Workgroup: OAuth Working Group
Internet-Draft:
draft-yusef-oauth-nested-jwt-05
Published: 14 June 2022
Intended Status: Standards Track
Expires: 16 December 2022
Authors: R. Shekh-Yusef
Okta

Multi-Subject JSON Web Token (JWT)

Abstract

This specification defines a mechanism for including multiple subjects in a JWT. A primary subject in an enclosing JWT with its own claims, and a related secondary subject in a nested JWT with its own claims.

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 16 December 2022.

Copyright Notice

Table of Contents

1. Introduction

JSON Web Token (JWT) [RFC7519] is a mechanism that is used to transfer claims between two parties across security domains. Nested JWT is a JWT in which the payload is another JWT. The current specification does not define a means by which the enclosing JWT could have its own Claims Set, only the enclosed JWT would have claims.

There are a number of use cases where there is a need to represent multiple related subjects in one JWT; a primary subject and a related secondary subject.

This specification defines a mechanism for including multiple subjects in a JWT. A primary subject in an enclosing JWT with its own claims, and a related secondary subject in a nested JWT with its own claims.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC8174].

2. Use Cases

The following are few use cases that might benefit from such a concept, that fall into two different categories:

2.1. One Issuer Category

In the following cases, both JWTs are issued by the same issuer.

2.1.1. Primary Subject with Secondary Authority Subject

A primary subject with a related secondary subject that has authority over the primary subject, e.g. Child/Parent, Pet/Owner.

The secondary user (e.g., parent) logs in to an application (e.g., pharmacy application), gets redirected to the authorization server, authenticates, and asks for permission to access resources (e.g., medication) for the primary subject (e.g., child). The authorization server then issues a JWT with the primary subject in the enclosing JWT and the secondary subject in the nested JWT.

2.1.2. Multiple Primary Subjects

Two or more primary related subjects e.g. a married couple. The authorization server is setup to provide one of the subjects with permissions to access the other related subject resources.

One user (e.g., wife) logs in to a application (e.g., pharmacy application), gets redirected to the authorization server, authenticates, and asks for permission to access resources (e.g., medication) for the other primary subject (e.g., husband). The authorization server then issues a JWT with the primary subject in the enclosing JWT and the other primary subject in the nested JWT.

2.1.3. Delegation of Authority

A primary subject delegates authority over a resource to a secondary subject who acts on behalf of the primary subject, as defined in [RFC8693].

2.2. Multiple Issuers Category

In the following cases, the JWTs are issued by different issuers.

2.2.1. STIR

[RFC8225] defines a PASSporT, which is a JWT, that is used to verify the identity of a caller in an incoming call.

The PASSporT Extension for Diverted Calls draft [STIR] uses a nested PASSporT to deliver the details of an incoming call that get redirected. An authentication service acting for a retargeting entity generates new PASSporT and embeds the original PASSporT inside the new one. When the new target receives the nested PASSporT it will be able to validate the enclosing PASSporT and use the details of the enclosed PASSporT to identify the original target.

In this case, the original JWT is issued by the calling service, and the new enclosing JWT is issued by the retargeting service.

2.2.2. Network Service Mesh (NSM)

Network Service Mesh [NSM] is a mechanism that maps the concept of a service mesh in Kubernetes to L2/L3 payloads.

NSM GRPS messages may pass through multiple intermediaries, each of which may transform the message. Each intermediary is expected to create its own JWT token, and include a claim that contains the JWT it received with the message it has transformed.

In this case, the original JWT is issued by the entity sending the initial message, and the new enclosing JWT is issued by the intermediate entity.

3. Authorization Request

To allow the AS to differentiate between an authorization request for a single subject and an authorization request for multiple subjects, this document defines the following parameter:

issuer-hint:
: A hint to the AS that the request is for a multi-subject token, which can take one of two values:

  Internal
  : Indicates that the AS handling the current request will be issuing both enclosing and enclosed JWTs.

  External

Indicates that an external entity has issued the JWT to be enclosed, which will be carried in access_token parameter.

If the access_token query parameter is included in the request, then the AS SHOULD embed the provided token in the issued token, if the issuer-hint has the "External" value.

4. JWT Content

The payload of the enclosing JWT is JSON object that contains the Claims Set of the primary subject, and one new claim that is used to hold the enclosed JWT and its relation to the primary subject.

This document defines a new claim, "rsub" (Related Subject) Claim, that is used to contain the enclosed JWT and its relation to the primary subject. The "rsub" contains two claims:

rel:
Defines the relationship between the enclosed JWT and the enclosing JWT. It can take one of the values defined in section Section 5

jwt:
Contains the enclosed JWT.

5. Token Relationship

The following relathionship types are defined by this specification:

urn:ietf:params:oauth:subject-type:authority
Indicates that the subject in the enclosed JWT has authority over the subject in the enclosing JWT.

This URN could be used in the child/parent use case described in Section 2.1.1.

urn:ietf:params:oauth:subject-type:primary
Indicates that the subject in the enclosed JWT is related primary subject

This URN could be used in the married couple use case described in Section 2.1.2.

urn:ietf:params:oauth:subject-type:actor
Indicates that the subject in the enclosed JWT is acting on behalf of the primary subject

This URN could be used in the delegation use case described in Section 2.1.3.

urn:ietf:params:oauth:subject-type:original
Indicates that the subject in the enclosed JWT is the original JWT that resulted in the primary subject JWT

This URN could be used in all the use cases described in Section 2.2.

6. Example

The following example is for a multi-subject token that represents a child/parent relashionship. The enclosing JWT represents the primary user, the child in this case, and the enclosed token in the "rsub" claim represents the secondary user, the parent in this case.

```
{
  "alg": "HS256",
  "typ": "JWT",
}
{
   "sub": "1234567890",
   "name": "John Doe",
   "iat": 1516239022,
   "rsub": {
      “rel” :  "urn:ietf:params:oauth:subject-type:authority"
      “jwt” : {
         "sub": "9876543210",
         "name": "Alice Doe",
         "iat": 1516239022,
      }
   }
}
```

In this use case, both JWTs are issued by the same entity handling the authorization request.

7. Security Considerations

The existing security considerations apply to the use cases where the JWTs are issued by the same entity. Allowing more than one subject to access the same account might open the door for potential abuse. Care must be taken to ensure that when a secondary subject is added to an account that an adequate approval process is in place.

In the multiple issuers use cases, the entity handling the incoming authorization request that contains a JWT MUST validate the token and ensure that it is coming from a trusted entity, before attempting to embed that JWT into a new multi-subject JWT issued by the AS.

8. IANA Considerations

TODO

9. Acknowledgments

TODO

10. References

10.1. Normative References

[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>.

[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>.

10.2. Informative References

[RFC8225] Wendt, C. and J. Peterson, "PASSporT: Personal Assertion Token", RFC 8225, DOI 10.17487/RFC8225, February 2018, <https://www.rfc-editor.org/info/rfc8225>.

[RFC8693] Jones, M., Nadalin, A., Campbell, B., Bradley, J., and C. Mortimore, "OAuth 2.0 Token Exchange", October 2018.

[STIR] Peterson, J., "PASSporT Extension for Diverted Calls", October 2018.

Author's Address

Rifaat Shekh-Yusef
Okta
Ottawa, Ontario, Canada

Email: rifaat.s.ietf@gmail.com