OAuth 2.1

Aaron Parecki
IETF 106 · Singapore
November 20, 2019
Current State of OAuth 2.0

RFC6749
- Authorization Code
- Implicit
- Password
- Client Credentials
Current State of OAuth 2.0

- Authorization Code
- Implicit
- Password
- Client Credentials
Current State of OAuth 2.0

- Authorization Code
- Implicit
- Password
- Client Credentials

RFC6749

RFC7636
PKCE

RFC8252
PKCE for mobile
Current State of OAuth 2.0

- Authorization Code
- Implicit
- Password
- Client Credentials
- Device Grant

RFC 6749

PKCE

RFC 7636

PKCE for mobile

RFC 8626

RFC 8252
Current State of OAuth 2.0

- Authorization Code
- Implicit
- Password
- Client Credentials
- Device Grant

RFC6749

- PKCE

RFC7636

- PKCE for SPAs

RFC8252

- PKCE for mobile

RFC8626

- Browser App BCP
Current State of OAuth 2.0

- Authorization Code (RFC6749)
- Password
- Client Credentials
- Device Grant (RFC8626)

Security BCP

PKCE

- RFC7636
- PKCE for confidential clients
- PKCE for SPAs
- PKCE for mobile (RFC8252)
- Browser App BCP

PKCE for mobile
OAuth 2.1

- Authorization Code + PKCE
- Client Credentials
- Device Grant
OAuth 2.1

Capture current best practices in OAuth 2.0 under a single name
Non-Goals:

No new behavior defined by OAuth 2.1

Don't include anything experimental, in progress or not widely implemented
OAuth 2.1

RFC6749 - OAuth 2.0 Core

Security BCP
- MUST support PKCE for all client types
- No password grant
- No implicit flow

Bring the device grant into 2.1

Native App & Browser-Based App BCPs

Token Revocation

Authorization Server Metadata
OAuth 2.1

Additional requirements on authorization servers that intend to interoperate with arbitrary resource servers

- Token Introspection
- JWT Access Tokens
- JWT BCP
OAuth 2.1

Let's work on this now!

Side Meeting

Wednesday 3:00-5:00pm
Butterworth Room