OAuth 2.1

IETF 113 • Vienna • March, 2022

`draft -05`

Aaron Parecki, Dick Hardt, Torsten Lodderstedt

Changes Since draft -04

- TLS is mandatory for redirect URI except loopbacks (Thanks Roberto)
- Reorganized and consolidated TLS language (Thanks Roberto)
- Editorial clarifications based on feedback and PRs
  - Updated more references to new RFCs
  - Lots more! Thanks Justin and Vittorio!
- Moved more normative text from security considerations inline in the main document
- Updated refresh token guidance to match Security BCP
- Added section explicitly mentioning the removal of the Implicit flow

https://github.com/aaronpk/oauth-v2-1/compare/draft-04...draft-05

Planned Changes for -06

- #70 Finish incorporating feedback from Justin and Vittorio (Sections 8-13)
- #64 Finish moving normative language from security considerations inline in the doc
- #97 Expand the differences from OAuth 2.0 to include for which roles each change is a breaking change

Still more open issues to discuss, some of this will be best on the mailing list rather than synchronously here.

https://github.com/aaronpk/oauth-v2-1/issues

Issues for Discussion

#46 `iss` response parameter

The Security BCP recommends the use of the `iss` response parameter to defend against AS mixup attacks.

We previously discussed this in October 2021, the consensus was to revisit this topic once the `iss` draft is an RFC.

The draft was published as RFC 9207 in March 2022. Time to revisit the discussion!

Proposal: Incorporate RFC 9207. Note this only applies to clients that support multiple ASs in a particular deployment, so many clients will not need changes.

#101 Bearer tokens are required to expire

Currently OAuth 2.0 Bearer Tokens RFC 6750 requires (in the security considerations) that bearer tokens have a limited lifetime, prohibiting unlimited length bearer tokens.

> To deal with token capture and replay, the following recommendations are made: First, the lifetime of the token MUST be limited; one means of achieving this is by putting a validity time field inside the protected part of the token. Note that using short-lived (one hour or less) tokens reduces the impact of them being leaked. Second, confidentiality protection of the exchanges between the client and

This doesn't match the reality of many deployments today.

Should we relax this to a SHOULD? Rephrase "lifetime" to encompass other criteria?

#106 AS requirement to support 3 redirect URI methods

From the Native Apps BCP, incorporated into OAuth 2.1:

> To fully support native apps, authorization servers MUST offer at least the three redirect URI options described in the following subsections to native apps. Native apps MAY use whichever redirect option suits their needs best, taking into account platform-specific implementation details.

- Private URI Scheme
- Claimed https URL
- Loopback Interface

Should this remain a MUST or be relaxed to allow profiles like FAPI to prohibit private URI schemes?

Future Work

https://github.com/aaronpk/oauth-v2-1/issues