ORY / summit-22

Ilya Migal/
Dominik Lekse

Technical Product Owner/
Cloud Architect @
Jochen Schweizer mydays
Group

One Auth Gateway to authenticate them all

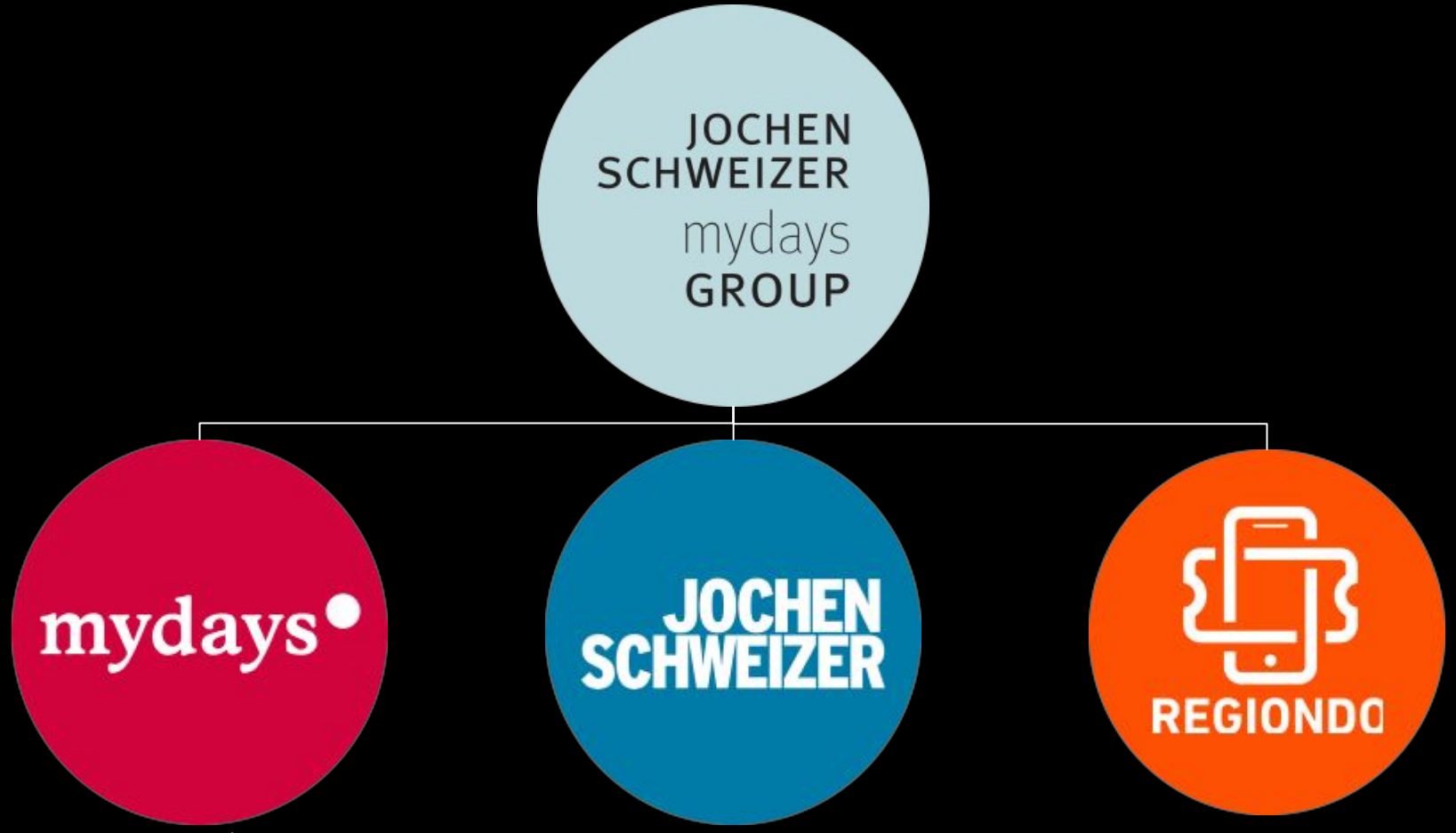
20 - 10 - 2022
@ Ory Summit 2022

Agenda

1. Introduction
2. Challenges
3. Objective
4. Solution
5. Learnings


JOCHEN SCHWEIZER mydays GROUP
Wir sind Erlebnis.

JOCHEN SCHWEIZER MYDAYS GROUP



Services

Infrastructure

Services

Infrastructure

Services

Infrastructure

Services

Infrastructure

Services

Identity & Access Management

Platform

Objectives: Authentication Gateway

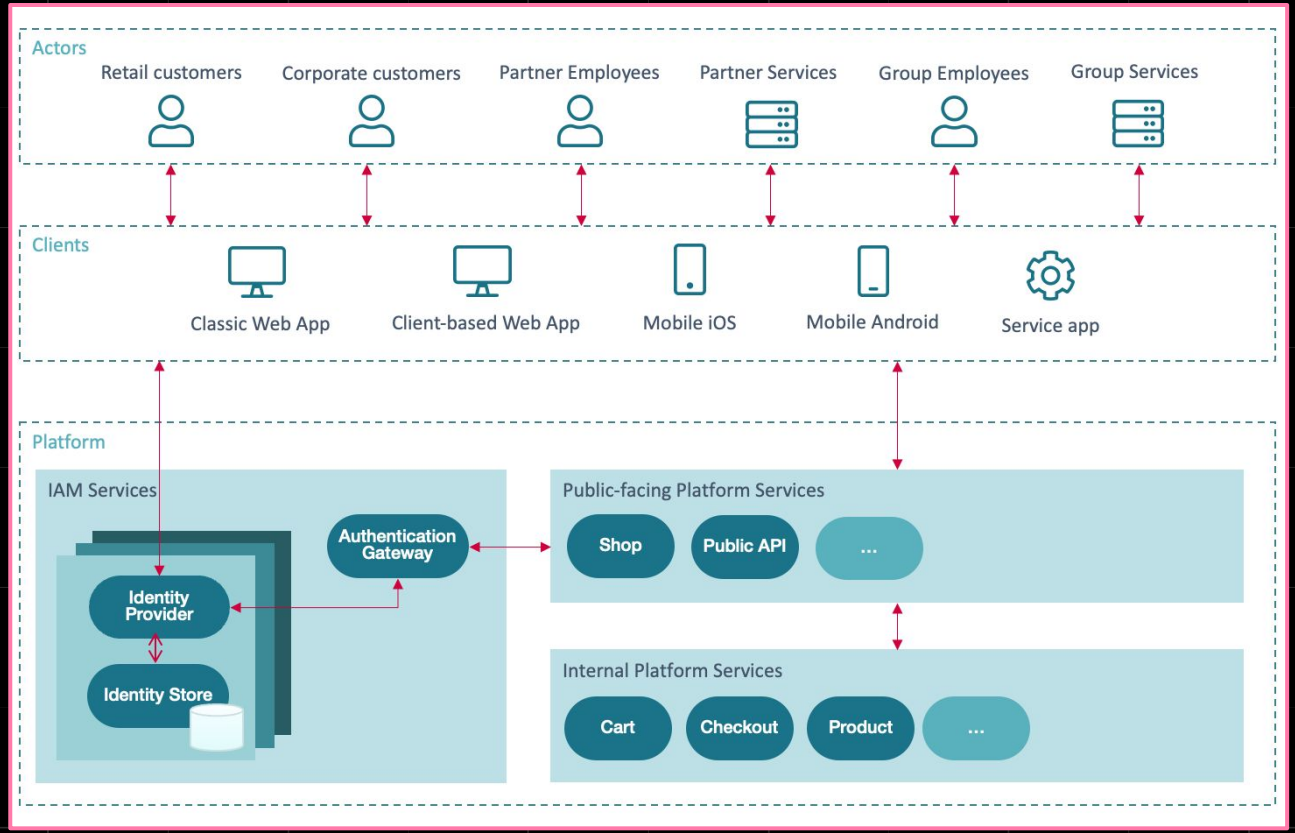
- Abstract from different identity providers
- Common internal identity representation
- Reduce development effort for service teams
- Reduce surface for implementation errors

Decision: Ory Oathkeeper

Outstanding reasons compared to alternatives:

- Access rule concept
- Pipeline composition with handlers
- Extensibility
- Decision API

Ory Oathkeeper: Integration



Ory Oathkeeper: Responsibilities

- Authentication decision for all inbound requests
- Verify external JWT access tokens
- Rotate public signature keys of trusted IdPs
- Issue internal identity token

Internal Identity Token

- Consistent identity representation
- Abstract from external IdPs
- Audience: Internal services
- Issued by Ory Oathkeeper
- Passed in transitive requests

Customizations & Extensions

- Authenticator: initiate and callback in OIDC auth code flow
- Authenticator: AWS Cognito User Pool
- Mutator: Internal identity token
- JWT token revocation check
- Allow matching any HTTP method in access rule

Learnings

The good parts:

- Oathkeeper scales
- Access rule standardization
- No deviators: All services rely on Oathkeeper

The hard parts:

- Managing access rules
- Releasing access rules


We are hiring!
Join us!

Thank you!

Questions?