OAuth 2.1

Interim Meeting • March 22, 2021

Aaron Parecki, Dick Hardt, Torsten Lodderstedt

Changes Since draft -00

- Updated terminology and references to obsoleted specs
  - RFC2616 -> RFC7231
  - RFC2617 -> RFC7235
- Editorial clarifications based on Justin and Vittorio's feedback
  - "Token" -> "Access token"
  - Authorization code definition
  - Reinforce authorization code and access token opaqueness to clients
  - "Client password" -> "Client secret"
  - https://mailarchive.ietf.org/arch/msg/oauth/t5y7AhnICFazpCTEH6wZuy6W_KM/
  - Lots more! Thanks Justin and Vittorio!
- Comments from Justin and Vittorio that were not yet addressed are opened as GitHub issues
  - https://github.com/aaronpk/oauth-v2-1/issues

Planned Changes

- #70 Incorporate editorial feedback from Justin and Vittorio (Sections 7-13)
- #61 Rearrange section 4 to be about all token endpoint requests rather than “obtaining authorization”
  - Including authorization code, refresh token, client credentials
- #65 Find out if relaxing the single-use requirement of authorization codes is safe if using PKCE
- #64 Move normative language from security considerations inline in the doc

Issues for Discussion

#46 `iss` response parameter

- The Security BCP will be recommending the use of the `iss` response parameter to defend against AS mixup attacks
- We should consider adding this to OAuth 2.1 despite it being a relatively late addition to the Security BCP
- Rationale: Add a solid and simple mix-up prevention to OAuth 2.1 for clients interacting with multiple ASs

#45 Referencing OpenID Connect Implicit Flows

- What is the most appropriate way to refer to OpenID Connect's additional response types in the security considerations?
  - No mention
  - State that deprecation of response_type "token" does not directly deprecate other extension types outside of the draft but responsible bodies should revisit
  - Explicitly prohibit any `response_type` containing `token`
  - Explicitly allow a `response_type` containing `id_token` providing that the ID token is not used as an access token
  - Encourage OpenID to officially deprecate response types containing `token`

#48 Protocol flow diagram

1.2. Protocol Flow

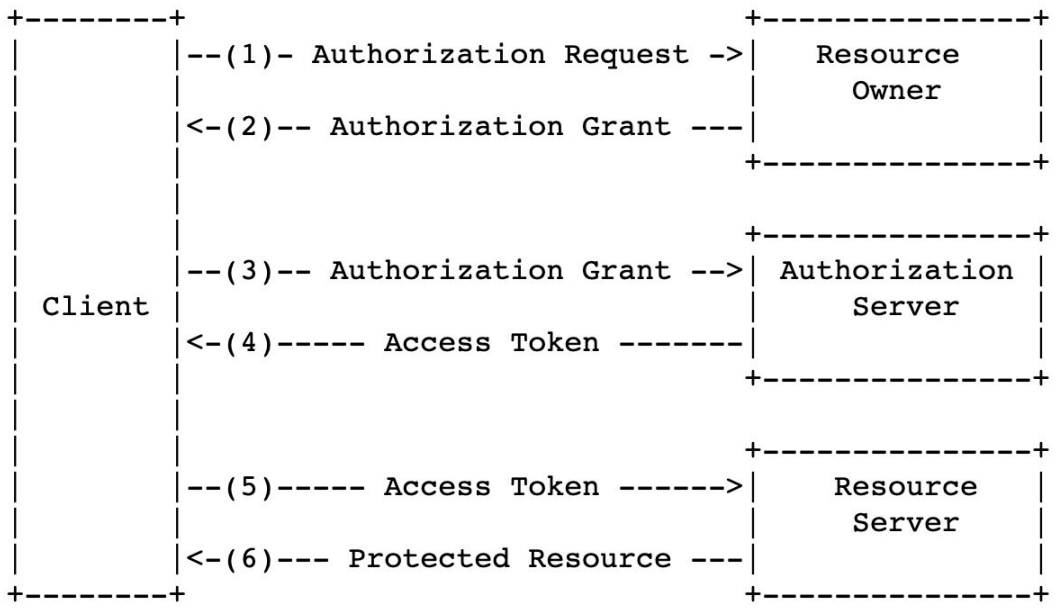

Figure 1: Abstract Protocol Flow