JWK Thumbprint URI
draft-ietf-oauth-jwk-thumbprint-uri-03

Abstract

This specification registers a kind of URI that represents a JSON Web Key (JWK) Thumbprint value. JWK Thumbprints are defined in RFC 7638. This enables JWK Thumbprints to be used, for instance, as key identifiers in contexts requiring URIs.

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 December 3, 2022.

Copyright Notice

Copyright (c) 2022 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 (https://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.
1. Introduction

A JSON Web Key (JWK) Thumbprint [RFC7638] is a URL-safe representation of a hash value over a JSON Web Key (JWK) [RFC7517]. This specification defines a URI prefix indicating that the portion of the URI following the prefix is a JWK Thumbprint. This enables JWK Thumbprints to be communicated in contexts requiring URIs, including in specific JSON Web Token (JWT) [RFC7519] claims.

JWK Thumbprints URIs are being used in the [SIOPv2] specification as one kind of subject identifier in a context requiring that the identifier be a URI. In this case, the subject identifier is derived from a public key represented as a JWK. Expressing the identifier as JWK Thumbprint URI enables this kind of identifier to be differentiated from other kinds of identifiers that are also URIs, such as Decentralized Identifiers (DIDs) [DID-Core].

2. 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
3. JWK Thumbprint URI

The following URI prefix is defined to indicate that the portion of the URI following the prefix is a JWK Thumbprint:

- "urn:ietf:params:oauth:jwk-thumbprint"

To make it explicit in a URI which hash algorithm is used, the prefix is followed by a hash algorithm identifier and a JWK Thumbprint value, each separated by a colon character to form a URI representing a JWK Thumbprint.

4. Hash Algorithms Identifier

Hash algorithm identifiers used in JWK Thumbprint URIs MUST be values from the "Hash Name String" column in the IANA "Named Information Hash Algorithm" registry [IANA.Hash.Algorithms]. JWK Thumbprint URIs with hash algorithm identifiers not found in this registry are not considered valid and applications will need to detect and handle this error, should it occur.

5. Mandatory to Implement Hash Algorithm

To promote interoperability among implementations, the SHA-256 hash algorithm is mandatory to implement.

6. Example JWK Thumbprint URI

Section 3.1 of [RFC7638] contains the following example JWK Thumbprint value:

NzbLsXh8uDCCd-6MNwXF4W_7noWXFZAfHkxZsRGC9Xs

A complete JWK Thumbprint URI using the above JWK Thumbprint and SHA-256 hash algorithm is:
7. Security Considerations

The security considerations of [RFC7638] also apply when using this specification.

7.1. Multiple Public Keys per Private Key

There are cryptographic algorithms for which multiple public keys correspond to the same private key. This is described in the security considerations of [RFC7748] as follows:

Designers using these curves should be aware that for each public key, there are several publicly computable public keys that are equivalent to it, i.e., they produce the same shared secrets. Thus using a public key as an identifier and knowledge of a shared secret as proof of ownership (without including the public keys in the key derivation) might lead to subtle vulnerabilities.

This consideration for public keys as identifiers equally applies to JWK Thumbprint URIs used as identifiers. A recommended way to ensure that the JWK Thumbprint URI corresponds to the actual public key used is to sign a message containing the correct public key with the private key. This signed message could also contain the JWK Thumbprint URI (although, by definition, it could also be computed directly from the public key).

8. IANA Considerations

8.1. OAuth URI Registration

This specification registers the following value in the IANA "OAuth URI" registry [IANA.OAuth.Parameters] established by [RFC6755].

8.1.1. Registry Contents

- URN: urn:ietf:params:oauth:jwk-thumbprint
- Common Name: JWK Thumbprint URI
- Change controller: IESG
- Specification Document: [[ this specification ]]
9. References

9.1. Normative References

[IANA.OAuth.Parameters]  IANA, "OAuth Parameters",
<http://www.iana.org/assignments/oauth-parameters>.

[RFC2119]  Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", BCP 14, RFC 2119,
DOI 10.17487/RFC2119, March 1997,

[RFC7638]  Jones, M. and N. Sakimura, "JSON Web Key (JWK)
Thumbprint", RFC 7638, DOI 10.17487/RFC7638, September

9.2. Informative References

[DID-Core]  Sporny, M., Guy, A., Sabadello, M., and D. Reed,
"Decentralized Identifiers (DIDs) v1.0", Aug 2021,
<https://www.w3.org/TR/2021/PR-did-core-20210803/>.

<https://www.iana.org/assignments/named-information/named-
information.xhtml#hash-alg>.

for OAuth", RFC 6755, DOI 10.17487/RFC6755, October 2012,

[RFC7517]  Jones, M., "JSON Web Key (JWK)"
, RFC 7517,
DOI 10.17487/RFC7517, May 2015,
Appendix A. Acknowledgements

Use cases for this specification were developed in the OpenID Connect Working Group of the OpenID Foundation. Specifically, it is being used as a key identifier in the [SIOPv2] specification.

The following individuals also contributed to the creation of this specification: John Bradley, Scott Bradner, Brian Campbell, Roman Danyliw, Vladimir Dzhuvinov, Lars Eggert, Warren Kumari, Adam Lemmon, Neil Madden, James Manger, Francesca Palombini, Aaron Parecki, Gonzalo Salgueiro, Rifaat Shekh-Yusef, Robert Sparks, David Waite, Robert Wilton, and Paul Wouters.
o Added security considerations about multiple public keys corresponding to the same private key.

o Added hash algorithm identifier after the JWK thumbprint URI prefix to make it explicit in a URI which hash algorithm is used.

o Added reference to a registry for hash algorithm identifiers.

o Added SHA-256 as a mandatory to implement hash algorithm to promote interoperability.

-00

o Created initial working group draft from draft-jones-oauth-jwk-thumbprint-uri-01.

Authors' Addresses

Michael B. Jones
Microsoft

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

Kristina Yasuda
Microsoft

Email: kryasuda@microsoft.com
URI: https://twitter.com/kristinayasuda