KEYCLOAK - OPEN BANKING

FRANCIS POUATCHA - ADORSYS
KANNAN RASAPPAN - BANFICO

OPEN BANKING

Opening up banking services to be provided to the consumer by regulated fintechs.

Consent and Data Privacy are key to open banking

Market Driven

Innovations
Financial Inclusion

Regulatory Driven

Improve Competition
Financial Inclusion

OPEN DATA EVOLUTION

- Data is the new oil
- Data belongs to the consumer - Consent and Authorisation
- Federation of data - bringing all customer data to one place
- Improve customer offerings through personalisation

Open Banking

UK and Europe lead the open banking regulations covering only payment accounts

Open Finance

is the next step of open banking - covers Investments, Pensions, Mortgage, Loans, Savings ..

Open Insurance

accessing and sharing insurance-related personal and non-personal data usually via APIs.

Open Energy

Open Energy makes it easier to discover, share, access and use energy and related datasets ...

OB BUILDING BLOCKS

- Authorisation Server - OpenID FAPI, CIBA
- Identity Provider Integration
- API Gateway
- Consent Management
- Strong Customer Authentication
- Regulatory Authorisation Checks
- Core Bank Integration

IAM vs APIM

Open Banking is more about IAM than APIM

IAM

- Authentication (SCA)
- Authorisation
- Consent Management

API Management

- Developer Portal
- API Analytics
- Product Catalogue
- Monetisation

KEYCLOAK

Keycloak/RHSSO is the most supported open source and is also widely used within the banking community

Very early implementors of FAPI or any new Identity standards for that matter - JOIN US

Authorisation Server

Open Banking standards across the world looked for strong authorisation model better than vanilla OAuth2 - which led to FAPI

Open Banking UK - started with the implementor draft of FAPI 1.0

Today - all jurisdictions are recommending/mandating FAPI - UK, Australia, Brazil, Bahrain, Saudi Arabia

Identity Brokering

Banks provided their own legacy or bespoke identity provider - some supported SAML, OpenID/OAuth2.

Banks didn't want the customer credentials inputted on the open banking platform

Support for

- redirect flow - web or app-to-app
- decoupled flow - push notifications (CIBA)

SPI

Many authentication methods were served through identity Brokering - but still, some are embedded as SPI in connecting to banks' IDP

Certain country-specific FAPI customisations are implemented as SPI

Token Management

Implementing different token strategies for AISP, PISP and others

access_token, refresh_Token, id_token - different configs for the flows

Long-lived token - change in regulation (90 days rule changed to long-lived)

CONSENT MODEL

Open Banking Consents

Resource-based fine-grained consent model

Each API had a consent resource associated and the checks were done in different ways - within the API, as IAM Policies

User Managed Access (UMA)

User-Managed Access (UMA) is an OAuth-based access management protocol standard - Kantara Initiative

Implemented in UK's - Open Pensions (Pensions Dashboard by Origo)

THANK YOU

FOR COMING