OAuth Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 13, 2020

R. Shekh-Yusef
Avaya

September 10, 2019

Nested JSON Web Token (JWT)
draft-yusef-oauth-nested-jwt-03

Abstract

This specification extends the scope of the Nested JSON Web Token (JWT) to allow the enclosing JWT to contain its own Claims Set in addition to the enclosed JWT.

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 March 13, 2020.

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.

This specification extends the scope of the Nested JWT to allow the enclosing JWT to contain its own Claims Set in addition to the

enclosed JWT.

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. Overview

RFC7519 defines Nested JWT as a JWT in which nested signing and/or encryption are employed. In Nested JWTs, a JWT is used as the payload or plaintext value of an enclosing JWS or JWE structure, respectively.

To indicate that the payload of an enclosing JWT is yet another JWT, the value of the Content Type Parameter of the JOSE header, i.e. "cty", must be set to "JWT", which means that the enclosing JWT cannot have its own claims.

This document updates the enclosing JWT content to allow it to represent a Claims Set and an enclosed JWT, using JSON data structures, and updates the Content Type to indicate this new nested content.

3. Use Cases

3.1. Native App

The use case is for a telephony application that is based on the "Native Apps Using the Browser" flow defined in RFC8252. The Native App needs access to a telephony and non-telephony services that are controlled by different authorization servers, where the Native App can validate tokens issued by only one of these authorization servers.

The Native App starts the process by interacting with a Client that requires the user to authenticate itself using a Browser. The Browser starts by contacting an AS, which redirects it to an OP. The user authenticates to the OP and obtains a Code, and then gets redirected back to AS. The Native App gets access to the Code, then sends the Code to the AS, which then interacts with the OP to exchange the Code for an ID Token and OP Access Token. Since the Native App has no way of validating the OP Access Token, when the AS creates an AS Access Token, it embeds the OP Access Token inside the AS Access Token, and returns it back to the Native App. The Native App gets the AS Access Token and is able to validate it and extract

the OP Access Token, and access the different services protected with these tokens.

3.2. 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 origianl target.

3.3. 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 throught multiple intermediaries, each of which may transform the message. Each intermediary is expected to create its own JWT token, and include a claim that conains the JWT it received with the message it has transformed.

4. JWT Content Type Header Parameter

The JOSE Header contains an optional parameter that could be used to indicate the type of the payload of a JWT. With a typical Nested JWT, the value of the "cty" header must be "JWT". To indicate that the payload contains a Claims Set in addition to the JWT, the value of the "cty" header must be "NJWT".

5. JWT Content

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

This document defines a new claim, "njwt", that is used to contain the enclosed JWT.

6. Example

```
{
  "alg": "HS256",
  "typ": "JWT",
  "cty": "NJWT"
}

{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022,
  "njwt": "<njwt>"
}
```

7. Security Considerations

TODO

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

[NSM] "Network Service Mesh (NSM), https://networkservicemesh.io".

[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>.

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

Author's Address

Rifaat Shekh-Yusef

Avaya
425 Legget Drive
Ottawa, Ontario
Canada

Phone: +1-613-595-9106
EMail: rifaat.ietf@gmail.com