Notes taker: **Jared Jennings**.

The Web Authorization Protocol (oauth) Working Group virtual interim meeting on 2020-04-20 from 12:00 to 13:00 America/Toronto (16:00 to 17:00 UTC).

Agenda:
1. Pushed Authorization Requests
https://datatracker.ietf.org/doc/draft-ietf-oauth-par/

2. Rich Authorization Requests
https://datatracker.ietf.org/doc/draft-ietf-oauth-rar/

Participants

1. Torsten Lodderstedt
2. Anthony Nadalin
3. Bhupinder Singh
4. Brian Campbell
5. Brock Allen
6. Cristofer Gonzales
7. Daniel Fett
8. Dominick Baier
9. Filip Sokokan
10. Francis Pouatcha
11. George Fletcher
12. Janak Amarasena
13. Jim Schaad
14. Justin Richer
15. Mark McFadden
16. Matt De Haast
17. Michael Breuer
18. Mike Jones
19. Peter Yee
20. Roman Danyliw
21. Sebastian Ebling
22. Tim cappalli
23. Tim Costello
24. Rifaat Shekh-Yusef

1. Hannes Tschofenig

Action Items

1. Torsten will provide the proposed text to the list after talking with the editors
2.

Torsten - Pushed Authorization Requests
DRAFT
What is it?

- new pushed authorization request endpoint, which allows
    - Pushed OAuth 2.0 payload (Authorization Request)
- Two modes of authorization
    - PAR Body
    - Signed/encrypted request object

Same data, but sent directly to AS

Benefits

- Support for large AUTHZ requests
- TLS provides integrity & confidentiality
- Client authentication and authorization
- Signed request object additionally provides non-repudiation

Draft Status

- WG draft adopted
- Part of FAPI 2 baseline profile
- Several implementations exist today
    - Norwegian eID system
    - Norwegian eHealth system
    - Proposed for adoption in Australia CDR initiative

Open: request_uri must refer to JWT

- PAR deviates from this requirement
    - Annabelle proposed to add the following text to PAR:
        - An AS MAY violate this requirement when it is generating the request URIs intended for its own consumption (e.g., URIs for pushed requests). This requirement exists to ensure interoperability in cases where the provider of the request_Uri is a seeparate entity from the consumer, such as when a client provides a URI reference an object stored o the client's backend service. When the AS is both provider and consumer, this interoperability concern does not apply.
    - Roman: If we need to make a change, it can be pulled from ISG review and updated and reposted for review.
    - George: How big of a change is this to JAR?
        - Torsten: What do existing PAR implementations feel about request_uri's.
    - Justin: Im were able to handle request_uri's and were able to use all the same fields because the request object already uses.
    - Filip: Also implemented JAR and was able to reuse the parameters. Does recommend that the spec parameter be fixed/updated, doesn't matter in which spec.
    - Torsten: Believes that keeping the request_uri parameter is be best option and update the wording.
    - Roman: Would like to see the updated text for review.
    - Torsten: The WG will be updated and voted on - action item
- Can AS require PAR?
    - Client specific and/or AS wide policy
        - Meaning: client is no longer allowed to use traditional
    - Can AS require request object?

        - Client specific and/or AS wide policy
        - Similar discussion in OpenID Connect WG resolve by using request_object_signing_alg client metadata parameter to signal client signed request objects only
        - We could adopt the same solution
        - Should we provide guidance on teh URI request structure

Rich Authorization Requests
What is it:

- It is a way to specify scopes and in JSON notation
- Each JSON may require authorization requirements for certain types of resource
- Allows APIs to define their own structure for authorization requests
- However, the draft also defines common elements

Features:

- Allows a bonination of requirements
- Locations can be combined
- Resoruce parameter is used to select authorization details for RS-specific access tokens
- authorization_details parameter can be used and can be used in combination with scope or instead of

Advantages:

- Flexible and type safe
- Allows definition of API-specific authorization data structures
- Common data set that addresses common use cases
- Interoperable and easy way to issue RS-specific Access Tokens and introspection Responses

Status:

- Draft adopted as WG document
- Part of FAPI 2 baseline profile
- Implementation experience
    - back ported from OAuth.XYZ to OAuth 2
    - Used by Authlete, Norwegian eHealthy system, Norwegian Tax System, Australian CDR initiative
- Used in XAuth proposal for TXAuth
- Base design works, a lot of details yet to be worked out
- Additional features might be required based on early implementer feedback

Open Topics:

- Interplace with scope, audience and resource parameters &claims
- Authorization_details in token request to narrow down previously granted consent
- Required vs. useful common eleemnts ("type", vs. "datatypes")
- Mutual alignment between RAR and TXAuth
- Guidance on schemas and versioning
- Enrichment authorization_details in token response
    - Account selection

- Validity of authorization detail
    - E.G. include duration of the authorization in the Token Response

Comments:

- George: Loves the idea, but it feels like we are trying to implement fine-grained authorization. We want to be careful with the wording. "We must be careful with the interop wording"
- Justin: Agrees with what Torsten has proposed. Yet, interop will be difficult, but a layered approach is best
- Matt: I would be hesitant to add layers and normative language. It maybe should be accomplished at higher levels, like how OIDC accomplished this.

Meeting Concluded

Meeting Recording:
https://ietf.webex.com/recordingservice/sites/ietf/recording/playback/17c34ecc178f437f9d34c45d50eac60a