JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens-02

Vittorio Bertocci

IETF 105
July the 26th
Agenda

• JWT profile for OAuth Access Tokens recap
• Changes and open issues
Recap
Why a JWT profile for OAuth2 ATs?

• Most providers already issue ATs as JWTs
• The tokens contain ~ the same entities, but different syntax
• No guidance led/leads to questionable choices
• Common antipattern: clients sending their idtoken to APIs
JWT profile for AT in a nutshell

• A claims layout for the entities most commonly included in existing JWT ATs
• Clear relationship between resource references, scopes and token content
• Token validation guidance
• Detailed security and privacy considerations

• Previous presentations on the topic:
  • OSW
    https://sec.uni-stuttgart.de/_media/events/osw2019/slides/bertocci_-_a_jwt_profile_f or_ats.pptx
  • IETF104
    https://datatracker.ietf.org/meeting/104/materials/slides-104-oauth-sessa-jwt-profile-f or-access-token-00
JWT Access Token Layout - Minimal

• Smallest possible JWT AT when scopes are requested

```json
{"typ":"at+jwt","alg":"RS256","kid":"RjEwOwOA"}
{
  "iss": "https://authorization-server.example.com/",
  "sub": "5ba552d67",
  "aud": "https://rs.example.com/inbox",
  "exp": 1544645174,
  "client_id": "s6BhdRkqt3_",
  "scope": "reademail sendemail"
}
```
Changes and open issues
00->01/2 main changes

• Changed definitions source for iss, exp, aud, sub, iat (OIDC->7519)
• Added introspection as source of claim types, explicit reference to arbitrary attributes
• Expended privacy sections
• Added reminder that clients should not peek into ATs
• IANA registration template for at+JWT, SCIM claims
• Auth_time updates
• Removed note on subject type
• Removed note on federated IdPs
Discussion

- Distinguishing between user and app tokens
- Auth_time behavior
- Authenticated encryption
Distinguishing between user and app ATs

• Approached discussed
  • No sub for app tokens
  • Have a “grant_type” claim
  • [sub == client_id] => app token
  • “subject_type” claim
Auth_time (amr, acr)

• Doubts about complexity, ambiguity
Authenticated encryption

• Should we recommend it despite the current specs being only symmetric?
Appendix
## JWT Access token layout

<table>
<thead>
<tr>
<th>claim name</th>
<th>original definition</th>
<th>function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>iss</strong></td>
<td>REQUIRED</td>
<td>7519</td>
</tr>
<tr>
<td><strong>exp</strong></td>
<td>REQUIRED</td>
<td>7519</td>
</tr>
<tr>
<td><strong>aud</strong></td>
<td>REQUIRED</td>
<td>7519</td>
</tr>
<tr>
<td><strong>iat</strong></td>
<td>OPTIONAL</td>
<td>7519</td>
</tr>
<tr>
<td>auth_time</td>
<td>OPTIONAL</td>
<td>OpenID.Core</td>
</tr>
<tr>
<td><strong>sub</strong></td>
<td>REQUIRED</td>
<td>7519</td>
</tr>
<tr>
<td>&lt;identity claims&gt;</td>
<td>OPTIONAL</td>
<td>OpenID.Core, Introspection, etc</td>
</tr>
<tr>
<td><strong>scope</strong></td>
<td>when scope is present in the request, REQUIRED</td>
<td>token exchange</td>
</tr>
<tr>
<td>groups, roles, entitlements</td>
<td>OPTIONAL</td>
<td>SCIM Core 7643</td>
</tr>
<tr>
<td><strong>client_id</strong></td>
<td>REQUIRED</td>
<td>.token exchange</td>
</tr>
<tr>
<td>jti</td>
<td>OPTIONAL</td>
<td>7519</td>
</tr>
<tr>
<td>acr, amr</td>
<td>OPTIONAL</td>
<td>OpenID.Core</td>
</tr>
</tbody>
</table>
Requesting JWT Access Tokens

- Any existing grant returning an access token can return a JWT access token
- If a request contains `resource`, its value must be reflected in `aud`
  - No multi-value `resource` admitted in reqs for JWT access tokens (scope confusion)
- Without `resource` in the req, the authorization server either
  - Infers the resource indicator from `scope` and assigns it to `aud`
    - All scope strings must refer to the same resource
    - Or assigns a default value
- If a request contains `scope`, the resulting JWT access token must feature a `scope` claim
- Whether to include identity claims, non-delegation claims or custom claims is an agreement between authorization server and resource server
  - The client has no say on the matter
<table>
<thead>
<tr>
<th>Claims</th>
<th>idtoken</th>
<th>Auth0</th>
<th>Azure AD</th>
<th>PingIdentity</th>
<th>IdentityServer</th>
<th>AWS</th>
<th>OKTA</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation</td>
<td>iss</td>
<td>aud</td>
<td>exp</td>
<td>iat</td>
<td>nonce</td>
<td>auth_time</td>
<td>iss</td>
<td>aud</td>
</tr>
<tr>
<td>Identity</td>
<td>sub</td>
<td>lots</td>
<td>sub</td>
<td>&lt;any&gt;</td>
<td>sub</td>
<td>name</td>
<td>preferred_username</td>
<td>oid</td>
</tr>
<tr>
<td>Authorization</td>
<td>N/A</td>
<td>scope</td>
<td>roles</td>
<td>scp</td>
<td>groups</td>
<td>scope</td>
<td>memberOf</td>
<td>scope</td>
</tr>
<tr>
<td>Context/misc</td>
<td>azp</td>
<td>acr</td>
<td>amr</td>
<td>azp</td>
<td>gty</td>
<td>allo</td>
<td>appid</td>
<td>idp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>