.

Author's Address

Michael B. Jones
Microsoft

Email: mbj@microsoft.com
URI: http://self-issued.info/