OAuth 2.0 JWT Authorization Request (OAuth JAR)

IETF 94 Yokohama

Nat Sakimura (Nomura Research Institute)

John Bradley (Ping Identity)

Received comments

- Two contributions (Hannes, Brian)
  - Editorial Comments: 12
  - Technical Comments: 9

Technical Comments

- 1. Introduction
  - 2. Statically signed request object – replay threats?
  - 3. Cached request – ditto
  - 4. Tampering advantage needs to be explained better.
- 3. Request Object
  - Unclear whether the request object be JWE only.
  - Conflict with PoP Key Distribution Draft
    - '... the Authorization Request Object SHOULD contain the Claims "iss" (issuer) and "aud" (audience) as members ...', however, that will produce a parameter name conflict with the "aud" parameter from OAuth 2.0 Proof-of-Possession: Authorization Server to Client Key Distribution. Seems like draft-ietf-oauth-pop-key-distribution will need to change its parameter name (aud in JWT is pretty well established). And shouldn't draft-ietf-oauth-jwsreq register some of the JWT's Registered Claim Names (at least iss and aud but maybe exp and others) as authorization request OAuth parameters?

Technical Comments (continued)

- 4.2.1. URL Referencing the Request Object
  - Drop second para as it is OIDC specific.
- Section 5.2
  - Should request_object_signing_alg live here or just normatively refe rence OIDC, or should it go to registration draft?
- Section 6
  - Error response: Just normatively reference 3.1.2.6 of OpenID Conn ect Core and do not duplicate here.
- Section 7
  - Flase statement:
    - The request_object_signing_alg OAuth Dynamic Client Registration Metadat a is pending registration by OpenID Connect Dynamic Registration specificati on.
    - The registry doesn't have it and Connect's Registration "makes no requests o f IANA".