GNAP Interim Meeting

May 6, 2021

Notetaker: Aaron Parecki

Attendees

(Not listed)

Minutes

Draft update review

Updates since last meeting

25 pull requests merged
https://github.com/ietf-wg-gnap/gnap-core-protocol/pulls?q=is%3Aclosed+merged%3A2021-02-23..2021-05-07 (https://github.com/ietf-wg-gnap/gnap-core-protocol/pulls?q=is%3Aclosed+merged%3A2021-02-23..2021-05-07)

New draft 05

Major changes:

- crypto updates
- subject identifiers
- interaction concept pulled out to say it doesn't have to be done in oauth-way
- entire section on RS-AS pulled into a new spec
    - closer to the oauth model

Editorial changes:

- clarifying stuff and cleaning up examples
- more rationale discussion
- minor changes and typos

Fabien published a blog post about GNAP

https://blog.fimbault.com/managing-authorization-grants-beyond-oauth-2
(https://blog.fimbault.com/managing-authorization-grants-beyond-oauth-2)

Fabien:

Crypto Updates

- Aligns GNAP syntax with the latest draft of HTTP Message Signatures draft
  - OAuth group meeting about HTTP signatures next week
- DPoP “ath” claim integrated into GNAP
- JOSE “typ” header (gnap+jws) to identify this type of object
- JOSE body signing (#201) solves some of the problems we had with detached signatures
- Crypto examples have been updated to match the current spec

Subject Identifiers

- Based on feedback from IETF 110, now using the secevent draft -07
- Updated the examples, removed email from examples
- This aligns better with section 4, the new definition of the role of the AS
- Open questions: included DIDs? (#221) Assertions (ID tokens and SAML tokens)

Yaron: How are assertions related to subject identifiers?

Fabien: sub IDs are returned along with assertions in the same place, e.g. you’d receive an ID token along with the sub ID

Adrian: When the subject ID is a DID, there’s an opportunity to provide service endpoints

Fabien: Might need to work with secevent WG

Justin: It makes sense, but where should that work be done? Can GNAP allow these things without getting too prescriptive, and where is the right place to define the details? We have yet to see a concrete proposal of what this would look like on the wire.

Adrian will make a first pass at providing an example in #221.

Yaron: Do we have a strong dependency on DIDs going into the subject IDs draft?

Justin: If we take on any kind of DID based description of user info then we do.

Yaron: Does subject identifiers draft create a registry that we could extend later on?

Justin: Yes. The changes in -07 were helpful for how we are using it in GNAP.

Resource Servers

Justin

Resource servers pulled into a new draft from what was previously section 10. Not many functional changes, mainly reorganizing and extracting.

This draft has its own repository. Draft -00 has been published.

The editors' plan is to keep issues in their respective repositories. Client-AS in core, AS-RS in the resource servers draft.

If you don't know where to file an issue, drop it in the main repo and the editors can move the issues between the two as appropriate.

This also sets precedent for other extension work as it comes up.

Denis: The RS document is not dedicated to only AS-RS interaction, it covers also client-to-RS interaction.

Justin: The editors are not convinced the lines are drawn all at the right place, content may still move back and forth between the two as we figured out how to functionally separate these. The WG could in the future decide to combine these again, the charter does not dictate how many documents to publish, just what problems we address. There is one section that talks about the client talking to the RS, that was previously in section 10 which is why it was brought over but that could change.

Denis: I would prefer to keep the client-RS interaction in the core document.

Justin: Yes that is possible

Adrian: Congrats, the resource server doc stands alone well. It would be nice to have more description of the key material.

Justin: Great feedback.

Yaron: Some parts of the draft looked unbaked. Do the authors think it's good enough for a full read to start filing issues or would you like to publish a -01 before?

Justin: I think it's good enough with the caveat that the question of where to draw the line may not be right in the first draft, so questions are welcome.

AS and RS Relationship

(diagram)

Justin: There was a lot of discussion around the AS/RS discovery and negotiation, which we realized was separate from the discussion of how clients interact.

Justin: This is a similar split to UMA as well. There is precedent for this being a good split.

Denis: The token format between the AS and RS should be defined in the core document.

Justin: No. This has been previously discussed. This does not require preestablished relationships.

Yaron: If you have specific issues with trust relationships in the document please raise it on GitHub.

Adrian: Denis can I talk to you about this offline I can try to help.

Justin: The goal is to allow modularity between different parts of the protocol. There are decisions that happen on one side of this line that shouldn't affect parties on the other side of the line. This allows for example a token format to be negotiated between the AS and RS when there is no prior relationship while the token format is still opaque to the client for preserving privacy.

AS Determining Authorization and Consent

Justin: We realized there was a lot of language that accidentally assumed the AS was directly interacting with the user. e.g. "interaction at the AS". This wasn't the intent, and nothing actually needs this to be true, it was mainly a holdover from OAuth. With this rewrite, the AS now has clearly spelled out ways to interact with the user that aren't necessarily in a browser.

(diagram, slide 12)

The language assume the AS was one block

(diagram, slide 13)

The language now says you use an "interaction method" that is out of scope of GNAP. The ability to have something that isn't a web page to collect authorization is now explicitly

called out.

(diagram, slide 14)

Adrian has a great use case for collecting consent from multiple parties. Now, GNAP doesn't define what goes into these orange arrows so that other specs can define it as extensions. Architecturally, GNAP isn't solving those arrows in one single way. GNAP does say that wherever the client instance gets involved, it may be able to say it can facilitate these interactions.

This was always hiding in the protocol structure before, especially because you can already do it with OAuth even if it's not explicit, so this rewrite makes this explicit so you know it's possible. e.g. go get claims from my wallet, the client may be able to faciliate that, then some other protocol might be used to push that to the AS.

Yaron: Shouldn't we call out the question mark components explicitly and give them names?

Justin: We have an issue for that. Could be "interaction server" or "interaction component".

Yaron: It's not a good idea to allude to the idea that two things are different functional components if we want people to implement them separately.

Justin: That was a big part of section 4, carving it into those blocks, but we haven't yet given them names.

Going Forward

Justin: With the last set of changes, the core is reasonably stable. With the large changes in -05 things are settling down. We need to start implementing. There are people outside the WG who are following the work as well.

This is definitely not ready for WG last call, but we're getting to a turning point of stability of the core.

Yaron: We have an RFC on the implementation status section, this is a good time to add this section to the draft. We need to see the RS draft maturing before last call. Would like to see an actual security analysis. Daniel Fett mentioned he might want to, don't know if this is the right time.

Justin: Sounds good to me.

Next Topics

Justin: There are some questions around key rotation and token rotation that will affect the security of the core protocol.

Justin: With the big crypto rewrite, which methods should remain in the core and which should be pulled out as extensions? Fabien started a discussion (#244) on the access request internals.

Justin: We would like another interim in mid-June.