Rich Authorization Requests

draft-ietf-oauth-rar

OAuth Interim 20.10.2021

Brian Campbell, Justin Richer, Torsten Lodderstedt

Rich Authorization Requests

new parameter "authorization_details" allows to convey fine grained and structured authorization data as JSON objects

designed to be used where “scope” is not sufficient

Inspired by use cases and solutions in:

- Open Banking
- eHealth
- eSigning
- eGovernment

```
[
 {
  "type": "payment_initiation",
  "instructedAmount": {
    "currency": "EUR",
    "amount": "123.50"
  },
  "creditorName": "Merchant",
  "creditorAccount": {
    "iban": "DE021001...7118603"
  }
]
```

What has happened since last interim?

- Added "authorization_details" **token request parameter** and discussion on authorization details comparison (based on interim feedback)

Started WGLC on -05

- Special thanks to Dave Tonge and Jacob Ideskog!

Changes (revision-06 to -08)

- removed use of resource indicators to filter authorization details in token response
  - authorization_details & scope/resource are decoupled now
  - authorization details token request parameter only way to determine authorization details assigned to access token
- Editorial
  - Wording (payment initiation vs payment)
  - Add PAR reference to security/privacy/implementation considerations
  - Clarification on RO granting a subset of requested authorization details and authorization details enrichment (account numbers)
  - Clarification on omission of authorization details values in the token response not required by the client (privacy)
  - Added further examples for common data elements

Status

- Part of FAPI 2
  - Adoption in Australian CDR initiativ
- Implementations
  - Products: Authlete (since 2.2.8), Pyoidc (scaffolding)
  - Projects: Norwegian eHealth system, yes® ecosystem (4 different implementations on top of products w/o RAR support)
  - Adoption planned in Norwegian Tax System (tax declaration for SMBs)
- No open issues
- Ready for publication