JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens

draft-ietf-oauth-access-token-jwt-05

Vittorio Bertocci

Virtual Interim Meeting

April the 13th, 2020

JWT AT profile in a nutshell

- Claims layout for the entities most commonly recurring in existing JWT ATs
- Token validation & AS metadata discovery guidance
- Detailed security and privacy considerations
- Clear relationship between resource references, scopes and token content

- Previous presentations on the topic:
  - OSW https://sec.uni-stuttgart.de/_media/events/osw2019/slides/bertocci_-_a_jwt_profile_for_ats.pptx
  - IETF104 https://datatracker.ietf.org/meeting/104/materials/slides-104-oauth-sessa-jwt-profile-for-access-token-00
  - IETF105 https://datatracker.ietf.org/meeting/105/materials/slides-105-oauth-sessb-json-web-token-jwt-profile-for-oauth-20-access-tokens-02-00

Working Group Last Call

- Issued on March 23rd, on version-04
- Many suggestions since then

Main Changes since WGLC

- Clarifications
  - `amr`, `acr`, `auth_time`, `iat` behavior
  - error responses to be used on validation errors (`invalid_token`)
  - Warning about the futility of using different keys for signing ATs and ID tokens as security measure
  - Clarified that the JWT AT validation steps aren’t meant to be executed in strict sequence
- Normative
  - Removed explicit `auth_time` check description
  - `iat`, `jti` OPTIONAL->RECOMMENDED
- General editorial cleanup

Open Questions

- Should JTI, IAT be REQUIRED?
- Should single resource/audience constraints be relaxed?
- New
  - Should the profile be richer? If yes, what’s missing?
  - “privacy”

Should `jti`, `iat` be REQUIRED?

- I think so.

Single resource/audience constraints (1/3)

client

```
{"typ":"at+jwt","alg":"RS256","kid":"RjEwOwOA"}
{
     "iss": "https://authorization-server.example.com/",
     "sub": " 5ba552d67",
     "aud":   "https://example1.org/someAPI
              https://example2.org/someOtherAPI",
     "exp": 1544645174,
     "client_id": "s6BhdRkqt3_",
     "scope": "read"
   }
```

example1.org/someAPI

Recognized scopes
read
write
someScope

example2.org/someOtherAPI

Recognized scopes
read
someOtherScope

Scope confusion: it’s not clear whether read has been granted for both API or just one, an in the latter case which one

Single resource/audience constraints (2/3)

- Section 3. Requesting a JWT Access Token

  If it receives a request for an access token containing more than one resource parameter, an authorization server issuing JWT access tokens MUST reject the request and fail with "invalid_request" as described in section 4.1.2.1 of [RFC6749] or with "invalid_target" as defined in section 2 of [RFC8707]

- Section 5. Security Considerations

  This profile explicitly forbids the use of multi value aud claim when the individual values refer to different resources, as that would   introduce confusion about what scopes apply to which resource-   possibly opening up avenues for elevation of delegated privileges attacks.

Single resource/audience constraints (3/3)

- We could weaken the language and turn it into a security recommendation
- Feels like a missed opportunity, tho

JWT Access token layout – anything missing?

claim name		function
iss	REQUIRED	validation
exp	REQUIRED	
aud	REQUIRED	
iat	RECOMMENDED	
auth_time	OPTIONAL	
sub	REQUIRED	identity
<identity claims>	OPTIONAL	
scope	when scope is present in the request, REQUIRED	authorization
groups, roles, entitlements	OPTIONAL	
client_id	REQUIRED	context
jti	RECOMMENDED	
acr, amr	OPTIONAL	

Privacy

- My initial position
  - this isn’t SSI: the privacy bar is the same as the rest of OAuth2/OIDC in use
  - The main extra nuance is the possibility that the client might have access to info that are passed form AS to RS directly in opaque tokens
- Anything missing?

Appendix