Lessons learned from implementing Native OIDC from scratch

Hej, jeg er The one with the braid

- [matrix] Consultant & Software Architect
    - Client development
    - OIDC
    - Sliding Sync
    - End-to-End Encryption
- Cryptography
- Unix, Flutter & AArch64
- ask me about night trains 🚂

Anything new ?

No ! I’m just sharing my humble experience.

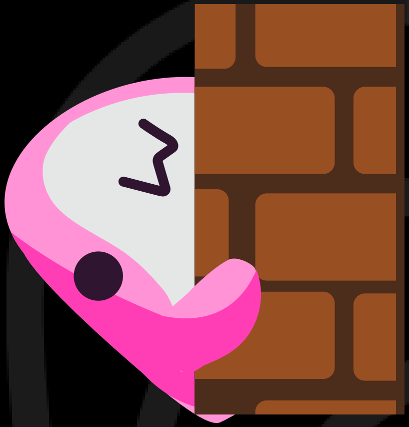
But why ?

Beep boop and I had too much time during boring work meetings. Using this client as a small piece to practice some matrix related stuff.

I’m especially considering to experiment with Sliding Sync and Flutter Linux-native integrations.

This is < polycule >

https://polycule.im/



< polycule >

– a geeky and efficient [matrix] client

What’s that ?

- Playground
- Geeky
    - Keyboard focussed
    - Accessible
    - Linux, postmarket OS, Android & web
- Next-gen
- ground work in Dart

Ground work

- Sliding Sync
  - See last year’s talk
- Vodozemac
- Widget experiments
- Matrix OIDC

Is it usable ?

No.

Matrix OIDC

- Considered frameworks
  - `package:app_auth`
  - `package:oidc_core`
- But compatibility ?
  - No native code

OIDC in the Matrix Dart SDK

Thanks to my friends from famedly for the amazing SDK !

- Drop-in
- Minimal (1k loc)
- Atomic
- No native code
- High-level redirect handler
- Zero-code token refresh

Implementation

- ☑ MSC 3861 - Next-generation auth for Matrix, based on OAuth 2.0/OIDC

Implementation

- ☑ MSC 1597 - Better spec for matrix identifiers
- ☑ MSC 2964 - Usage of OAuth 2.0 authorization code grant and refresh token grant
- ☑ MSC 2965 - OAuth 2.0 Authorization Server Metadata discovery
- ☑ MSC 2966 - Usage of OAuth 2.0 Dynamic Client Registration in Matrix
- ☑ MSC 2967 - API scopes
- ☑ MSC 3824 - OIDC aware clients

Implementation

- MSC 4108 - Mechanism to allow OIDC sign in and E2EE set up via QR code - **not planned at this time**
- MSC 4190 - Device management for application services - **not planned at this time**

Implementation

- ☑ MSC 4191 - Account management deep-linking

Lessons learned

Redirect URLs

are cursed

URL encoding

is cursed

Token rotation during SSSS

is cursed

Multi-threading

is cursed

Dnamic Client Registration Metadata Localization

is cursed

systemd-oomd

is cursed

Discovery

is cursed

- MSC2965
  - Via `/auth_metadata`
  - Via matrix `.well-known` (deprecated)
  - OIDC native via `.well-known` (deprecated)
  - Via `/auth_issuer` (deprecated)

Can you try it ?

Yes ! https://polycule.im/web/

https://github.com/famedly/matrix-dart-sdk/pull/2024

Thanks a lot to Quentin !

Get in touch

- I’m [matrix] consultant and Software Architect
- info@braid.business
- @braid:alsace.hair

🌈 rights are human rights !

Questions

https://areweoidcyet.com/