Assurance for JWT

Jim Basney <jbasney@ncsa.illinois.edu>
28th TAGPMA Face-to-Face Meeting
Dec 13 2019
Goal of this session

With the publication of the WLCG Common JWT Profiles (https://doi.org/10.5281/zenodo.3460257) and adoption by the scitokens.org project (and others), it is timely for TAGPMA to discuss assurance for these tokens and how it relates to our existing assurance frameworks.
Assurance

https://refeds.org/assurance

Maps to Kantara and IGTF assurance levels

https://refeds.org/profile/sfa

https://refeds.org/profile/mfa
JSON Web Token (JWT)

JSON Web Tokens are an open, industry standard RFC 7519 method for representing claims securely between two parties.

Standard claims: "iss" (Issuer), "sub" (Subject), "aud", "exp" (Expiration Time), "nbf" (Not Before), "iat" (Issued At), "jti" (JWT ID)


https://jwt.io/
JWTs in OAuth / OIDC

OAuth
Authorization
access_token (opaque)

OpenID Connect (OIDC)
https://openid.net/connect/
Authentication
id_token (JSON)
Example id_token

{
   "iss": "http://server.example.com", "sub": "248289761001",
   "aud": "s6BhdRkqt3", "nonce": "n-0S6_WzA2Mj",
   "exp": 1311281970, "iat": 1311280970,
   "name": "Jane Doe", "given_name": "Jane", "family_name": "Doe",
   "gender": "female", "birthdate": "0000-10-31",
   "email": "janedoe@example.com",
   "picture": "http://example.com/janedoe/me.jpg"
}

https://openid.net/specs/openid-connect-core-1_0.html#id_tokenExample
WLCG Common JWT Profiles

Group Based Authorization (wlcg.groups) and Capability Based Authorization (scope)

3 scenarios: 1) Identity Token with Groups, 2) Access Token with Groups, and 3) Access Token with Authorization Scopes

https://doi.org/10.5281/zenodo.3460257
SciTokens

Capability Based Authorization (scope)

OAuth access_token (JWT)

Following WLCG JWT Profile type 3: Access Token with Authorization Scopes

https://scitokens.org/
WLCG JWT Example (1)

```json
{
    "wlcg.ver": "1.0",
    "sub": "e1eb758b-b73c-4761-bfff-adc793da409c",
    "iss": "https://dteam.wlcg.example",
    "wlcg.groups": ["/dteam/VO-Admin", "/dteam", "/dteam/itcms" ],
    "preferred_username": "aresearcher",
    "nonce": "334b0e05b65a3", "jti": "aef94c8c-0fea-490f-9027-ff444dd66d8c",
    "aud": "https://dteam-test-client.example.com",
    "auth_time": 1523363636, "exp": 1523365436, "iat": 1523363636,
    "email": "a.researcher@cern.ch",
    "eduperson_assurance": ["https://refeds.org/assurance/profile/espresso"],
    "acr": "https://refeds.org/profile/mfa"
}
```
WLCG JWT Example (2)

{
    "wlcg.ver": "1.0",
    "jti": "a46ae991-6f1c-4e06-979b-967966740abb",
    "iss": "https://demo.scitokens.org",
    "sub": "joe",
    "nbf": 1555060120,
    "iat": 1555060120,
    "exp": 1555060720,
    "scope": "storage.read:/home/joe"
}
OpenID Connect for Identity Assurance

https://openid.net/specs/openid-connect-4-identity-assurance-1_0-ID1.html
"iss": "https://server.example.com",
"sub": "24400320",
"aud": "s6BhdrKq7t3",
"nonce": "n-056 WzA2Mj",
"exp": 1311281976,
"iat": 1311280976,
"auth_time": 1311280969,
"acr": "urn:mace:incommon:iap:silver",
"email": "janedoe@example.com",
"preferred_username": "j.doe",
"picture": "http://example.com/janedoe/me.jpg",
"verified_claims": {
  "verification": {
    "trust_framework": "de_aml",
    "time": "2012-04-23T18:25:43.511+01",
    "verification_process": "676q3636461467647q8498785747q487",
    "evidence": {
      "type": "id_document",
      "method": "pipp",
      "document": {
        "type": "idcard",
        "issuer": {
          "name": "Stadt Augsburg",
          "country": "DE"
        },
        "number": "53554554",
        "date_of_issuance": "2012-04-23",
        "date_of_expiry": "2022-04-22"
      }
    }
  },
  "claims": {
    "given_name": "Max",
    "family_name": "Meier",
    "birthdate": "1956-01-28"
  }
}
Discussion