

Changes from IETF 113 Discussion

- #123 Removed "credentialed client" term
- #107 #102 #42 #41 #34 #33 Simplified definition of "confidential" and "public" clients and related changes
- #46 Incorporated the iss response parameter referencing RFC9207
- #101 Added section on access token validation by the RS, removed "lifetime... MUST be limited" in favor of further discussion in security considerations
- #106 Removed requirement for authorization servers to support all 3 methods of private URI schemes, loopback interface, and https URIs for native apps

OAuth 2.1

More Changes Since draft -05 (Vienna)

- Fixes for some references (Thanks Falko)
- Updates HTTP references to RFC 9110, removes unused refs (Thanks Roberto)
- Updates reference for application/x-www-form-urlencoded to WHATWG URL
- #29 Clarifies "authorization grant"
- #27 Clarifies client credential grant
- #55 Clean up authorization code diagram

Diff: https://github.com/aaronpk/oauth-v2-1/compare/draft-05...draft-06

Issues: https://github.com/aaronpk/oauth-v2-1/milestone/4?closed=1

OAuth 2.1

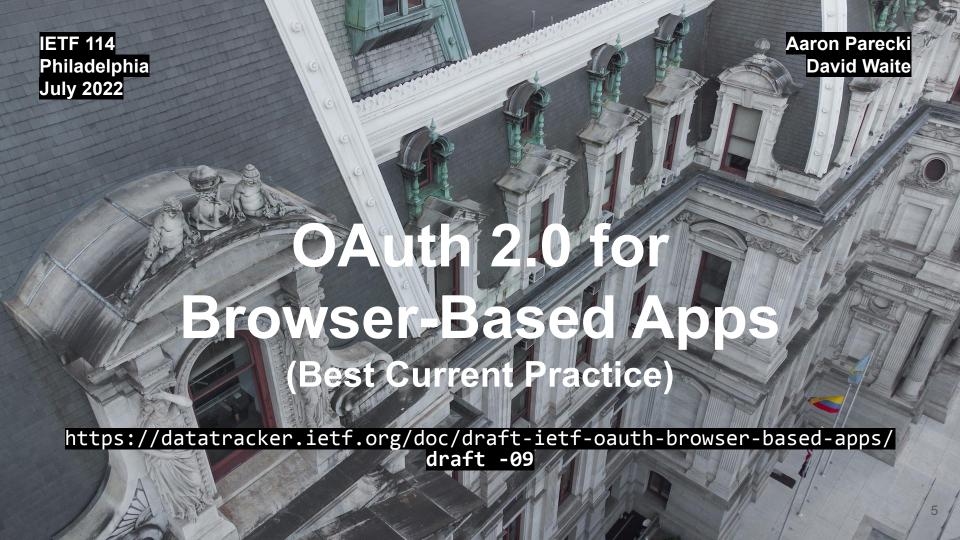
Planned Changes for -07

- #70 Finish incorporating feedback from Justin and Vittorio (Security considerations, native apps)
- #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

Still more open issues to discuss!

https://github.com/aaronpk/oauth-v2-1/issues

OAuth 2.1



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"

Last presented draft -06 in April 2020

Changes from -06 to -09

- Clarified PKCE requirement applies only to issuing access tokens
- Added reference to new "iss" parameter recommendation
- Added additional context for same-domain architecture pattern
- Updated to May 2021 recommendations from Security BCP
- Editorial fixes and improvements

In-Progress Changes

- Adding the Service Worker pattern as another option
 - https://github.com/aaronpk/oauth-browser-based-apps/pull/13 (Thanks Yannick!)

Planned Changes

- Add a section with recommendations and considerations for storing tokens
 - e.g. storing tokens in memory vs in LocalStorage
- Review recent changes to the Security BCP to ensure this draft is consistent