### **Nested JWT**

Rifaat Shekh-Yusef
IETF105, OAuth WG, Montreal, Canada
26 July 2019

# 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.

#### **Nested JWT Limitation**

 As currently defined, the payload of the enclosing JWT is limited to containing the full enclosed JWT only.

### Goal

 Extend the scope of the Nested JWT to allow the payload of the enclosing JWT to contain its own Claims Set in addition to the enclosed JWT.

# **Native App Use Case**

- A Native App that needs access to:
  - A telephony service controlled by an AS
  - A non-telephony service controlled by an OP
- The Native App is aware of the **AS**, but not **OP**.

#### Flow:

- Native App launches a browser to authenticate the user
- Browser calls AS, which redirects it to OP
- User authenticates and obtains a code from OP
- Native App gets the code and sends it to AS
- AS exchanges the code with an OP Token
- AS creates its own AS Token and embeds the OP Token inside it.

#### **STIR Use Case**

 PASSporT Extension for Diverted Calls draft uses nested PASSporTs to deliver information about diverted calls.

#### • Flow:

- A calls B with a JWT (PASSporT)
- A's call is retargeted to C
- An authentication service acting for a retargeting entity generates new JWT and embeds the original JWT inside the new one.

## **JWT Content Type Header Parameter**

Define a new value for the cty header, e.g.
 NJWT, to indicate that the payload contains a
 Claims Set in addition to the JWT.

#### **JWT Content**

 Define a new claim, e.g. njwt, that would be used to contain the enclosed JWT.

## **Example**

```
"alg": "HS256",
"typ": "JWT",
"cty": "NJWT"
"sub": "1234567890",
"name": "John Doe",
"iat": 1516239022,
"njwt": "<njwt>"
```

# **Questions?**

Adoption?