OAuth 2.1

https://tools.ietf.org/html/draft-ietf-oauth-v2-1-00

Dick Hardt, Aaron Parecki, Torsten Lodderstedt

Interim Meeting
August 3, 2020

OAuth 2.1

Consolidate the OAuth 2.0 specs,
adding best practices,
removing deprecated features

Capture current best practices in OAuth 2.0
under a single name

Add references to extensions that didn't
exist when OAuth 2.0 was published

OAuth 2.1

No new features defined by OAuth 2.1

Don't include anything experimental,
in progress or not widely implemented

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

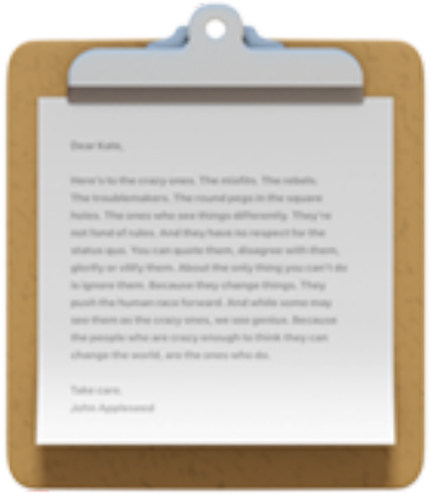
- No Bearer tokens in query strings

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

- Implicit and password grants are omitted

OAuth 2.1 Client Types

Public



Credentialed

Confidential

Credentialed Client

- A client that has credentials, but whose identity is not confirmed
- e.g. a client that obtains a client secret via dynamic client registration

What's next?

- Some editorial work is still needed
- Add examples of credentialed clients
- Collect WG feedback