NESTED JWT

RIFAAT SHEKH-YUSEF
IETF104, OAuth WG, Prague, Czech Republic
28 March 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.
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.
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?