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

Rifaat Shekh-Yusef, Dick Hardt, Giuseppe De Marco
OAuth WG, IETF114, Philadelphia, PA, USA
July 25th, 2022
Goal

• There are several use cases that require one or more embedded tokens to be represented in a JWT.
• The goal of this draft is to define a JWT that can represent these embedded tokens and the relationship between them.
Purpose

• Audit trail
• Real-time display of information
• Evaluation
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.
Multiple Issuers for same Subject

• A JWT may have embedded claims from one or more separate Issuers.
  – An ID Token may have identity claims from independent issuers such as DOB and a professional accreditation.
Multiple Attribute Authorities

• A JWT may have embedded tokens to be consumed by one or more Attribute Authorities.
  – An ID Token may have multiple special tokens issued by OP/AS to be used by the client to contact the AA to obtain access tokens
JWT Content

• Define a new claim, e.g., **tokens**, to hold the **embedded tokens** and their **relationship** with the **primary subject**.
Child/Parent Token

{
    "sub": "1234567890", //Child
    "name": "John Doe",
    "iat": 1516239022,
    "tokens": [{
        "type": "urn:ietf:params:oauth:subject-type:authority",
        "jwt": {  //Parent
            "sub": "9876543210",
            "name": "Alice Doe",
            "iat": 1516239022
        }
    }]
}

}
Multiple Embedded Tokens

```json
{
iss: "https://op.it/",
sub: "0P-1234567890",
aud: "https://rp.it/",
acr: "https://www.spid.gov.it/SpidL2",
at_hash: "qiyh4XPJGsOZ2MEAyLkfWqeQ",
iat: 1519032969,
nbf: 1519032969,
exp: 1519033149,
jti: "nw4J0zMwRk4kRbQ53G7z",
nonce: "MBzGqyf9QytD28eupyWhSqMj78WNqpc2",
tokens: [
  {
type: "https://spid.gov.it/attribute-authority/grant-token",
aud: "https://deleghedigitali.gov.it",
token: "eyJhbGciOiJS... " },
  {
type: "https://spid.gov.it/attribute-authority/grant-token",
aud: "https://as.aa2.it",
token: "eyJhbGciOiJS... " },
  {
type: "https://spid.gov.it/attribute-authority/grant-token",
aud: "https://as.aa3.it",
token: "eyJhbGciOiJS... " }
]
}
```
Questions?

• Any thoughts?
• Should the WG work on this problem?
• Any other use cases?