# OAuth WG Interim Meeting

## Date

October 20, 2021, 12:00pm EDT

## Topic - RAR

Presenters: Torsten Lodderstedt
Draft: RAR
Slides: RAR Slides

# Notes

*Note Taker:* ***Aaron Parecki***

Admin update

- iss draft publication request sent
- will try to continue weekly meetings with the last on nov 3

RAR - Presented by Torsten

- Recap of RAR - enables fine-grained and structural authorization data in place of scope
- Updates since last interim - May
  - added "authorization_details" as token request parameter
  - published revision -05 and started WGLC
- Changes (revisions -06 to -08)
  - most significant change was to remove use of resource indicators
- Justin: authorization_details doesn't prohibit scope/resource indicators with this, but RAR doesn't define a relationship between the two. It's up to the AS to decide the relationship if any. RAR is encouraging the use of authorization_details to convey all the info now.
- Torsten: Status
  - RAR is part of FAPI version 2, Australian CDR is adopting RAR

    - Implementations in several products and some planned
    - No open issues
    - Ready for publication
- Queue open
- Jeff: OAuth 2.0 has a broad definition for scope grammar which presumably could be used for a similar purpose. With OAuth 2.1 in consideration should we narrow the grammar for scope in favor of RAR?
- Torsten: Seen lots of attempts at packing complex things into scope. As co-author of 2.1 I would prefer to point out to implementers that there is something else if they have complex authorization details, but not necessarily limit the syntax of scope.
- Justin: I sympathize with the desire to get rid of structured scopes. But in practice you can't get away from people defining an internal syntax of scopes. Agreed with Torsten that 2.1 should say something about scope-based access and point people to RAR. But I don't think we can go as far as changing the ABNF for scope values at this point, even in 2.1 narrowing that will lead to people being non-compliant and not caring that they are non-compliant.
- Dick: In 2.1 we agreed to not have normative changes, only best practices. It would be great to point to RAR in the scope section of 2.1 if you want richer scopes.
- Aaron: +1 to that approach
- Denis: Two concerns with the privacy section. If RAR is suppose to replace scope, I was expecting to have more flexibility for the AS sub value. If there is none, then I would expect this document to mention that there is no flexibility in choosing the sub claim.
- Torsten: authorization details, like scope, requests access to something that results in an access token being issued. What "sub" claim are you referring to, the "sub" claim in an access token?
- Denis: The sub claim in an access token. [read quote from JWT access token spec] Without scope, then there is no flexibility in RAR to choose the sub values.
- Torsten: Whether there is AS/RS separation is between those, not the client. I would not expect the client to be able to influence anything in the access token. Whether the client uses scope or RAR has no effect. RAR lets the AS issue audience-specific access tokens. The client can describe where it wants to use the access token, then the AS can put the correct scope in the access token. RAR allows even better than scopes to use different subjects or resource values.

- Denis: When we speak about privacy we speak about privacy of the user. The JWT profile says the AS should choose sub value according to the level of privacy required. The end user is in the best place to choose what level of privacy is required, not the AS or RS.
- Torsten: If you're expecting the user to decide what identifier to use then it doesn't make a difference whether to use RAR or scope. I understand from your last statement that you want the user to choose what sub value is in the token
- Denis: Not the value, but the type.
- Torsten: You can implement that, but I don't see how scope or authorization details are related to that. They relay the requirements of the client to the AS, not the requirements of the user.
- Justin: Agreeing with Torsten, this is orthogonal. you can solve this with or without scopes and RAR. RAR is not intended to be a way for the client to say "put these claims in a JWT", it's not meant to allow that type of direct editing. It's meant to be a multi-dimensional scope value. Ultimately it's up to the AS to decide what goes into an access token. RAR doesn't mention what should go into the access token itself.
- Denis: If I want to give control of the sub value then I should use the scope value as usual
- Justin: no that's not what I said
- Denis: Today the sub value is basically controlled by the scope and knowing what RS is being accessed
- Justin: You could implement that same magic with RAR if you wanted to. RAR is not going to define the interop of that magic.
- Denis: Since in the JWT profile we had text of the use of the sub values, it would be nice to have some mention of the sub value in this doc
- Justin: This document doesn't have anything to do with the sub value or contents of access tokens, that's what the JWT doc is for
- Takahiko: Did you mention grant management?
- Torsten: As part of FAPI 2, we are working on an API for clients to manage grants, "Grant Management". This also uses RAR. The RAR spec is already used in subsequent specs to make the content of a grant transparent to a client. Other specs are being built on RAR already.
- Rifaat: WGLC ended in June already, I'll get it moving

# Attendees

- Rifaat Shekh-Yusef/Auth0 (chair)
- Hannes Tschofenig/Arm (chair)
- Torsten Lodderstedt/yes.com (presenter)
- Jeff Craig/Google
- Aaron Parecki/Okta
- Peter Yee/AKAYLA
- Justin Richer (co-author)
- Roman Danyliw/CMU
- Filip Skokan (Auth0)
- Dick Hardt (Hellō)
- Denis Pinkas DP Security Consulting
- Vittorio Bertocci (Auth0/Okta)
- Brock Allen (Duende Software)
- Takahiko Kawasaki (Authlete)
- Kelley Burgin/MITRE

# Recording

For some reason, the recordong captured only the first 2 minutes of the meeintg. I might have pressed the wrong button when I stopped sharing. Sorry about that.