ORY / summit-22

Shota Sawada

TIER IV

shota@sslife.tech

@sawadashota

How TIER IV Replaced its Identity Server with Ory

October 20th 2022

About me

Shota Sawada
Auth Engineer at TIER IV
https://tier4.jp/en/

LinkedIn: sawadashota
Twitter: @xioota
GitHub: @sawadashota

Before we start

Posted on Ory's website as a case study
ory.sh/case-study-identityserver-alternative-open-source

In Japanese (TIER IV's Tech Blog)
link.medium.com/K8wsfVUZDsb

Agenda

01 Identity Server at Autonomous Driving Platform

02 Why Ory?

03 Architecture (Before/After)

04 Working for Replacement

05 Conclusion

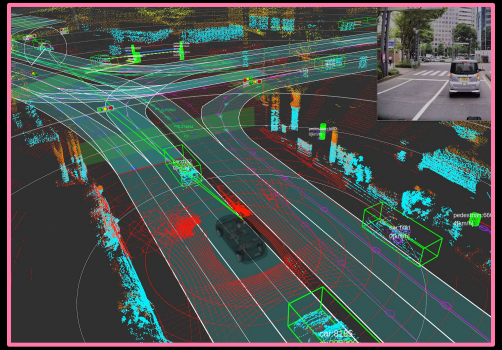
01

Identity Server at Autonomous Driving Platform

01

About TIER IV

TIER IV Develops Software for Autonomous Driving



About the Identity Server

Multi Purpose of Account

Personal Account

Organization Account

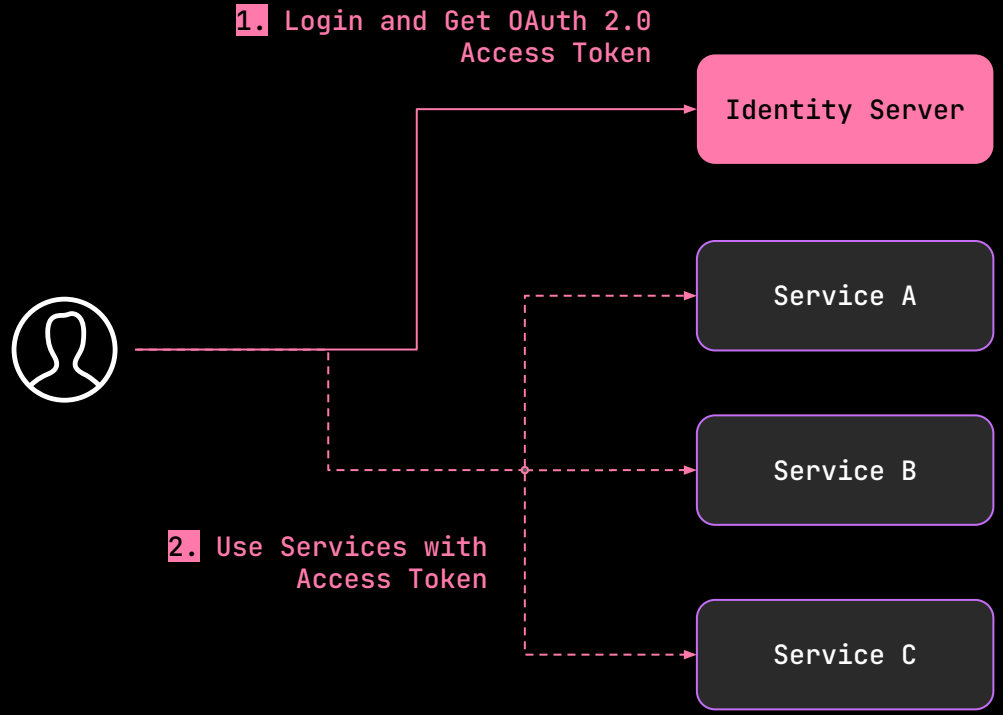
High Productivity

High Reliability

High Performance

Scalable

About the Identity Server



02

Why Ory?

02

Data Migration

- Can we change the identifiers for existing account?
- Can we force-reset user passwords?
- Can we change the OAuth Client ID and secrets?

02

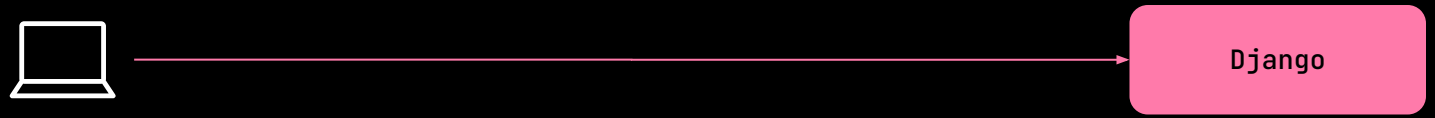
Can we contribute, too?

- Good OSS maintainers and community
- Our team is familiar with Go language

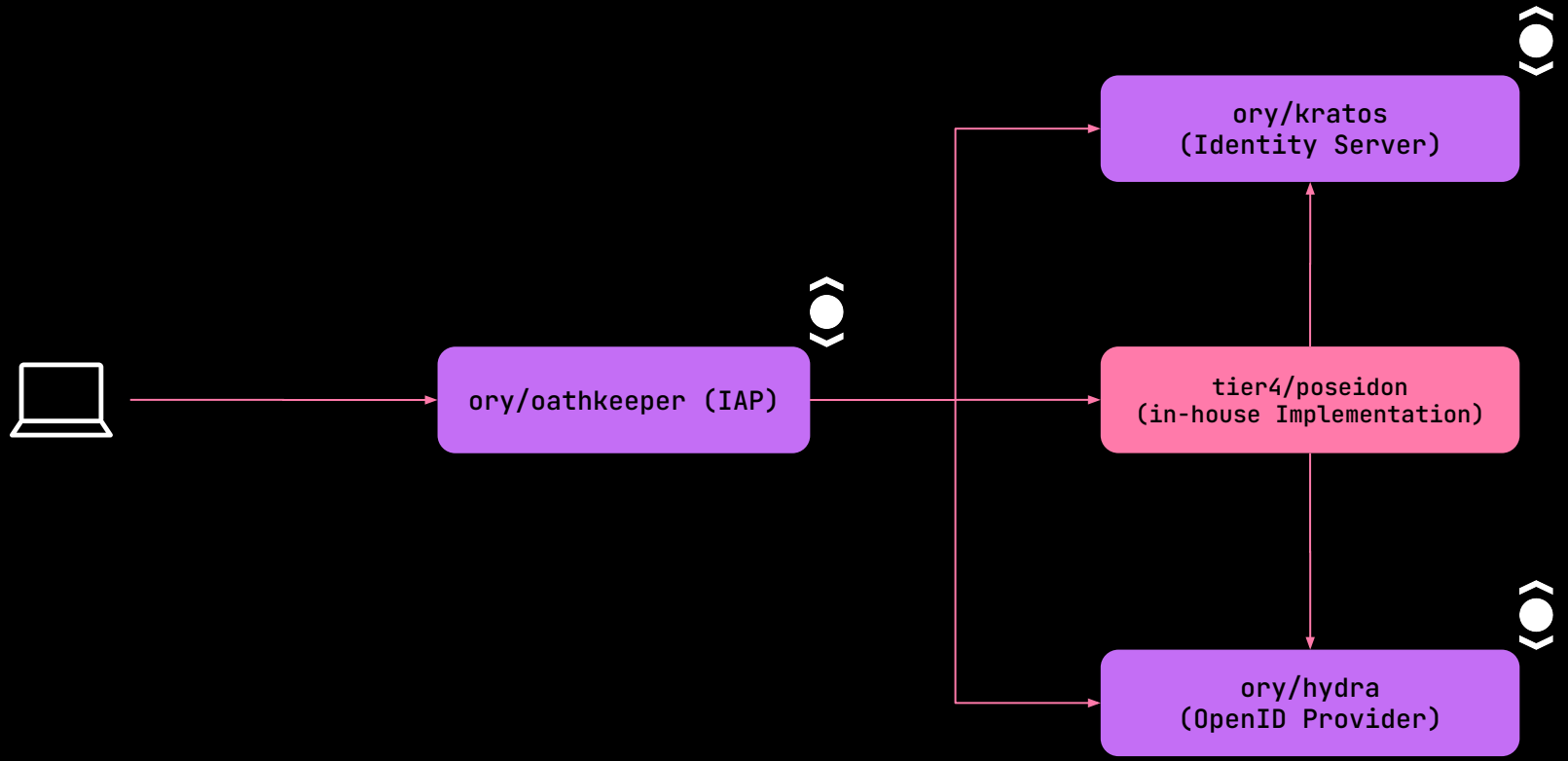
03

Architecture (Before/After)

Architecture (Before)

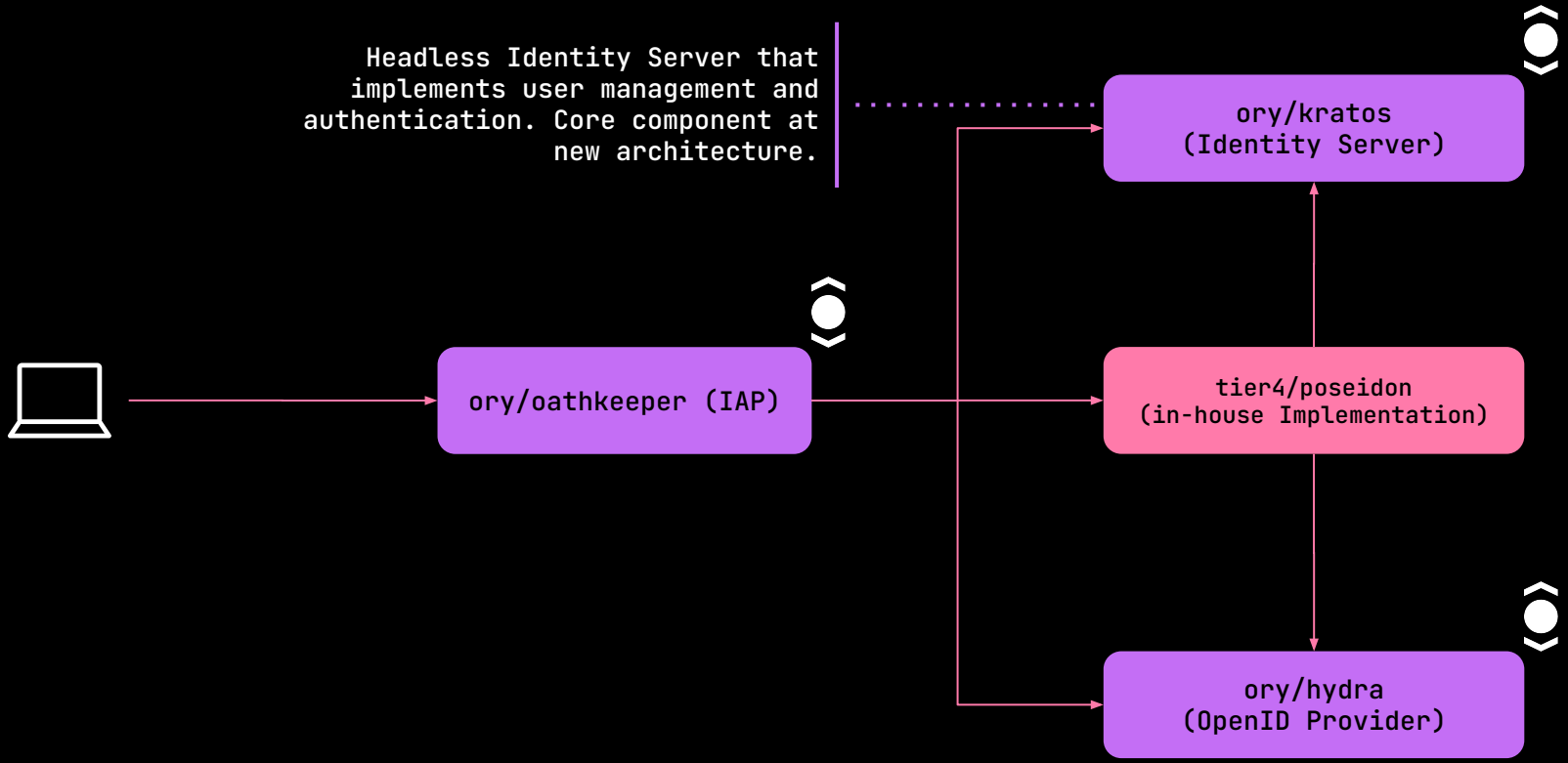


Architecture (After)

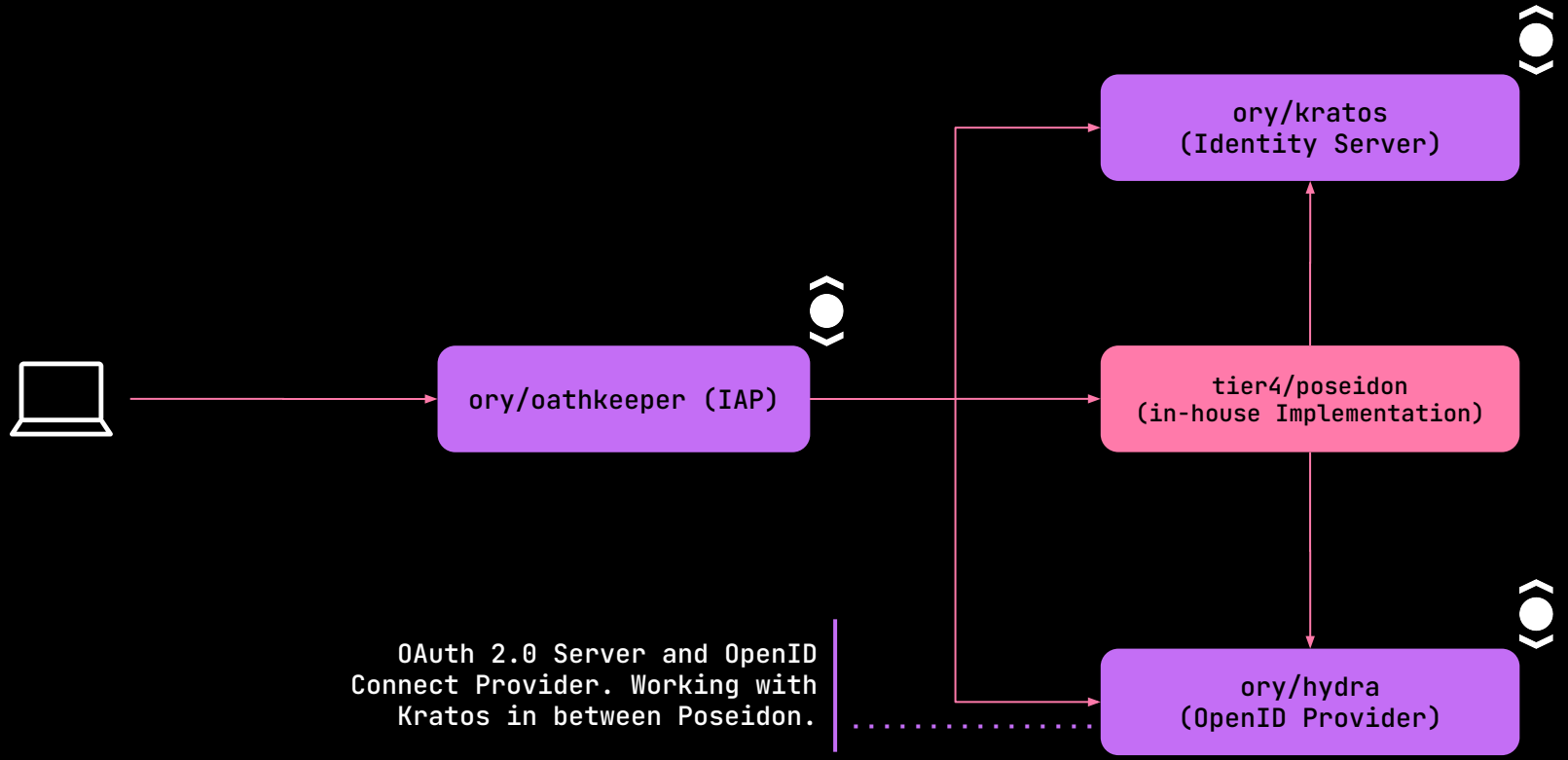


Architecture (After)

Headless Identity Server that implements user management and authentication. Core component at new architecture.

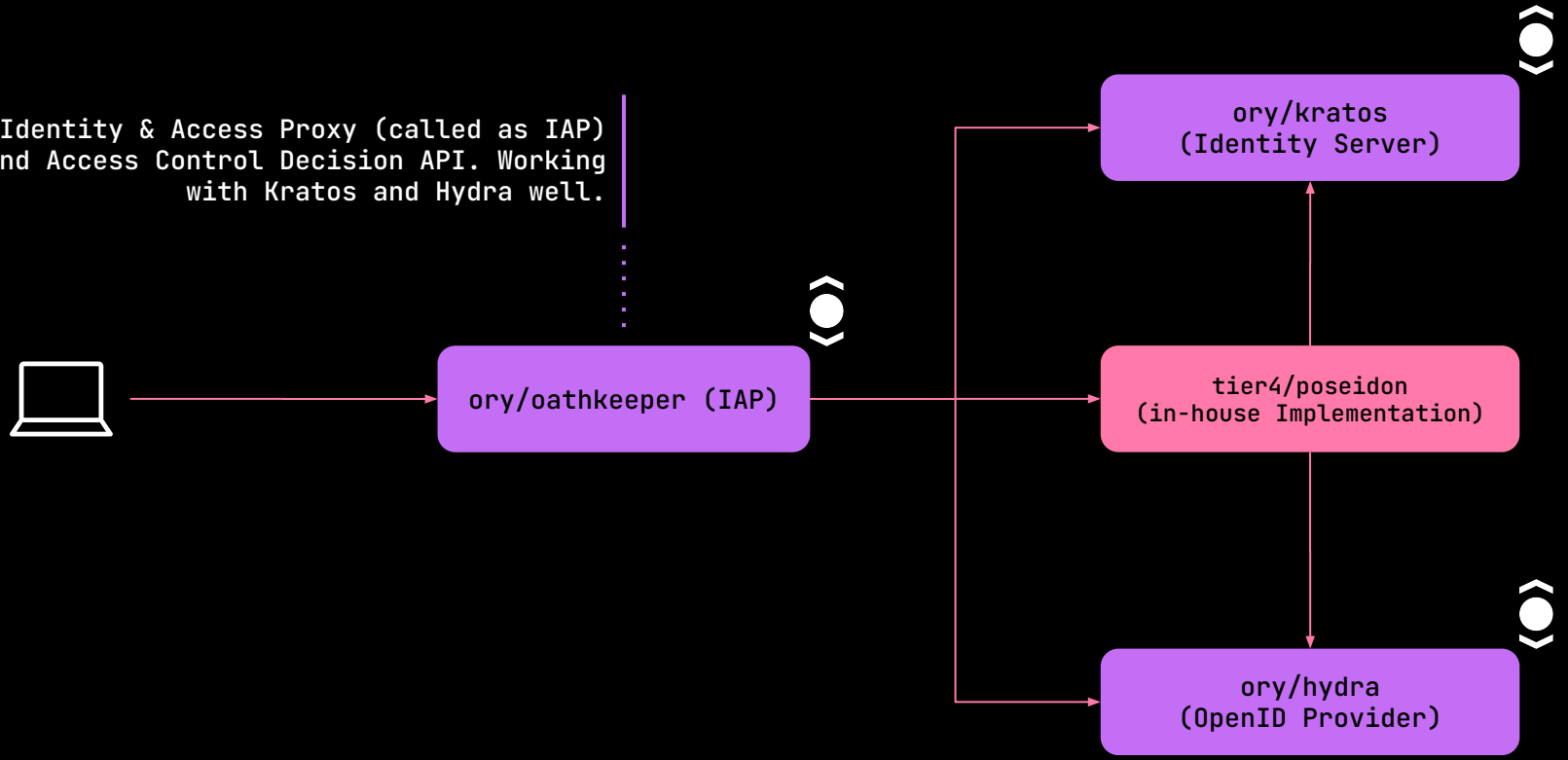


Architecture (After)



Architecture (After)

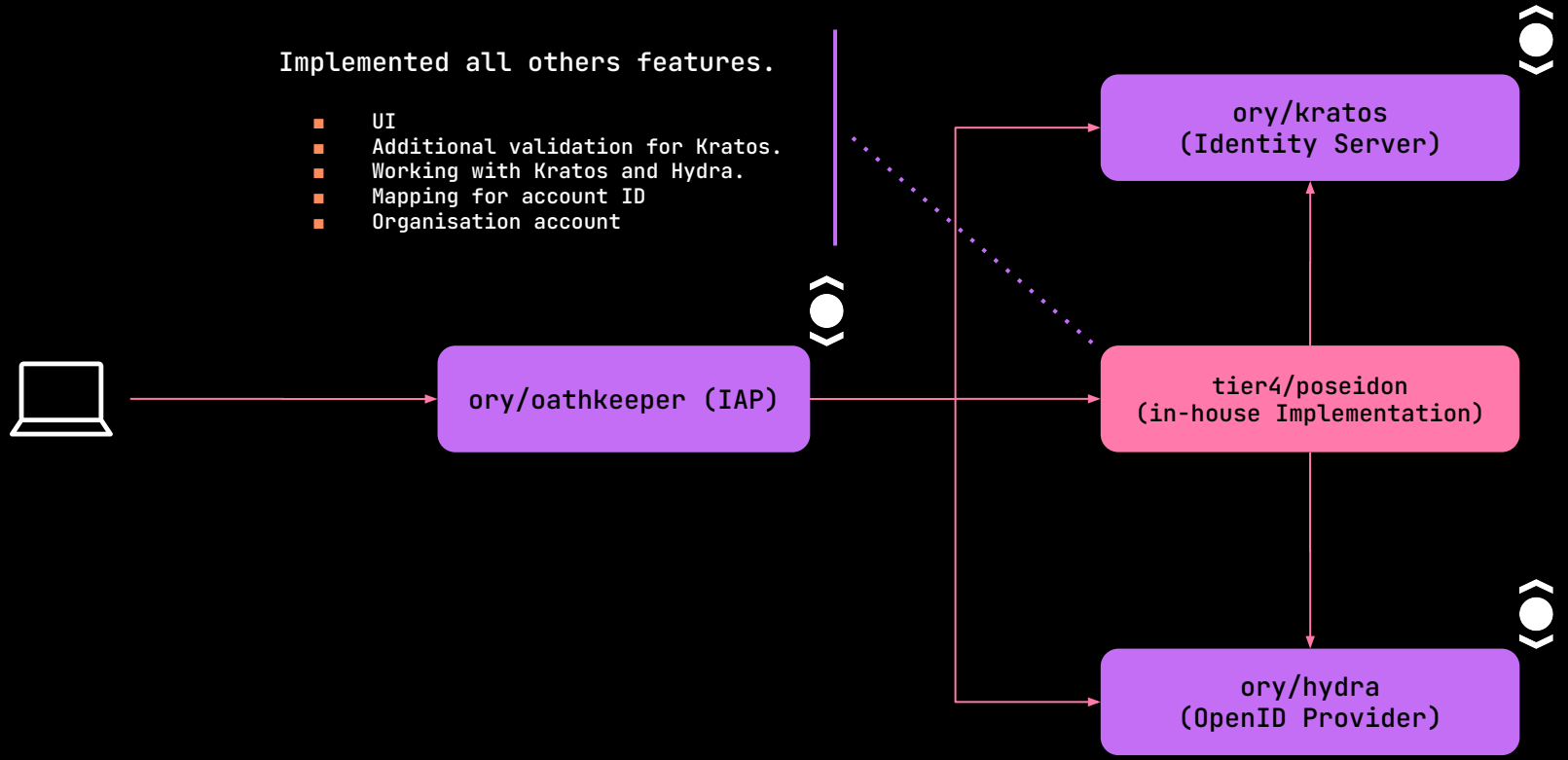
Identity & Access Proxy (called as IAP) and Access Control Decision API. Working with Kratos and Hydra well.



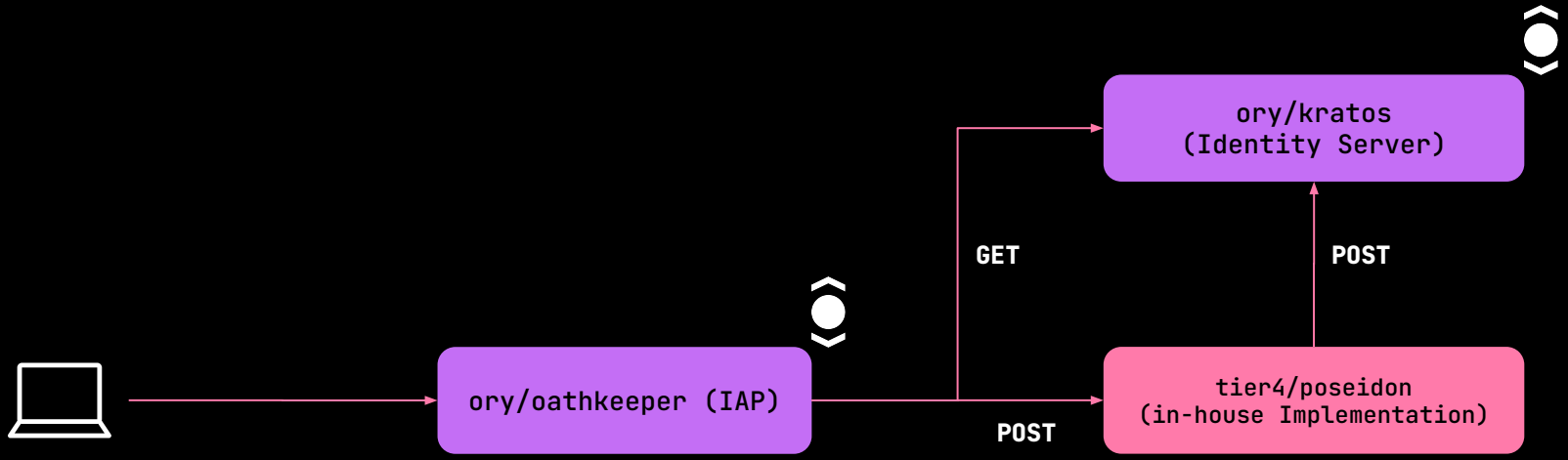
Architecture (After)

Implemented all others features.

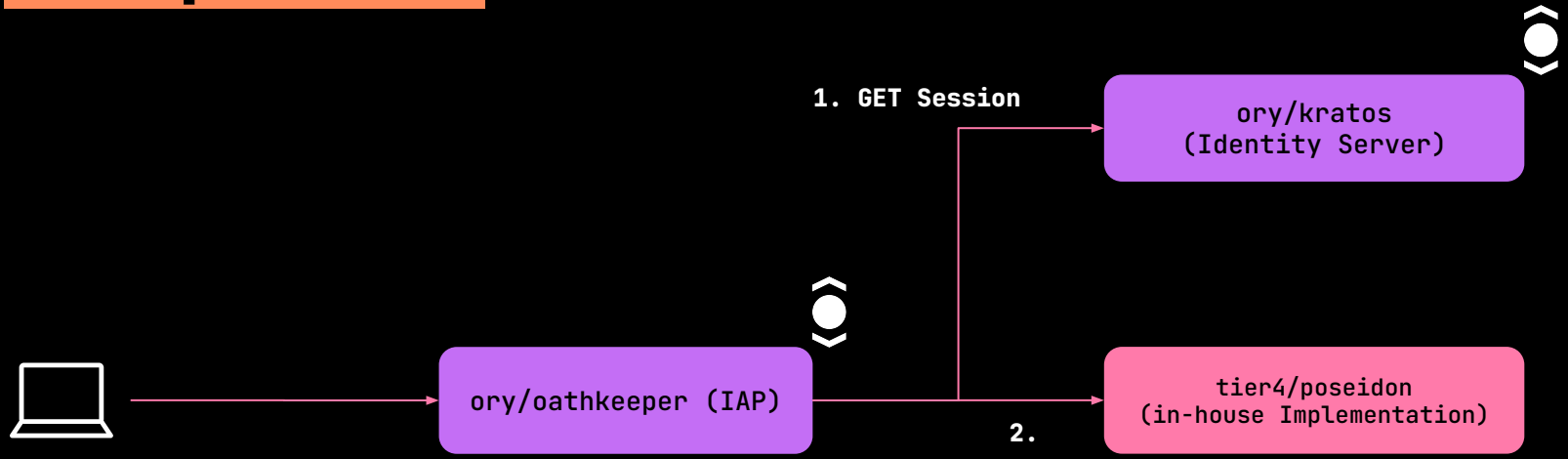
- UI
- Additional validation for Kratos.
- Working with Kratos and Hydra.
- Mapping for account ID
- Organisation account



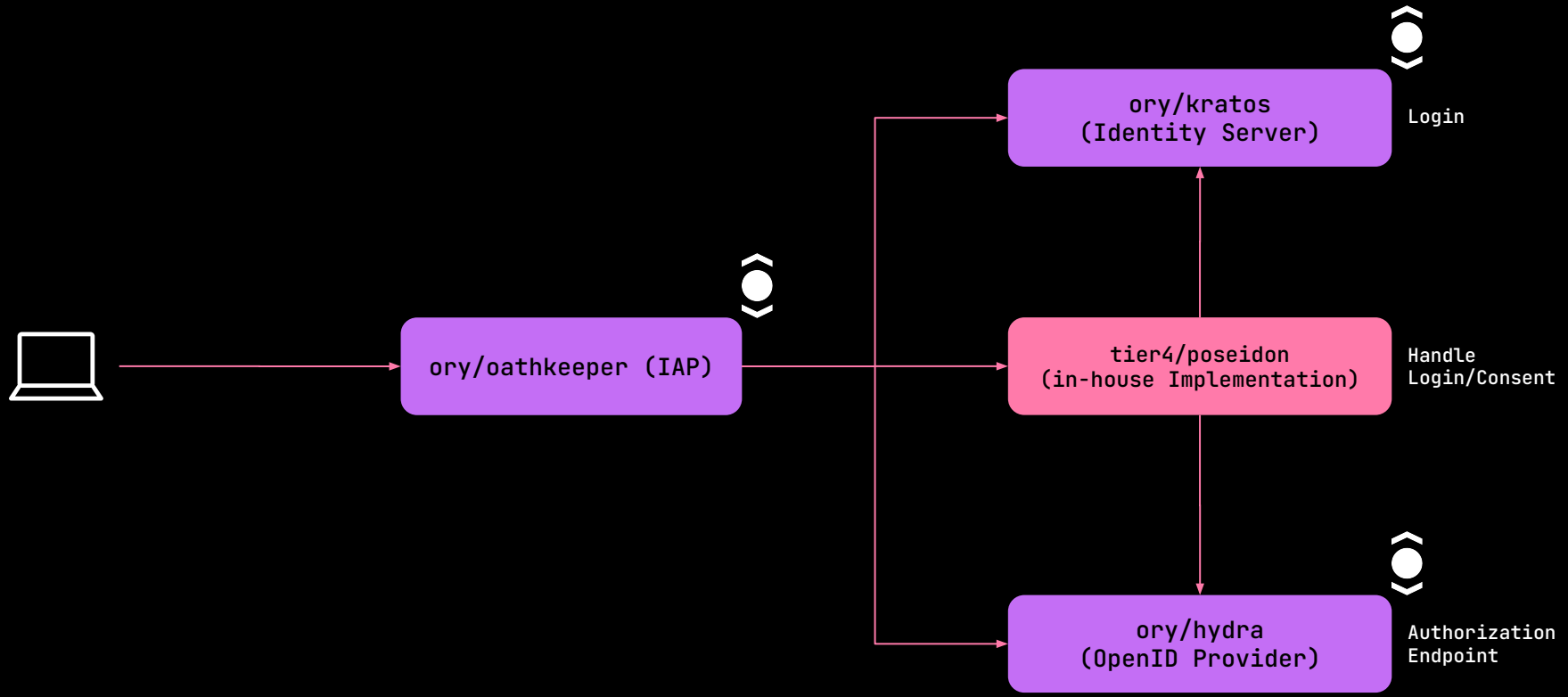
Account Management UI



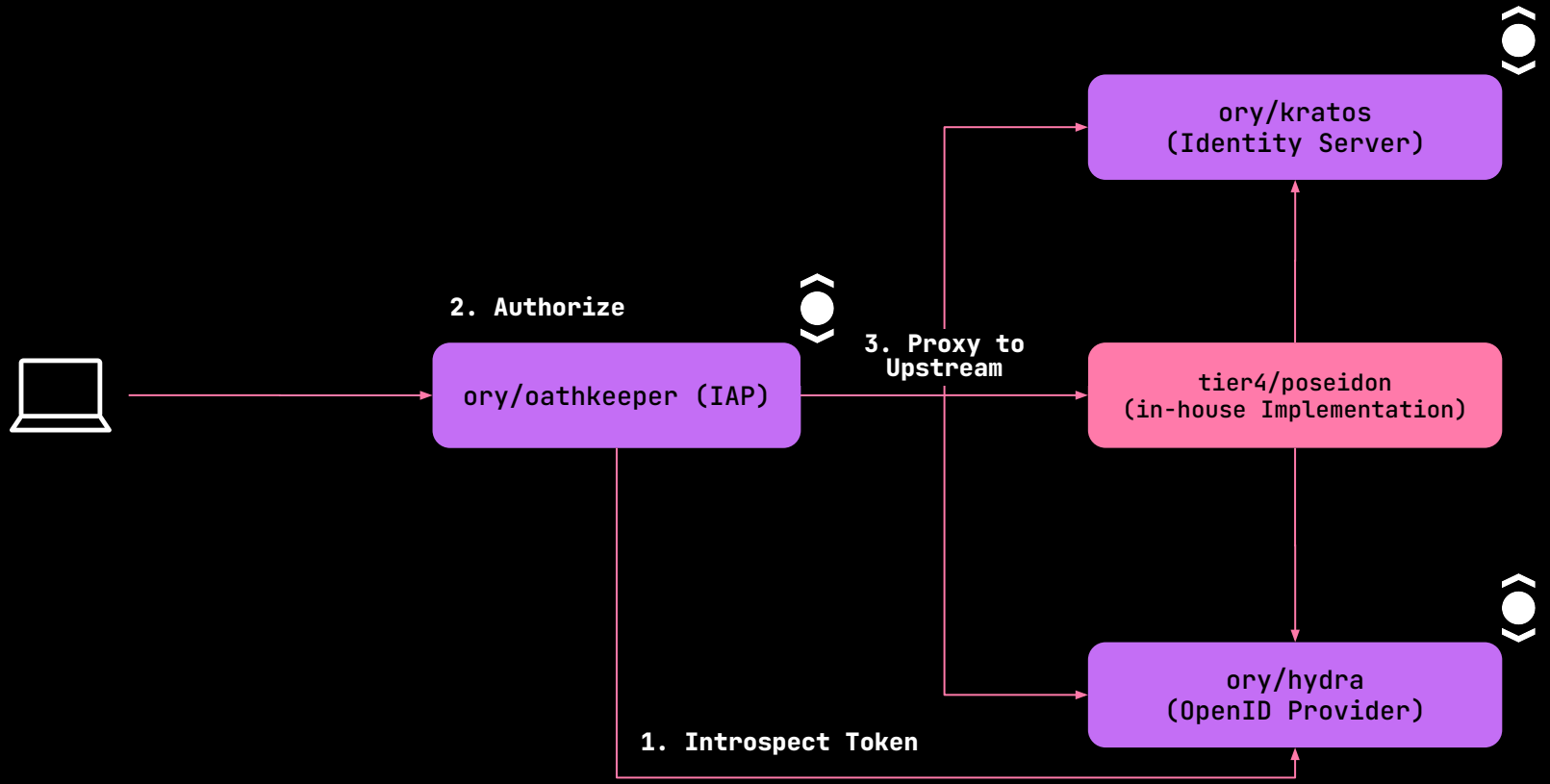
Oathkeeper Propagates Session to Upstream



Authorization Code Flow



Admin API


ory/kratos
(Identity Server)
2. Authorize
ory/oathkeeper (IAP)
3. Proxy to
Upstream
tier4/poseidon
(in-house Implementation)
ory/hydra
(OpenID Provider)
1. Introspect Token

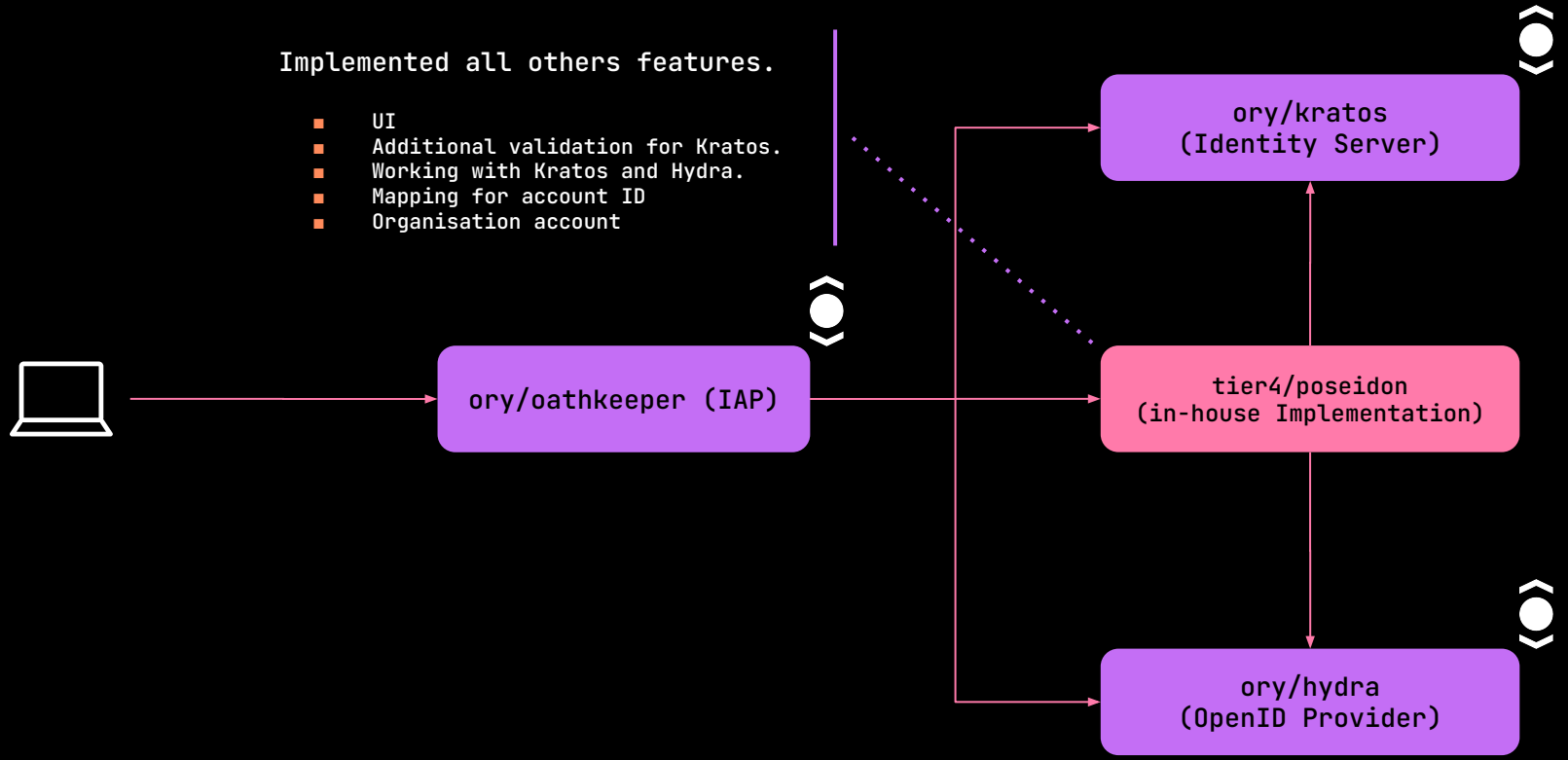
04

Working towards Replacement

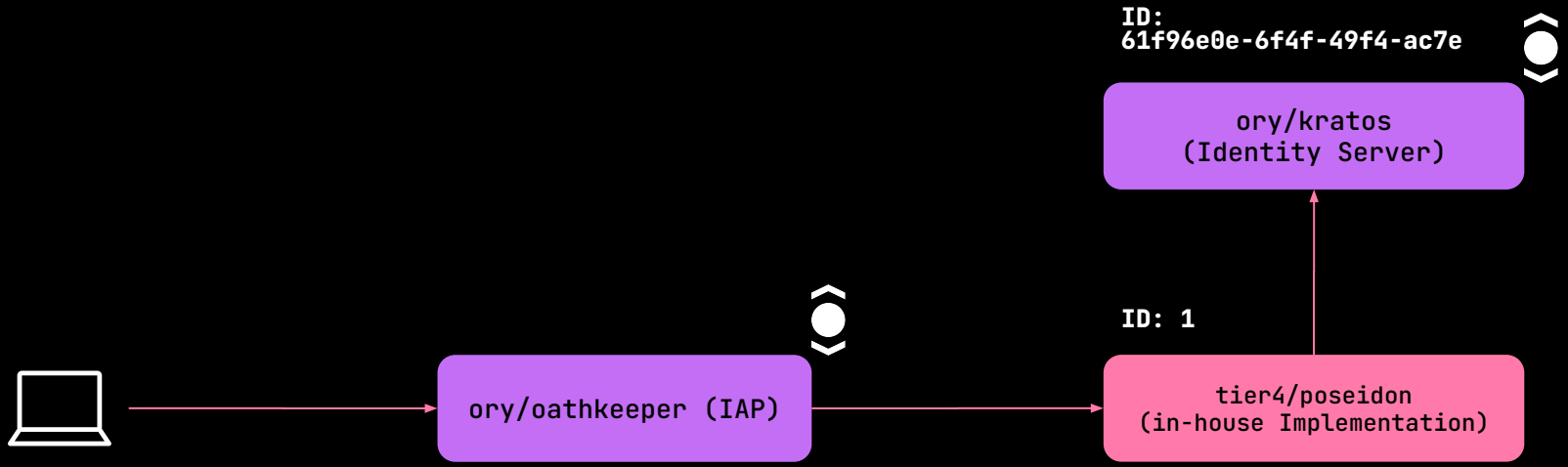
Implementation for Poseidon

Implemented all others features.

- UI
- Additional validation for Kratos.
- Working with Kratos and Hydra.
- Mapping for account ID
- Organisation account



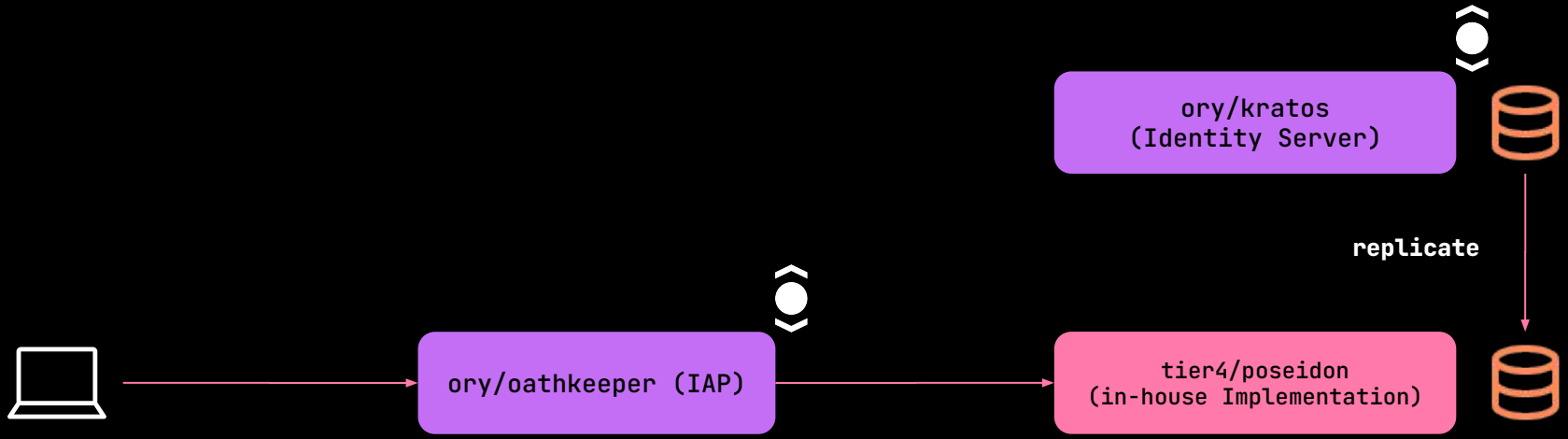
Mapping for Account Identifier



Implementation - Organization Account

- Account management by organization admin
  - Only organization admin can update email of an account
  - Only organization admin can delete an account
  - Create/invite an account by organization admin
- Organization policy
  - Enforce MFA/2FA

Replicate Some Kratos Data for Query



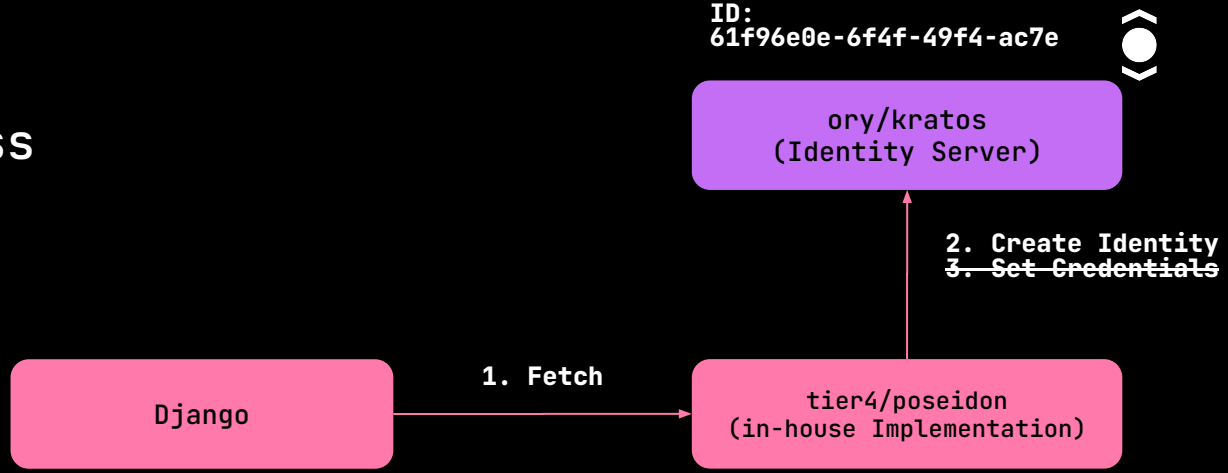
04

Data Migration

- User
- OAuth client

Data Migration - User

- Name
- Identifier
- Email Address
- Password



Data Migration - User

PBKDF2 Format at Django

<algorithm>$<iterations>$<salt>$<hash>

PBKDF2 Format at Kratos

$pbkdf2-<algorithm>$i=<iteration>,l=<length>$<salt>$<hash>

https://www.ory.sh/docs/kratos/concepts/credentials/username-email-password#pbkdf2

Data Migration - OAuth Client

```
$ hydra clients create --id <id> --secret <secret> …
```

05

Conclusion

05

Conclusion

- We completed replacing an identity server in 3 months by using Ory stack
- We need a lot of work because we want features such as organization accounts
- Kratos is evolving day by day. You may migrate your Identity Server with Ory stack more easily.

Thanks Again!

Contact Us:
https://tier4.jp/en/