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_for_ats.pptx
  - IETF104 https://datatracker.ietf.org/meeting/104/materials/slides-104-oauth-sessa-jwt-profile-for-access-token-00

JWT Access Token Layout - Minimal

- Smallest possible JWT AT when scopes are requested

```
{"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

claim name		original definition	function
iss	REQUIRED	7519	validation
exp	REQUIRED	7519	
aud	REQUIRED	7519	
iat	OPTIONAL	7519	
auth_time	OPTIONAL	OpenID.Core	
sub	REQUIRED	7519	identity
<identity claims>	OPTIONAL	OpenID.Core, Introspection, etc	
scope	when scope is present in the request, REQUIRED	token exchange	authorization
groups, roles, entitlements	OPTIONAL	SCIM Core 7643	
client_id	REQUIRED	token exchange	context
jti	OPTIONAL	7519	
acr, amr	OPTIONAL	OpenID.Core	

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 assign 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

Claims	idtoken	Auth0	Azure AD	PingIdentity	IdentityServer	AWS	OKTA	Profile
Validation	iss aud exp iat nonce auth_time	iss aud exp iat	iss aud exp iat nbf	iss exp jti [aud]	iss aud nbf exp auth_time	iss iat exp auth_time	iss aud iad exp	iss aud exp iat jti auth_time
Identity	sub lots	sub <any>	sub name preferred_username oid ipaddr unique_name	sub email uid	[sub]	sub username	sub cid uid	sub
Authorization	N/A	scope	roles scp groups	scope memberOf	scope	scope	scp	scope roles, groups, entitlements
Context/misc	azp acr amr	azp gty	aio app_displayname appid idp tid uti ver xms_tcdt --- azp azpacr	idpid client_id	client_id idp amr	token_use	ver	client_id acr amr