Introduction and Context  Chairs  10 min

No new WG this session, this may result in a future WG or a change to an existing WG Charter to take on this work.

Limitations and Feature Requests

Limitations of OAuth  Justin  10 min

OAuth world has grown up, too many specifications and how they all fit together.
Overuse of front channel, easy to use but security considerations
Things like the implicit flows are at risk
Based on single users
Static world, not dynamic, like SPA needs more dynamic resources
Issues with token presentations
Scopes are a mess, not well defined

Limitations of OAuth  Torsten  5 min

Rich authz requests
Use cases based upon open banking, strong identity, signatures
PSD2; Consent, dynamic lining, signatures
Needs all claims
Privileges are narrowed
Authz data fine grained on what needs access
Transaction values
Authz data may contains PII thus confidentiality
Integrity and confidentiality

Feature Requests  Justin  10 min

Feature Requests  Torsten  5 min

Sending data in URLs is very limiting, use a consistent data language/models
Extensions reinvent concepts
Device flows
JWT assertions
OAuth is about delegation
Software talking to software
Get the user involved
Grant types are the interaction types
Web based interactions
Who is the user
There are non-authorization needs, key introduction
OAuth is client heavy
This is SOAP for OAuth
Transport agnostic
Backwards compatibility

Non Authorize Features  Annabelle  15 min

How do you deal with other errors that are out of the scope of auth, like insignificant funds, out of ink, etc.
Sending email, email fails why?
The main issue is connection multiple contexts for bi-lateral communications
Multiple channels involved
  End-user to source
  Source to problem
  End user notifications
  End user resolution context how to proceed
Source context may not be interactive

Proposals

OAuth XYZ [1] Justin  20 min

Reinvent OAuth not extension
  JSON
  Flexibility
  Consistency
  Transactions
User interaction definition
Non web interactions
Let’s go build OAuth 3

RAR & PAR [2] Torsten  20 min

Pushed Authorization Request
  Work based upon OpenID draft, complements JAR, pus authz payload to auth server
This is based upon OAuth 2 not something new

Rich Authz Requests
  Carry fine grained auth params in JSON
  Base upon FAPI WG and on XYZ
  Not a fixed structure, let them be app based
  User consent is complicated and needs to be able to be represented
  Data structures can be optimized to resource server/API no one size fits all
Mike, no doubt that OAuth has grown and gotten complex, but OAuth 2 is successful and creating a oauth 3 will splinter the community.

Took a sense of the room. There was consensus (though not unanimous) that there is a problem that needs to be solved.

Next Steps

Proposal to work on both an new OAuth and continue with the current extension path. A new version does not have to be totally different data structures. Get to a point of 1 document not all the docs we have now. Is OAuth the right solution for the problem or should there be something else? Amount of time to devote to both would be problematic.


https://datatracker.ietf.org/doc/draft-lodderstedt-oauth-rar/
https://datatracker.ietf.org/doc/draft-lodderstedt-oauth-par/