IETF 120
Vancouver
July 2024

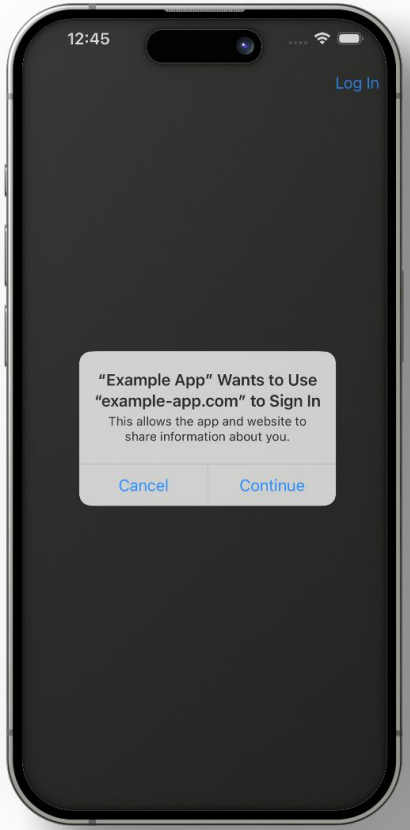
Aaron Parecki
George Fletcher
Pieter Kasselman

OAuth for First-Party Apps

https://datatracker.ietf.org/doc/draft-parecki-oauth-first-party-apps/
draft -02

Why?

Developers want a better user experience for first-party apps



What is happening today

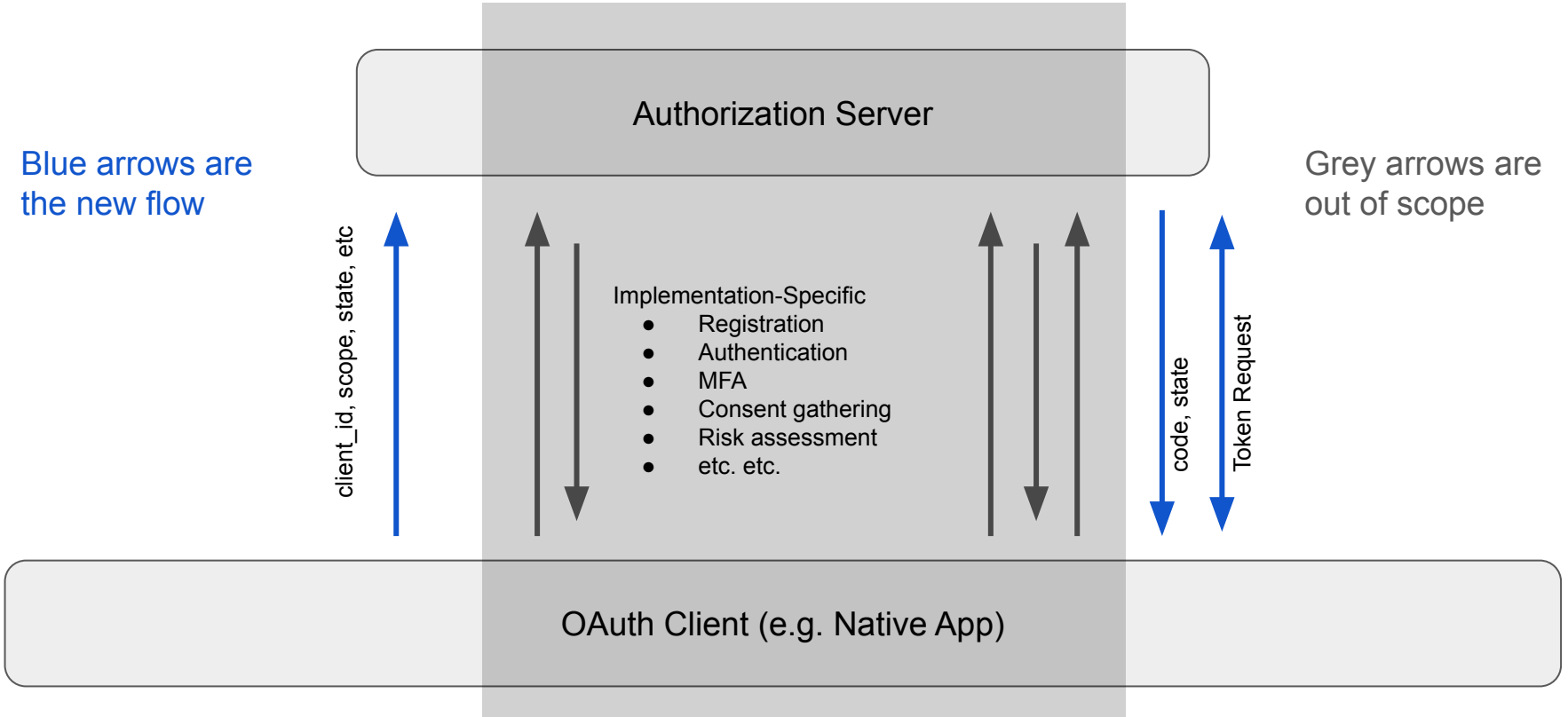
People are finding workarounds to avoid RFC8252

- Custom DIY solutions for native apps
- Using Resource Owner Password Grant
  - (Unable to add MFA)
- OAuth servers creating proprietary APIs to facilitate direct interaction with native apps
- Scripting hidden web views to emulate user interaction with the AS

Goals

- Reuse existing OAuth building blocks as much as possible
- Mirror the web authorization code flow, defining how the client starts and ends the flow
  - Leave the specifics of the user authentication out of the core framework
- Specifics of user authentication can be proprietary to an AS as they are today, or can be defined as extensions
  - Especially if based on standards like FIDO

First-Party Apps Flow



Authorization Challenge Endpoint

- New endpoint
- Accepts parameters that would have been included in the query string to the authorization endpoint
  - including any extensions such as Resource Indicators, OpenID Connect, JAR, etc
- Accepts POST from client to start and continue an authorization
  - The AS defines what the client sends in the requests and defines its own error responses
- Response is an authorization code, error, “redirect_to_web”, or custom
  - The AS may want to interact with the user directly, e.g. based on risk assessment, new authentication method not implemented in the app, or exceptions like account recovery
- Further interaction with the user can happen at custom endpoints

Changes since IETF 119

- Updated authorization code binding with DPoP (#59)
- Removed "`ash`" claim for DPoP binding (#58)
- Enable PAR as an optional optimization for "redirect to web" (#46)
  - Turned "redirect to web" response into an error response
  - Also added "`request_uri`" to error response
  - If the client expects "redirect to web" frequently, it can include a PKCE code challenge in the initial authorization challenge request
- Clarified follow-up requests are not required to be form-encoded (#50)
  - Feedback from Brian Campbell at IETF 118
- Require `auth_session` is bound to a device (#57)
  - Prohibits moving sessions across devices

In-Progress Implementations

- Microsoft
  - https://devblogs.microsoft.com/identity/introducing-native-auth/
  - (based on an earlier version of this draft)
- Yahoo
  - https://identiverse.com/idv24/session/2089642/
- Auth0 by Okta
  - (in progress, no public docs yet)

Interest From

- Keycloak
  - https://github.com/keycloak/keycloak/discussions/25014

Next Steps

- Working group adoption?
- Create an extension to this draft for passkeys
  - In progress work from Tim Cappalli https://github.com/aaronpk/oauth-first-party-apps/pull/93