Details for today's meeting can be found at
https://datatracker.ietf.org/doc/agenda-interim-2020-oauth-08-oauth-01/

WebEx recording can be found at
https://www.youtube.com/watch?v=Yhz2u-LR6SI

Agenda

1. Client Intermediary Metadata
    a. https://tools.ietf.org/html/draft-parecki-oauth-client-intermediary-metadata-00
2. Reciprocal OAuth
    a. https://tools.ietf.org/html/draft-ietf-oauth-reciprocal-04

Announcements

- WGLC on JWT Profile to Access Tokens
- WGLC on JWT response to OAuth Token Introspection
- New email address: rifaat.s.ietf@gmail.com

Attendees

1. Hannes Tschofenig
2. Rifaat Shekh-Yusef
3. Aaron Parecki
4. Andreas Falk
5. Annabelle Backman
6. Anthony Nadalin
7. Bhunpinder Singh
8. Brian Campbell
9. Denis
10. Dick Hardt
11. Filip Skokan
12. Francesca Palombini
13. Francis Pouatcha
14. Hadeel Elbitar
15. Janak Amarasena
16. Jared Jennings
17. Jonathan Huot
18. Justin Richer
19. Matt de Haast

20. Micah Silverman
21. Mike Jones
22. Peter Yee
23. Roman Dayliw
24. Thumilan Mikunthan
25. Tim Cappalli
26. Torsten Lodderstedt
27. Wiliam Lassiter

Reciprocal OAuth

Dick Hardt

Overview of Reciprocal Protocol Flow

- How can we simplify the flow of multiple parties?

Status

- WGLC on draft-ietf-oauth-reciprocal-04 Sep-6-19
- Some feedback (still to be incorporated)
- Question: Is there any WG interest in seeing this draft
    - Justin R: Interesting use case, but doesn't relate to anything Justin is working with right now.
    - Aaron P: Sounds like an interesting problem, but no immediate need.
- Comment: Dick H: TXAuth does address this and does make it much easier.
- Comment: Brian C: Did provide feedback earlier, but it was from wanting to provide feedback, but does not have any immediate need.
- **Roman D: The document will be parked at this time.**

Client Intermediary Metadata

Aaron Parecki

Use Case

1. **OAuth and User Consent** - Bank Application needs specific details of the request

    a. This works fine if the OAuth Client is a registered application with the Bank API
    b. Practically, likely this app is connected or could be connected to multiple banks. Meaning the developer hasn't registered it's application with all those banks.
    c. In reality, an Aggregator is used that has contracts / relationships with the various banks. The client would have a relationship with the aggregator.
        i. In this case, what is the client_id? The aggregator or the client app?
    d. The Goal:
        i. We want to demonstrate who the data will be shared with. The intermediary entity (The aggregator)

Goal

1. Build on-top of existing OAuth, but add Client Intermediary Metadata. "Intermediary"

Question

- **Annabelle** B: Why do the intermediary? Does the client need to know this intermediary?
    - Aaron P: This is deeply rooted in Financial Institutions and a current request.
- **Francis** P: In Europe, the account information must be provided by the provider. What appears to be the end-user application, but the license is with the entity (bookings), the business process. It is essential, by Law, the entity must display who has or will be using the data.
- **Dick** H: The aggregators are not always in the middle, but sometimes the customer data is moved / copied at the service. (It does not stay at the original location)
- **Annabelle**: What is the driver, or purpose or intent of the spec and what problem is being solved.
- **Francis** P: The problem being solved - showing which real authorizations are being given.
    - **Example**: Explicitly designed so that you can have multiple consents.
        - This falls apart today because if you revoke a consent, you revoke all consents.
        -
- **Torsten** L: Do we fully understand the problem we are trying to solve. "The problem is that the Aggregator provides its own set of API's."

    - Question: Who is the client in this scenario? It seems that the client flips.
    - Aaron P: In most cases:
        - The aggregator is acting on behalf of many end users applications.
        - In the case of Mint, Mint is not shown as the client, but the aggregator.
    - Torsten L: How many deployments already have this?
        - Aaron P: This is an active development situation and the entity is trying to build the standard now.
- Annabelle B: Is the expectation that the Bank is the authority on who has access at the Aggregator
    - Aaron P: No, the bank has a license with the aggregator.
    - Annabelle B: Who gets to revoke or gets final authority to who gets/denies access.
    - Aaron P: We need the metadata and information.
- Francis P: We have to distinguish which data is public here. In most cases, the relationship is between the Aggregator and the Bank, not the user or the third-party client.
    - We need to discuss and distinguish between:
        - Metadata: what does the bank need on the EUA
        - How to hold and when does this get transmitted to the banks

    Also consider

    -> Grant management. API

    Beware of Redirect-URI. Unless there is one client-id per EUA.

    -> Redirect-URI

- Tim C: Capital One and Chase both use similar flows and provide similar consent flows.

General Meeting Topics

One Topic meeting

Should meetings contain multiple topics or one topic.
Multiple +1 one topic per meeting.

Topic Duration

One Hour seems ideal or maybe 90 minutes.

Most support one hour per topic/meeting.

Meeting closed.