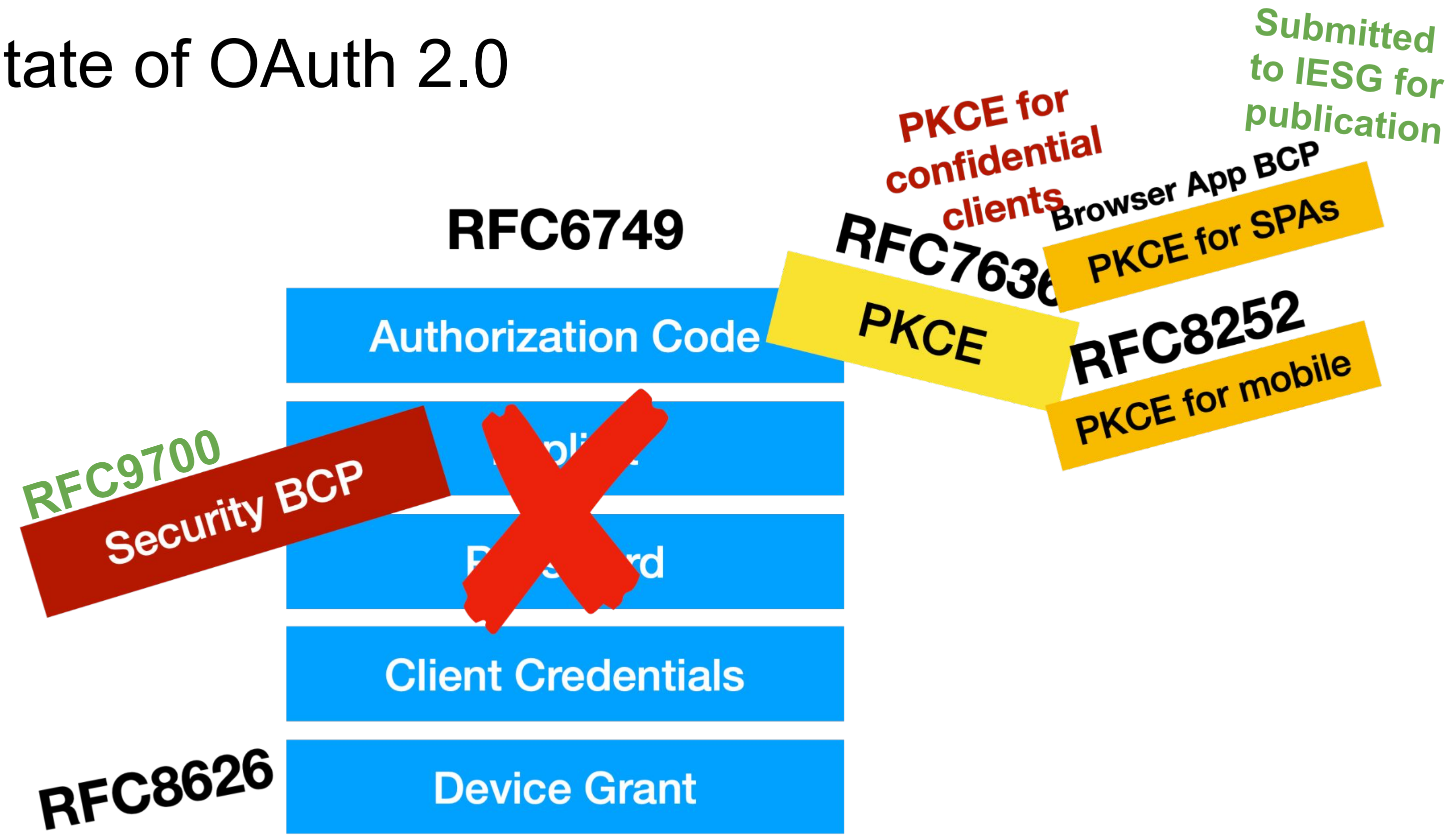
IETF 122
Bangkok
March 2025

Aaron Parecki
Dick Hardt
Torsten Lodderstedt

OAuth 2.1

https://datatracker.ietf.org/doc/draft-ietf-oauth-v2-1/
draft -12

Current State of OAuth 2.0



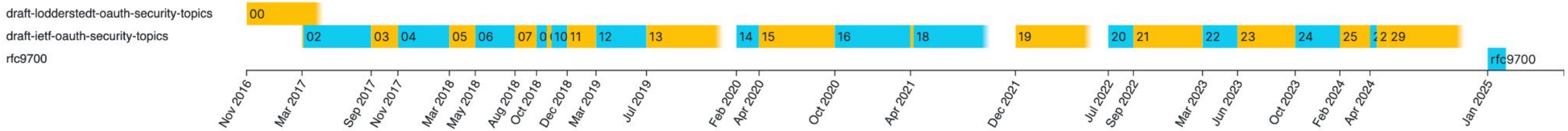
Goals

- Capture current best practices in a single name
  - RFC6749 + RFC6750
  - RFC7636 (PKCE)
  - RFC8252 (Native Apps BCP)
  - RFC9207 (iss response parameter)
  - RFC9700 (Security BCP)
  - Browser Apps BCP - *Submitted to IESG for Publication*
- No new behavior defined by OAuth 2.1

Best Current Practice for OAuth 2.0 Security

RFC 9700 also known as [BCP 240]

Status | Email expansions | History



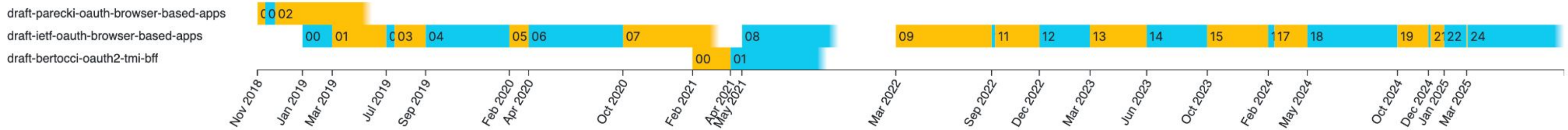
OAuth 2.0 for Browser-Based Applications

draft-ietf-oauth-browser-based-apps-24

Status | IESG evaluation record | IESG writeups | Email expansions | History

Versions:

00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24



Browser Apps BCP

Lots of editorial updates from last call reviews!

-24

- Updated terminology definitions
- Fixed typos
- Updated acknowledgements

-23

- Ensure acronyms and other specifications are defined and referenced on first use, and added to terminology
- Clarified malicious JavaScript is the basis of the threat analysis earlier in the document
- Clarified why filesystem storage of private key is a concern
- Clarified JS runtimes in intro
- Addressed feedback from secdir review
- Clarified that the specific attacks described are the relevant ones for this document because they are OAuth-specific
- Described the relationship to session fixation attacks
- Clarified that section 8 is talking about OAuth tokens specifically
- Mentioned that localStorage is synchronous
- Applied suggestions about scope of malicious JS code from Martin Thompson's review
- Clarified "attacking the service worker" to be explicit that this is about the authorization code flow
- Clarified the intent of storing the refresh token in a web worker
- Mention explicitly access token and refresh token instead of "set of tokens" on first use per section
- Slightly rephrased Web Worker section to not sound like a recommendation
- Editorial edits to remove the phrase "perfect storage mechanism"
- Fixed references
- Addressed all feedback from the genart, opsdir, artart, secdir, and httpdir reviews

-22

- Addressed AD review
- Moved RFC6819 reference to informal
- Added missing references from prose
- Replaced references to living standards with references to snapshots

On the agenda for the April 24 IESG telechat

https://datatracker.ietf.org/doc/draft-ietf-oauth-browser-based-apps/

Changes since draft -11

- Added DPoP and Step-Up Auth to appendix of extensions
- Updated language around client registration to better reflect alternative registration methods such as those in use by OpenID Federation and open ecosystems
- Moved `client_id` requirement to the individual grant types
- Consolidated the descriptions of serialization methods to the appendix

Changes since draft -11

- Added DPoP and Step-Up Auth to appendix of extensions
- Updated language around client registration to better reflect alternative registration methods such as those in use by OpenID Federation and open ecosystems
- Moved `client_id` requirement to the individual grant types
- Consolidated the descriptions of serialization methods to the appendix
- Added **`bEaReR`** as an example of case-insensitivity

Open Issues

https://github.com/oauth-wg/oauth-v2-1/issues?q=is%3Aissue+is%3Aopen

Most have been discussed either in the thread or during past meetings.

HTTP / TLS Requirement

Issue #201

RFC9200 defines a non-HTTP transport for OAuth

Should OAuth 2.1 be updated to be less strict about binding to HTTP?

e.g. update sentences like:

```
OAuth URLs MUST use the https scheme except for loopback
interface redirect URIs, which MAY use the http scheme.
```

https://www.ietf.org/archive/id/draft-ietf-oauth-v2-1-12.html#section-1.5

Next Steps

Editors (and anyone else who wants to help!) to work on edits based on feedback from recent discussions, tracking in GitHub issues.

Move to Working Group Last Call before IETF 123.