IETF 121
Dublin
November 2024

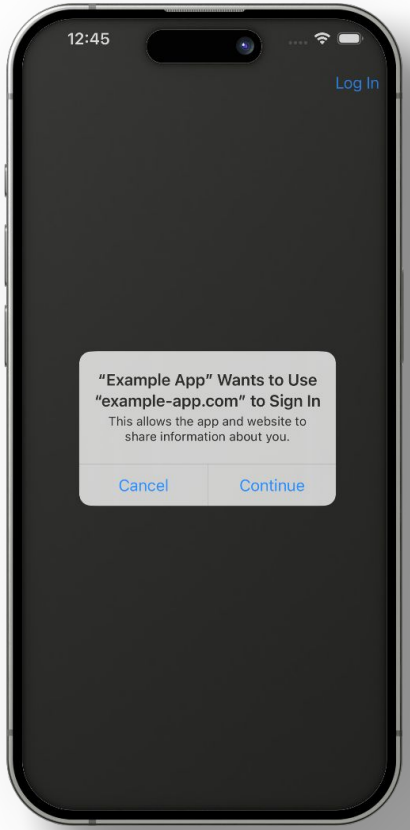
Aaron Parecki
George Fletcher
Pieter Kasselman

OAuth for First-Party Apps

https://datatracker.ietf.org/doc/draft-ietf-oauth-first-party-apps/
draft -00

Why?

Developers want a better user experience for first-party apps

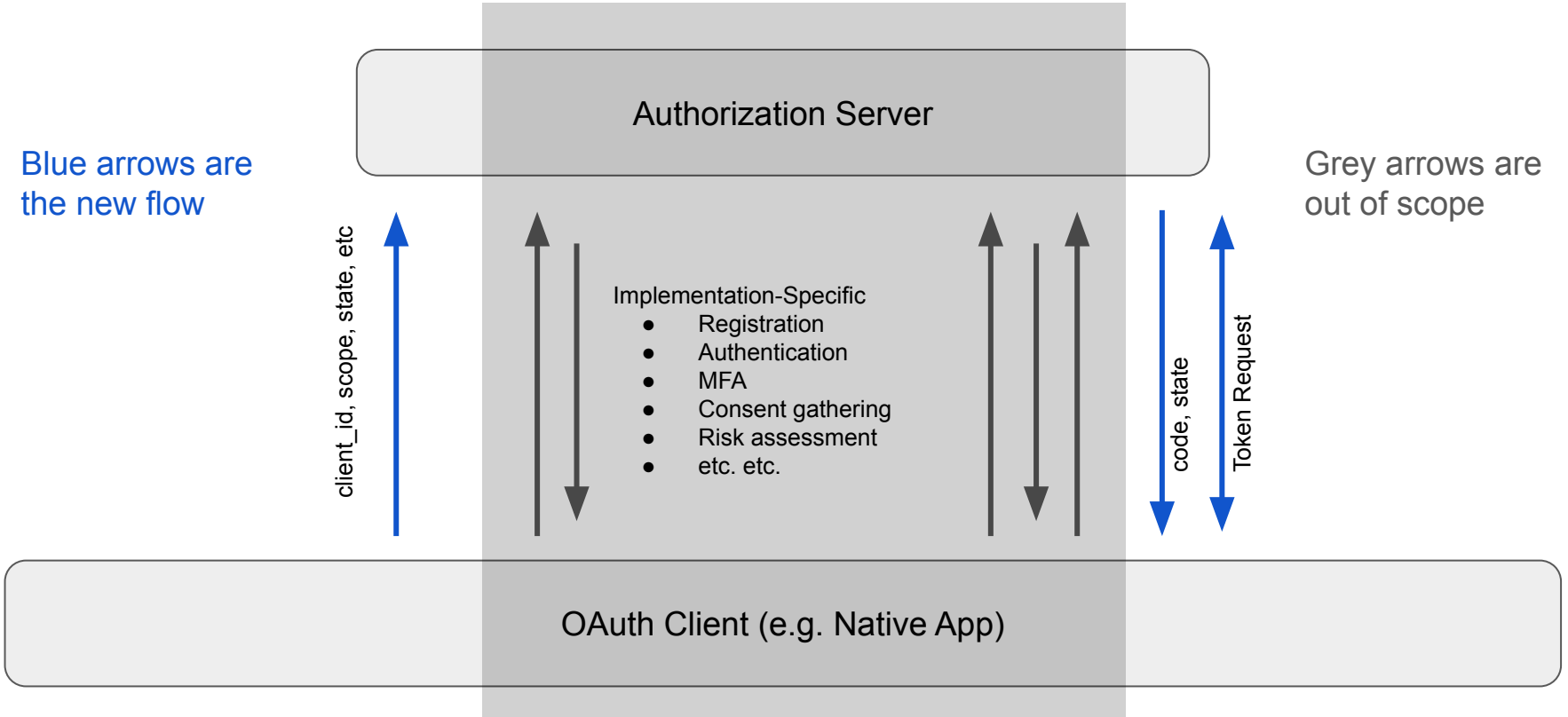


What is happening today

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

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

What’s New?

Adopted in the OAuth WG!

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

New Implementations

WSO2 - Presentation from IIW last week

https://drive.google.com/file/d/1_KQC9AjyTY4xSgSp2G9Lz7Fz85Ygyjw9/view

Open Source Client

https://github.com/asgardeo/mobile-ui-sdks

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
  - (in progress, no public docs yet)
- Keycloak
  - https://github.com/keycloak/keycloak/discussions/25014

Next Steps

Create an extension to this draft for passkeys

- In progress work from Tim Cappalli https://github.com/oauth-wg/oauth-first-party-apps/pull/93

Should this be an extension, or incorporated into this doc?