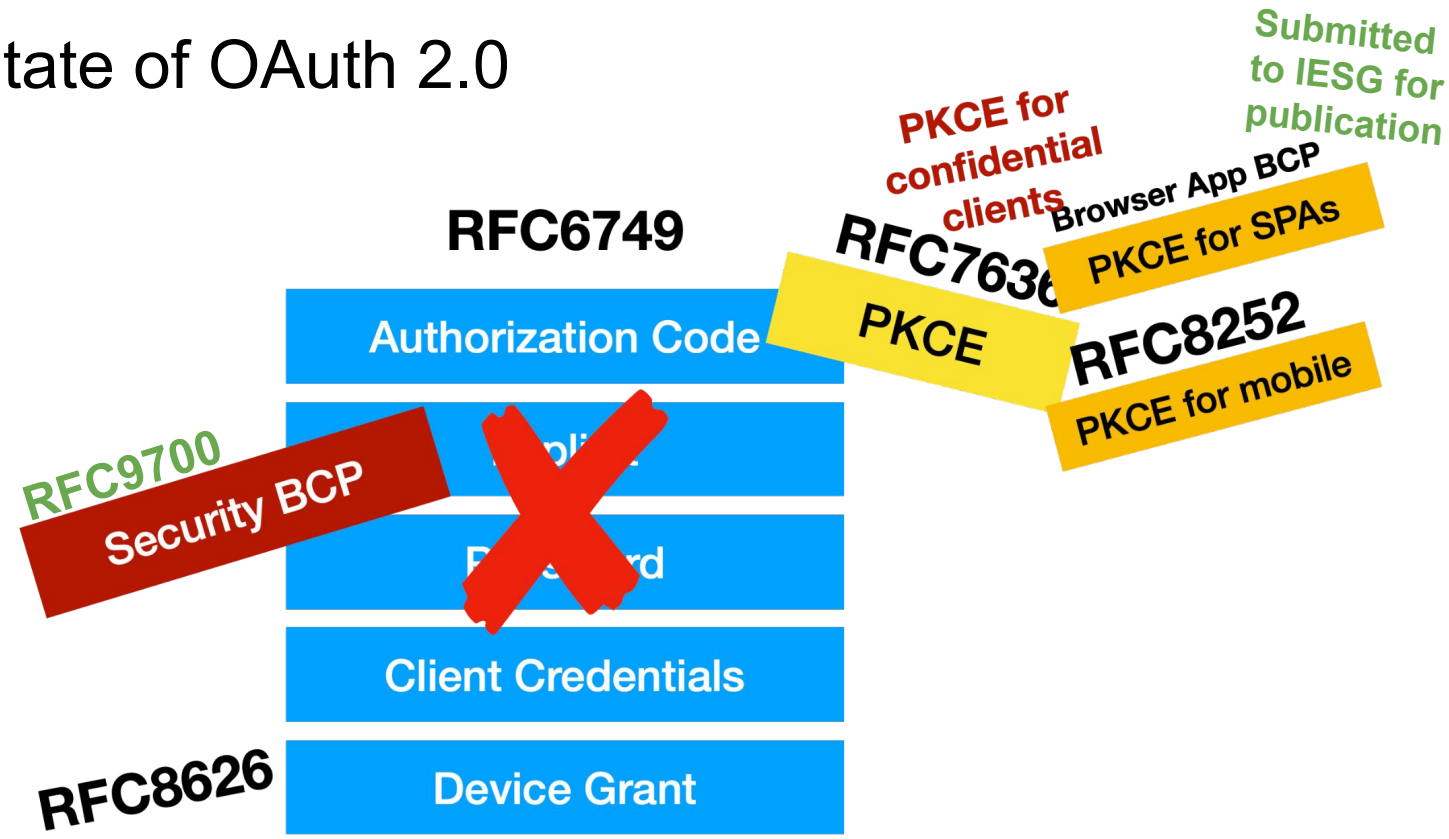
IETF 125
Shenzhen
March 2026

Aaron Parecki
Dick Hardt
Torsten Lodderstedt

OAuth 2.1

https://datatracker.ietf.org/doc/draft-ietf-oauth-v2-1/
draft -15

Current State of OAuth 2.0



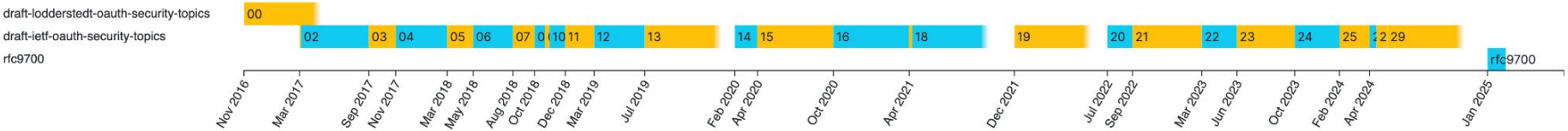
Goals

- 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, blocked on HTTP rfc6265bis*
- 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



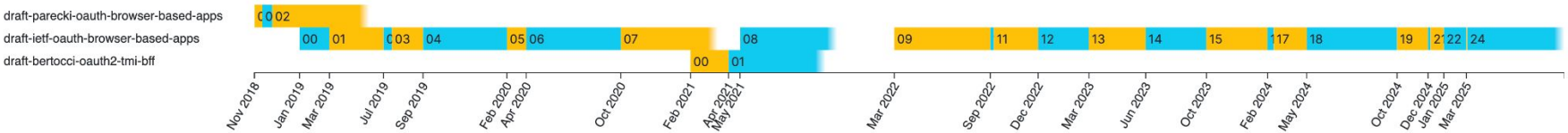
OAuth 2.0 for Browser-Based Applications

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



Changes since draft -14

- Resolved ambiguity around repeated parameters (Errata 5708)
- Applied erratas 3500 and 6613
- Synced language from RFC9700 about open redirect considerations
- Added additional context for JWT client authentication and specifically recommend following RFC7523bis
- Other editorial clarifications and updates

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.

#233 Make mix-up mitigation via iss response mandatory?

OAuth 2.1 already incorporates RFC9207's `iss` response as a possible mitigation to mix-up attacks (The other mitigation is distinct redirect URIs per AS)

Some ecosystems regularly interact with multiple ASs, and don't have the option to use distinct redirect URIs (MCP, and most clients using CIMD)

Also recommended in the "Updates to OAuth 2.0 Security BCP" [link]

The `iss` response is easy for the AS to add, and can easily be ignored for clients that don't need to check it.

Requiring `iss` means *each ecosystem doesn't have to make the decision on their own*, and many prefer not to because they look to the OAuth experts for the recommendation

#236 Forbid PKCE “plain” mode

The “plain” challenge mode was included in RFC7636 (2015) for devices that lack hashing functions.

OAuth 2.1 requires TLS 1.2+. TLS 1.2+ requires SHA-256.

JavaScript has had SHA-256 in the WebCrypto API since 2015.

Dropping “plain” eliminates downgrade attack vector.

Next Steps

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

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