JWT Embedded Tokens

Rifaat Shekh-Yusef, Dick Hardt, Giuseppe De Marco
OAuth WG, IETF117, San Francisco, CA, USA
July 26, 2023
Problems

1. Bind claims generated by independent issuers
2. Bind access tokens to each other and other claims
3. Bind claims generated during each stage of processing
Use Cases

• Example Use Cases
  – Network Service Mesh (NSM)
  – Identity Chaining
  – Entity Attestation Token (EAT)

• References
  – W3C-Verifiable Credentials Data Model v1.1
    • https://www.w3.org/TR/vc-data-model/
  – More Instant Messaging Interoperability (MIMI) Identity Concepts
    • https://datatracker.ietf.org/doc/draft-mahy-mimi-identity/
  – Dipartimento per la trasformazione digitale (PCM), Italia
    • https://docs.italia.it/italia/spid/spid-cie-oidc-docs/it/versione-corrente/standards.html#technical-references
  – Identity Chaining/Transaction Tokens
    • https://datatracker.ietf.org/doc/draft-tulshibagwale-oauth-transaction-tokens/
Possible Approaches

1. Each problem space defines its own claim type

2. A general mechanism to embed one or more tokens as claims in a new token.
   - Top level claim: "tokens": [{"type": "xxx"}]
     A. Generic Types "type": "id_token"
     B. Specific Types "type": "claim_specific_identifier"
2(A) Generic Type

• Other claims are likely required for context

```json
{
  "sub" : "1234",
  "tokens" : [
    {
      "type" : "id_token",
      "token" : "eyasas....",
      "delegate" : "mother"
    }
  ]
}
```

Eg types: access_token, id_token_reference
2(B) Specific Type

• Other claims are likely required for context

```json
{
    "sub":"1234",
    "tokens"[{
        "type":"https://spid.gov.it/aa/grant-token",
        "access_token":"eyasas...."
    }]
}
```
Is Approach 1 Good Enough?

- Each problem defines their own top level claim

```json
{
    "sub":"1234",
    "https://spid.gov.it/aa/grant-token":"eyasas...."
}
```
Latest Document Change

In some cases, the embedding of tokens into a new token could be done \textit{locally}, if that entity is trusted to do so. If this is the case, the request/response process to the AS is not required.
Adoption?

• Is the WG interested in solving this problem?