Workgroup: OAuth Working Group
Internet-Draft:
draft-ietf-oauth-jwk-thumbprint-uri-02
Published: 16 May 2022
Intended Status: Standards Track
Expires: 17 November 2022

Authors: M.B. Jones   K. Yasuda
         Microsoft   Microsoft

JWK Thumbprint URI

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 will expire on 17 November 2022.

Copyright Notice

Table of Contents

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 capitals, as shown here.

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 considered invalid 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:

```
urn:ietf:params:oauth:jwk-thumbprint:sha-256:NzbLsXh8uDCcd-6MNwXF4W_7n
```

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, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7638] Jones, M. and N. Sakimura, "JSON Web Key (JWK) Thumbprint", RFC 7638, DOI 10.17487/RFC7638, September 2015, <https://www.rfc-editor.org/info/rfc7638>.

[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>.

9.2. Informative References

[DID-Core] Sporny, M., Guy, A., Sabadello, M., and D. Reed, "Decentralized Identifiers (DIDs) v1.0", 3 August 2021, <https://www.w3.org/TR/2021/PR-did-core-20210803/>.

[IANA.Hash.Algorithms] IANA, "Named Information Hash Algorithm Registry", <https://www.iana.org/assignments/named-information/named-information.xhtml#hash-alg>.

[RFC6755] Campbell, B. and H. Tschofenig, "An IETF URN Sub-Namespace for OAuth", RFC 6755, DOI 10.17487/RFC6755, October 2012, <https://www.rfc-editor.org/info/rfc6755>.

[RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <https://www.rfc-editor.org/info/rfc7517>.

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

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/info/rfc7748>.

[SIOPv2] Yasuda, K. and M. B. Jones, "Self-Issued OpenID Provider v2", 18 December 2021, <https://openid.net/specs/openid-connect-self-issued-v2-1_0.html>.

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 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, Adam Lemmon, Neil Madden, James Manger, Aaron Parecki, Gonzalo Salgueiro, Rifaat Shekh-Yusef, Robert Sparks, and David Waite.

Appendix B. Document History

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

-02

- Addressed IETF last call comments by clarifying the requirement to use registered hash algorithm identifiers.

-01

- Added security considerations about multiple public keys coresponding to the same private key.
- Added hash algorithm identifier after the JWK thumbprint URI prefix to make it explicit in a URI which hash algorithm is used.
- Added reference to a registry for hash algorithm identifiers.
- Added SHA-256 as a mandatory to implement hash algorithm to promote interoperability.

-00

- 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