OAuth WG Interim Meeting

Date

October 13, 2021, 12:00pm EDT

Topic - OAuth 2.1

Presenters: Aaron Parecki
Draft: OAuth 2.1 (https://datatracker.ietf.org/doc/draft-ietf-oauth-v2-1/)
Slides: OAuth 2.1 slides (https://datatracker.ietf.org/meeting/interim-2021-oauth-12/materials/slides-interim-2021-oauth-12-sessa-oauth-21-00)

Notes

Note taker: Hannes Tschofenig & Dick Hardt
Rifaat presented upcoming meetings and discussed process
Aaron presented OAUth 2.1 slides. He explained the changes to the draft (slide 2) and planned changes on slide 3.

Issues for discussion:

- Removal of the implicit grant
  Aaron motivated the removal with new text. Vittorio and Justin think it is a good change. Brian said “do it do it”.

- iss response parameter
  Aaron suggested to add a requirement for the iss response parameter to OAuth 2.1 since it helps to defend against AS mixup attacks.

Mike objects against the change because he believes this change extends what the document was chartered to do.

Aaron resonds that he made this change because it is in the Security BCP.

Dick: OAuth 2.1 was not just a sub-set but rather the best current practice. I don’t think it adds more functionality but additional security.

Mike is concerned that there are no OAuth deployments doing this functionality.

Janak Amarasena: How does disallowing tokens from authorization ep affect the OIDC Hybrid flow?

Brian Campbell: we've added PKCE...

Justin Richer: @Janak: OIDC Hybrid is not OAuth 2.1, then.
(It's still 2.0 though)

Karsten Meyer zu Selhausen: +1 for adding iss to 2.1 (obviously as one of the iss draft authors)

Justin: Authlete ships with this feature (iss) today.

Torsten says that there are deployments using this functionality.

The work on 2.1 was supposed to incorporate BCP. If we don't do that, where else would we add it. PKCE is also added.

Mike: PKCE is a completed RFC but the Security BCP is still a draft.

Rifaat: We are going to ship the security BCP any day now. Does this help?

Mike: It does not help a lot.

?: I agree that this is very similar to the PKCE case.

Mike: I am worried about the "feature creap"

Dick: I appreciate that you want us to avoid "feature creap".

Aaron: This is not required for every OAuth deployment.

Mike: What is the language proposed?

Aaron: It is described in the "iss" spec. It is relevant about the multiple AS deployments.

Karsten Meyer zu Selhausen: Current implementations for iss parameter:

- Duende Software: https://duendesoftware.com/products/identityserver (https://duendesoftware.com/products/identityserver)
- Authlete: https://www.authlete.com/developers/relnotes/2.2.2/#oauth-2-0-authorization-server-issuer-identifier-in-authorization-response (https://www.authlete.com/developers/relnotes/2.2.2/#oauth-2-0-authorization-server-issuer-identifier-in-authorization-response)
- Authress: https://authress.io/ (https://authress.io/)

- OIDF Conformance Suite: https://www.certification.openid.net/login.html (https://www.certification.openid.net/login.html)

Justin: We are coming back to the issue of “if you are solving problem X in an alternative way then X”. We are spending a lot of time discussing the work-arounds of OpenID Connect instead of focusing on the foundational technology

So, OpenID Connect 1.0 may not be OAuth 2.1 compliant and that’s OK.

Farasath Ahamed: Isn’t naming this 2.1 a bit confusing in terms of the usual versioning terminology :)

Aaron: I think it is useful to backport many of the solutions into the core so that other solutions besides OpenID Connect also benefit from it.

Justin: Agree w/Aaron. I contributed a number of backports to do exactly this issue.

Aaron: consensus is to hold the ‘iss’ feature until the iss draft is an RFC

- Require HTTPS redirect URLs

Brian and Justin agree.

- Drop complex authorization code replay mitigations in favor of PKCE

Proposal is to remove solutions #65, #82, and #54 in favor of PKCE since PKCE offers a solution.

Filip: Does it probit ASes from enforcing the other solutions?

Aaron: No, you can still implement the other techniques.

Brian: I agree with removing the redirect_uri (which is redundant). This is a compatibility-breaking change.

Dick Hardt: That it is not a breaking change. The AS may require it and if the AS requires it then it must send it.

Brian: I am not sure how to do it without breaking it.
An implementation may be make the check dependent on other parameters.

Dick: The checking on the AS was the hard part. It seems easy for the client.

Brian + Torsten: It is also difficult for the client.

Dick: It is implemented today.

Justin Richer: it’s harder for the client in practice

Torsten: We already have the breaking changes due to PKCE.

Justin: Our notion of breaking and non-breaking changes is important. We need to look at what happens when a 2.1 client talks to a 2.0 server. What changes are fine and which onces are not fine. We need to understand what we accept and what
not.

Hannes talking about the notion of minor and major versions. Will check whether there is some IETF guidance.

Justin pointed to an expired draft: https://tools.ietf.org/id/draft-claise-semver-00.html (https://tools.ietf.org/id/draft-claise-semver-00.html)

Brian mentioned the TLS 1.x example.

Vittorio: Developers have an expectation about semantic versioning, whether that’s enshrined in IETF or otherwise

Aaron: redirect_uris are not allows required, and so not all clients send it, but some AS do require it.

Brian: this is a potentially a break, and we should call it out.

Aaron: agreed

Dick: Maybe we should have a section about what is different from 2.0 and what is a breaking change.

Justin: Also note who it is breaking for. What changes are needed for clients vs servers.

Brian: eg. PKCE requirements are an area where which versions work with which versions

Aaron: seems like these are good changes and have them well documented as to the impacts

Hannes: TLS has version negotiation so that the client and server can align on the version to use. The OAuth case is slightly different.

Dick: today we have clients and servers that are 2.0 but have PKCE. With 2.1, the clients and servers can be 2.1 and know that PKCE is implemented.

Aaron: we have a number of smaller items on the list, including the definition of client types that has been discussed on the mailling list

Hannes: when would be a likely completion date? Q1 20222?

Aaron: that seems fair, and at next interim will have a small list of what is remaining

Vittorio: an area of my feedback is the difference between native and mobile clients. I was expecting some discussion on those sections.

Aaron: section 8 and above are still being worked on. We have done simple and non-confrontational changes, we have done it. We will get to Vittorio's discussion points when we get to section 8.

Rifaat: any other comments questions?

Rifaat: end meeting.

Attendees

- Rifaat Shekh-Yusef/Auth0 (chair)
- Hannes Tschofenig/Arm (chair)
- Aaron Parecki/Okta (Presenter)
- Dick Hardt (Hellō)
- Justin Richer
- Filip Skokan (Auth0)
- Vittorio Bertocci (Auth0 | Okta)
- Marie-Helene Bouchard (Government of Canada 🇨🇦)
- Karsten Meyer zu Selhausen
- Marius Ciocan
- Brian Campbell (Ping)
- Denis Pinkas (DP Security Consulting)
- Dmitry Telegin
- Mike Jones (Microsoft)
- Torsten Lodderstedt (yes)
- Brock Allen
- Dave Robin
- Janak Amarasena (WSO2)
- Farasath Ahamed (WSO2)
- Torsten Lodderstedt (yes.com (http://yes.com))
- Tony Nadalin (Microsoft)
- Pieter Kasselman

- Takahiko Kawasaki
-

Recording

https://ietf.webex.com/webappng/sites/ietf/recording/44fc7b220e6d103aafff0050568ced19/playback (https://ietf.webex.com/webappng/sites/ietf/recording/44fc7b220e6d103aafff0050568ced19/playback)