Multi-Subject JWT
https://datatracker.ietf.org/doc/draft-yusef-oauth-nested-jwt/

Rifaat Shekh-Yusef
OAuth WG, Interim Meeting
March 29th, 2021
Background

- RFC7519 defines the JSON Web Token (JWT) concept and includes a description of the Nested JWT concept.
- Nested JWT is a JWT that its payload contains another JWT.
Goal

• There are several use cases that require **multiple related subjects** to be represented in a token.

• The goal of this draft is to define a **JWT** that can represent these **multiple subjects** and the **relationship** between them.
Primary/Secondary Related Subjects

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

• A primary subject delegates authority over a resource to a secondary subject who acts on behalf of the primary subject, e.g., user/admin.
Replaced Primary Subject – STIR

• PASSporTExtension for Diverted Calls draft uses nested PASSporTs to deliver information about diverted calls.
Replaced Primary Subject – NSM

• **Network Service Mesh (NSM)** is a mechanism that maps the concept of a service mesh in Kubernetes to L2/L3 payloads.
  – [https://networkservicemesh.io/](https://networkservicemesh.io/)

• NMS messages pass through, and might be transformed, by multiple intermediaries.
• 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.
JWT Content

• Define a new claim, e.g., rsub (Related Subject), to hold the secondary subject and its relationship with the primary subject.
Example

```json
{
    "sub": "1234567890", // primary subject
    "name": "John Doe",
    "iat": 1516239022,
    "rsub": { // related subject
        "rel": "urn:ietf:params:oauth:subject-type:authority",
        "rel": "urn:ietf:params:oauth:subject-type:primary",
        "rel": "urn:ietf:params:oauth:subject-type:actor",
        "rel": "urn:ietf:params:oauth:subject-type:original",
        "jwt": "<jwt>
    }
}
```
Questions?