OAuth 2.0 for Browser-Based Apps
(Best Current Practice)


draft-14
OAuth 2.0 for Browser Based Apps

- Includes recommendations for implementers building browser-based apps using OAuth 2.0
- "Browser-based apps" are defined as applications executing in a browser, aka "SPA" or "single-page apps", and may include a backend component
Changes from -13 to -14

● Minor editorial changes
● Updated references
● Added a paragraph noting the possible exfiltration of a non-exportable key from the filesystem
Open Issues

- None!
OAuth 2.1

https://datatracker.ietf.org/doc/draft-ietf-oauth-v2-1/draft-09
Changes from draft-08 and IETF 117 Discussion

- Revised introduction
- Updated references
- Synced recent changes from the Security BCP into 2.1
  - MUST NOT support CORS requests at authorization endpoint
  - CSRF description
  - Client impersonating resource owner
  - Refresh token rotation
  - Redirect URI matching
  - Updates to sender-constrained access token section
- Removed “redirect_uri” from token request (from last IETF discussion)
Planned Changes for -10

- #64 Finish moving normative language from security considerations inline in the doc
- #97 Expand the differences from OAuth 2.0 to include for which roles each change is a breaking change
- #128 Describe application/x-www-form-urlencoded

Still a few more open issues

https://github.com/oauth-wg/oauth-v2-1/issues
Timeline

- **Bring Security BCP to IESG**
  - Finish syncing all Security BCP changes into OAuth 2.1
- **Browser BCP WGLC**
  - Add references to Browser BCP in OAuth 2.1 where appropriate
- **Ask for preliminary review from HTTP WG?**
- **OAuth 2.1 WGLC**