OAuth WG Interim Meeting

Date

October 6, 2021, 12:00pm EDT

Topic - OAuth PoP Tokens with HTTP Message Signature

Presenters: Justin Richer
Draft: HTTP Signature
Slides: HTTP Signature slides

Notes

Note taker: **Dick Hardt**

Rifaat started off meeting and congradulated authors of RFC 9101 and 9126; and noted the upcoming schedule of interim meetings:

- OAuth 2.1 - October 13
- RAR - October 20
- DPoP - October 27

Justin presented his slides https://datatracker.ietf.org/meeting/interim-2021-oauth-11/materials/slides-interim-2021-oauth-11-sessa-http-message-signatures-00.pdf

Justin: questions so far on HTTP Signing?
Rifaat: You can have multiple signatures. Use case?
Justin: Allow intermediary to validate signature, and add their own signatures, and downstream can trust signatures it needs. Different signers can sign different components. See doc for more use cases.
Justin mentioned another use case where one signture is computed using one algorithm and a second signature using a different algorithm.
Yet another use case is to have an intermediary sign the signature as well as a different part of the message.

Justin: how do we take this and apply it to OAuth 2.0

Rifaat: questions on technical proposal? (silence)
Justin: Is it clear what the draft is solving and why it is solving it?

Jeff Craig: Who would be implementing this?
Justin: I see HTTP Sig being used in a lot of related spaces. Makes sense for OAuth to make use of the same mechanisms. Covers use cases that DPoP was not designed to cover. FAPI is extending DPoP in HTTP Sig like ways.
I'm concerned we will see unintentional complexity, which comes with unintentional security issues. Let's take the slightly more complex thing where the parameters are better understood.
Jeff Craig: ??? (was trying to figure out who was talking)
Justin: expires is currently optional, opinion of signer how good the signature is good for. HTTP Sig takes a soft stance on what the expires means.
Denis Pinkas: what is missing is details on user mechanism – need to know before we can make a decision.
Justin: clarify?
Denis: how do you know from how the signatures are coming from.
Justin: signed by the client. This is an example of where the OAuth WG would want to specify more clarity. For example, the OAuth extension could require the client ID as a parameter. Has nothing to do with the user.
Aaron Parecki: Where would the key id come from? An implementation, or would be in the OAuth draft?
Justin: FANTASTIC question. IMO, this is something that the OAuth draft would be very specific about. Lots of debate could happen on this. Specifically because the HTTP draft does not have an opinion on this. OAuth draft would be the application, and is where we would have specifics.
Hannes: You have been vocal about all the different specifications we have, how do we explain which ones they should use?
Justin: First saw DPoP, thought it was general purpose, then realized it was a narrow solution. Not living in a world where presregistered keys make sense. Deploy DPoP where they are doing SPAs and JOSE stuff. DPoP is a good fit. Instead of trying to stretch DPoP to fit those, use HTTP Sig.
Denis: currently there are sections that are empty. Eg, the client could use the same key for all RS. RS could correlate client. There are missing sections.
Justin: it is a 00 draft. Lots left to do, and completing those sections is TBD. Some of those will be covered by the HTTP Sig draft, which Justin and Annabelle are working on. Will benefit from importing all the considerations from the HTTP Sig draft.
Filip: DPoP did not make sense until key was there all the time. For any scheme that it is not DPoP like, how does AS and RS. Would it be possible for a DPoP like

feature.
Justin: we have thought of having features in HTTP Sig. Be aware of security implications of having key by value. ??
Filip: asking for clarification on key
Justin: … managing key resolution is TBD
Brian: DPoP origin story is in SPA, it is not limited to SPA. It was driven by non-repudiation requirements. Driven by lack of HTTP Sig. I think that key distribution needs to be outlined, because that is one of the areas that are challenging. One of the issues of DPoP is the asymetric signatures on each request, and they may be one of the same issues with HTTP Sig and OAuth.
Justin: not trying to dis DPoP. Woke up WG to have POP tokens. DPoP not a good fit for some use cases. A deterministic protocol. Key management systems do exist that could be used. We need to answer these key management and communication issues.

Rifaat: I will take this to the list to ask for adoption.

Meeting ended.

Attendees

- Rifaat Shekh-Yusef (chair)
- Hannes Tschofenig (chair)
- Justin Richer (presenter)
- Aaron Parecki
- Dick Hardt
- Roman Danyliw
- Carsten Bormann
- Brian Campbell
- Filip Skokan
- Marie-Hélène Bouchard
- Janak Amarasena
- Vittorio Bertocci
- Bjorn Hjelm
- Chamath Samarawickrama
- Denis Pinkas

- Dmitry Telegin
- Takahiko Kawasaki
- Dominick Baier
- Janak Amarasena
- Jeff Craig
- Karsten Meyer zu Selhausen
- Marius Ciocan
- Sergey Puzin
- Torsten Lodderstedt
- Meysam

Recording

Sorry, forgot to record the meeting.