OAuth 2.1

https://tools.ietf.org/html/draft-parecki-oauth-v2-1-02

Aaron Parecki
IETF 107 • Virtual Meeting
April 27, 2020
OAuth 2.1 Summary

Authors: Dick Hardt, Aaron Parecki, Torsten Lodderstedt

- OAuth 2.1 is a consolidation of:
  - OAuth 2.0 (RFC6749), Native Apps BCP (RFC8252), PKCE (RFC7636), Browser-Based Apps BCP (draft), Security BCP (draft), Bearer Tokens (RFC6750)

- Grant types defined: Authorization Code with PKCE, Client Credentials

- Exact redirect URI matching

- No Bearer tokens in query strings

- Refresh tokens must be sender-constrained or one-time use

- Implicit and password grants are omitted
Changes Since -01

- Added HTTP 307 redirect section from Security BCP into OAuth 2.1
- Editorial and typo fixes
- Updated references to other specs such as HTTP
Open Questions

• Should we reference Dynamic Client Registration and AS Metadata as optional methods for registration and discovery respectively?

• Should TLS be required on redirect URIs? (except for localhost and non-HTTP redirect URIs)
Confidential Clients

Authorization servers SHOULD consider the level of confidence in a client’s identity when deciding whether they allow such a client access to more critical functions, such as the client credentials grant type.

- The client credentials example possibly conflicts with the section 4.2 statement “The client credentials grant MUST only be used by confidential clients” and the statement earlier in section 2.1 “Clients requiring a higher level of confidence...use credentials to authenticate with the authorization server.”

- What is the intended definition of confidential clients?

- Client identity assurance vs ability for a client to authenticate?
What's next?

- Some editorial work is still needed
- Adopt as a WG draft?