Virtual Interim Meeting
April the 13th, 2020

JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens
draft-ietf-oauth-access-token-jwt-05

Vittorio Bertocci
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)

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?

<table>
<thead>
<tr>
<th>claim name</th>
<th>function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>iss</strong></td>
<td>REQUIRED validation</td>
</tr>
<tr>
<td><strong>exp</strong></td>
<td>REQUIRED</td>
</tr>
<tr>
<td><strong>aud</strong></td>
<td>REQUIRED</td>
</tr>
<tr>
<td>iat</td>
<td>RECOMMENDED</td>
</tr>
<tr>
<td>auth_time</td>
<td>OPTIONAL</td>
</tr>
<tr>
<td><strong>sub</strong></td>
<td>REQUIRED identity</td>
</tr>
<tr>
<td>&lt;identity claims&gt;</td>
<td>OPTIONAL</td>
</tr>
<tr>
<td><strong>scope</strong></td>
<td>when scope is present in the request, REQUIRED authorization</td>
</tr>
<tr>
<td>groups, roles, entitlements</td>
<td>OPTIONAL</td>
</tr>
<tr>
<td><strong>client_id</strong></td>
<td>REQUIRED context</td>
</tr>
<tr>
<td>jti</td>
<td>RECOMMENDED</td>
</tr>
<tr>
<td>acr, amr</td>
<td>OPTIONAL</td>
</tr>
</tbody>
</table>
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 from AS to RS directly in opaque tokens

• Anything missing?
Appendix