OAuth WG Interim Meeting - DPoP

Date

November 30th, 2020

Notes

Note taker: Dick Hardt

Brian reviewed what DPoP is with meeting slides

Open issues

Freshness & Signature Coverage

Dick: explained JWT binding token proposal posted on list that binds access token to client's key
Brian: does not see requirement to have binding be a separate layer – easy to modify the access token
Filip: Is Dick's proposal allowing for the RS to detect a given token is actually DPoP bound?
Brian: No it isn't. There's no way to have simulatenous support for bearer and dpop. It's a deficiency.
Filip: Agreed. A big one, we discussed at length in the past that a "hybrid" approach is important for a frictionless rollout of dpop into existing ecosystems.
Mike: is there progress on using symmetric keys?
Brian: yes – but using symmetric keys is a different protocol
Dave: Is the hash not included because of size?
Brian: The protocol is fairly clean and symmetric currently. Perhaps doing the access token and only access token may be a good compromise.
Dave: adding a binding to the access token in the DPoP proof could prevent some attacks.
Brian: Perhaps.
Denis: The MUST in the security considerations should be in the text of the document. The expiry of the DPoP proof??? (DH: I was not sure Denis' point)
Brian: I don't see how that is relavent. Unclear what Denis issue is.
Justin: We should keep in mind that "this is sufficiently okay"; we can address issues by

pointing them out as known shortcomings to be avoided
Rifaat: Is any against staying the way the draft is?
Brian: I will summarize the options and post to the list.

Confirmation Bias

Brian: reviewed slide
Justin: there are lots of other similar issues where the client may not perform all of is checks.
Daniel: valid point – but by making specification very explicit on what to check and the proper order an implementation should be ablet to avoid these issues
Brian: I will take this issue to the list and provide the choices.

Does the World need a new OAuth client to AS Authentication method?

Brian: reviewed slide.
Rifaat: out of time. Please take all three of these issues to the list.
Brian: will take to list.

Attendees

- Rifaat Shekh-Yusef
- Hannes Tschofenig
- Justin Richer
- Dick Hardt
- Mike Jones
- Aaron Parecki
- Daniel Fett
- Brian Campbell
- Nikos Fotiou
- Vittorio Bertocci
- Dave Tonge
- Peter Yee
- Filip Skokan
- Tim Cappalli
- Janak Amarasena
- Phil Hunt
- George Fletcher
- Cristofer Gonzales

Documents

https://datatracker.ietf.org/doc/draft-ietf-oauth-dpop/ (https://datatracker.ietf.org/doc/draft-ietf-oauth-dpop/)

Recording

https://ietf.webex.com/recordingservice/sites/ietf/recording/d1e9ae1c7d90475f8816d998bc31f15f/playback (https://ietf.webex.com/recordingservice/sites/ietf/recording/d1e9ae1c7d90475f8816d998bc31f15f/playback)