OAuth 2.0 for Browser-Based Apps

draft-ietf-oauth-browser-based-apps-04

Aaron Parecki

IETF 106 • Singapore
November 20, 2019

OAuth 2.0 for Browser Based Apps

- Includes recommendations for implementors building browser-based apps using OAuth 2.0

- "Browser-based apps" are defined as applications running in a browser, aka "SPA" or "single-page apps"

OAuth 2.0 for Browser Based Apps

- **MUST** use the OAuth 2.0 authorization code flow with the PKCE extension
- **MUST NOT** return access tokens in the front channel (e.g. no Implicit flow)
- **MUST** use the OAuth 2.0 state parameter to carry one-time use CSRF tokens
- The AS **MUST** require an exact match of the redirect URI

What's New Since IETF105?

- Updates to bring this in line with the Security BCP
- Disallow the password grant even for first-party applications
- Allow refresh tokens in SPAs as long as they conform to Security BCP
- Editorial clarifications

Open Questions

State parameter

- Should "state" be used for CSRF protection even if PKCE is used?
- Should we mention the possibility of static "state" values if the client knows PKCE is available?

Open Questions

Refresh Tokens

- Should we make a recommendation on how to silently refresh tokens in a browser such as using a hidden iframe like OIDC?

Content Security Policy

- Should we mention specific recommendations for a strong CSP? e.g. disable inline scripts?