Since 1822
(Christiania Sparebank)

More than 10.500
Employees

About 3.300.000
Private Customers

220.000 Corporate
Customers

Presence in 15
countries in

Europe, America,
Asia and Australia

Identity Day Norway 2024

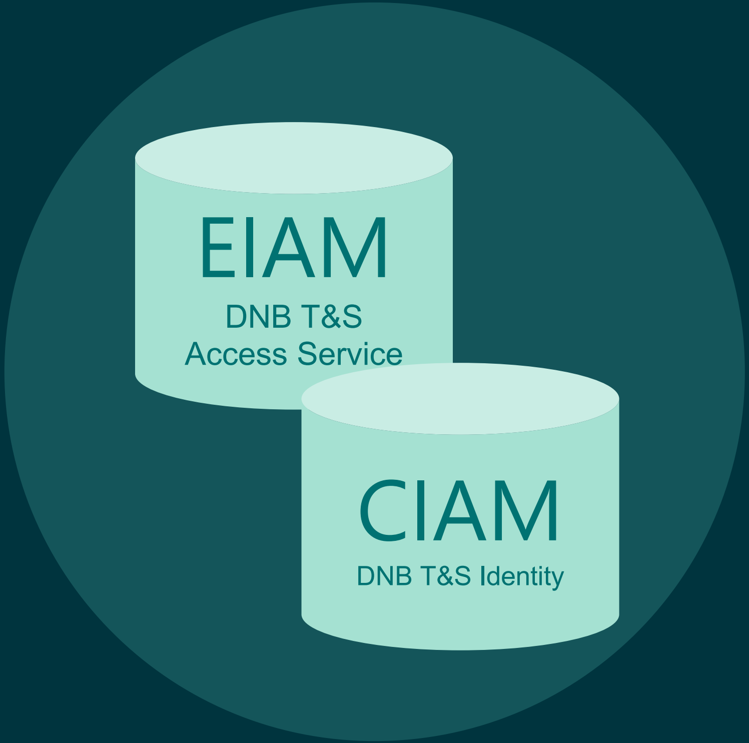
DNB

Enterprise & Customer IAM in DNB

Subject Lead EIAM, Stig B. Sivertsen
Product Manager CIAM, Sverre Tesdal Mjelde
Engineering Manager CIAM, Olov Pettersson
Lead Architect CIAM, Jan Winbrant

19. April 2024

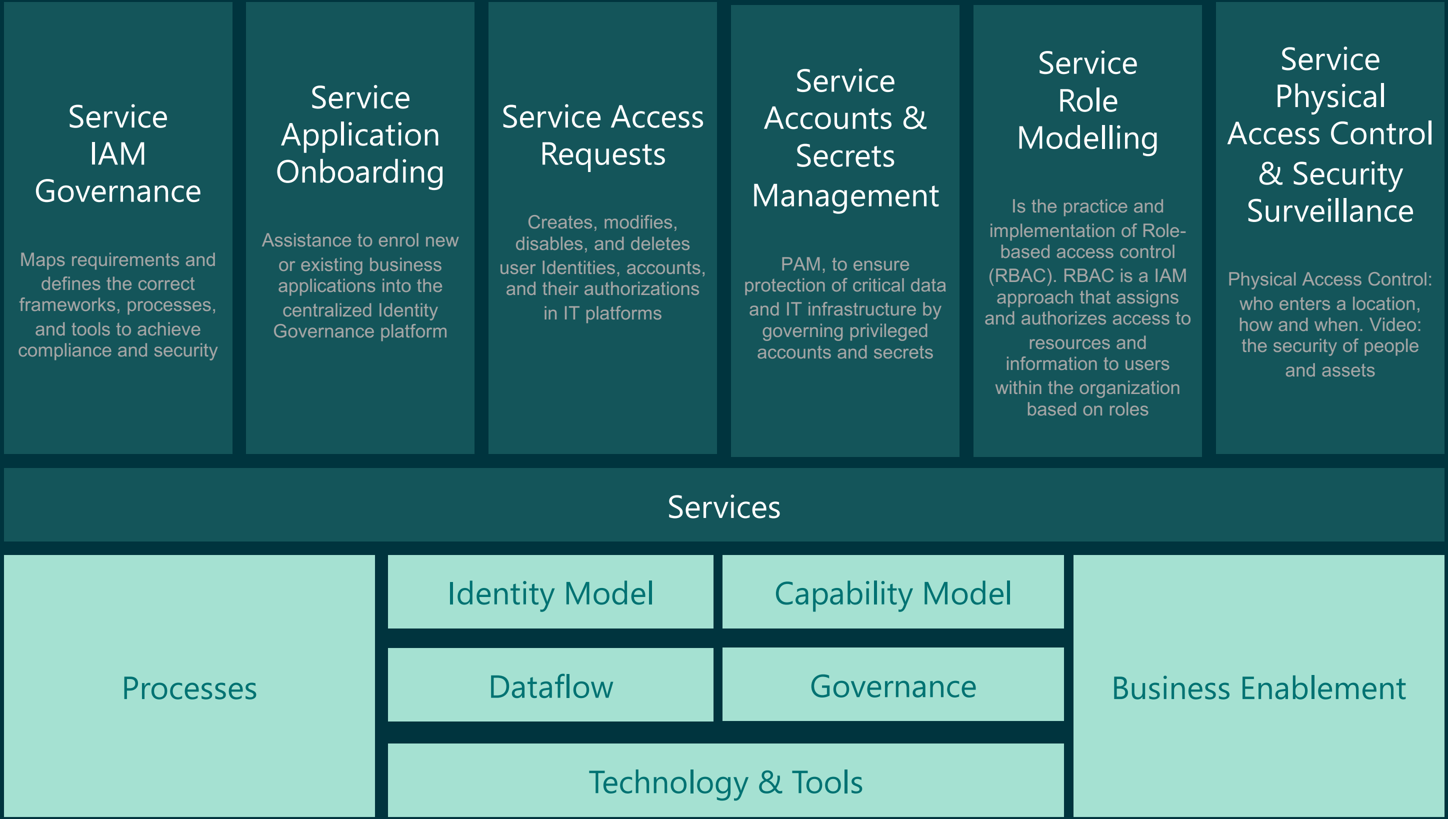
DNB IAM Organization



- Two large mature IAM environments
- **EIAM** is 42 employees divided into 5 teams
  - 800+ applications
  - 500.000+ entitlements
  - 32.400+ roles, of which more than 3300 roles are fully automated
  - Managed about 37.000 requests in 2023

- **CIAM** is about 45 employees divided into 4 product teams
  - About 2.000.000 authentications per day
  - About 30.000.000 PDP decisions per day
  - About 2.200.000 eSignings per year

Enterprise IAM Foundation



Service IAM Governance

Maps requirements and defines the correct frameworks, processes, and tools to achieve compliance and security

Service Application Onboarding

Assistance to enrol new or existing business applications into the centralized Identity Governance platform

Service Access Requests

Creates, modifies, disables, and deletes user Identities, accounts, and their authorizations in IT platforms

Service Accounts & Secrets Management

PAM, to ensure protection of critical data and IT infrastructure by governing privileged accounts and secrets

Service Role Modelling

Is the practice and implementation of Role-based access control (RBAC). RBAC is a IAM approach that assigns and authorizes access to resources and information to users within the organization based on roles

Service Physical Access Control & Security Surveillance

Physical Access Control: who enters a location, how and when. Video: the security of people and assets

Services

Processes

Identity Model

Capability Model

Dataflow

Governance

Technology & Tools

Business Enablement

DNB and the Identity Fabric

DNB T&S Identity

The Identity (CIAM) Family in DNB

Product areas

- Authentication
- Access Management
- Approval Systems
- BankID
- Identity proofing
- Authorization
- eSigning
- User and device Management

Our drivers

- Customer experience
- Enabler
- Modernization
- Efficiency
- Regulations

Authentication - example

Channels

WEB	App	API	S2S (system)

Authentication mechanisms

BankID	Other eIDs	DNB Biometric	Code device	Federation/SSO

Flows

Log-in	Transaction approval	Federation

Roles

Individuals	Corporate	Systems

Clients

Spare, Mobilbanken, Sbanken app, Bedrift, Cloud online bank, DNB Regnskap, Open Banking

Authentication - example

Channels

WEB

App

API

S2S (system)

Authentication mechanisms

BankID

Other eIDs

DNB Biometric

Code device

Federation/SSO

Flows

Log-in

Transaction approval

Federation

Roles

Individuals

Corporate

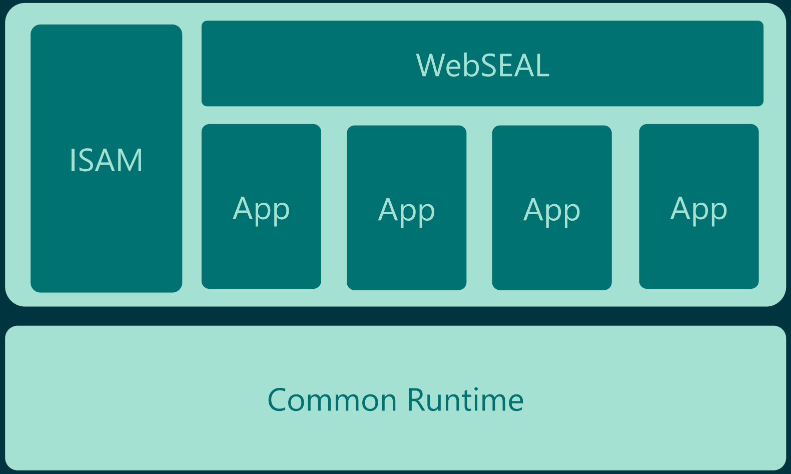
Systems

Clients

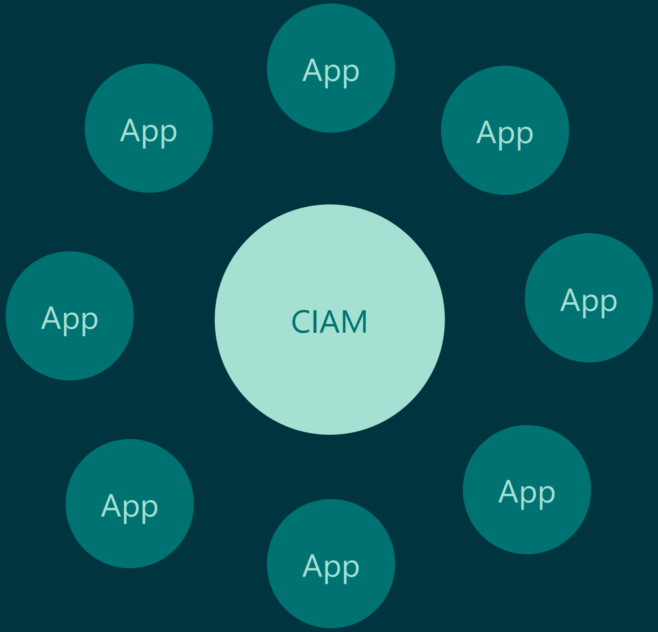
Spare, Mobilbanken, Sbanken app, Bedrift, Cloud online bank, DNB Regnskap, Open Banking

An organization in change

Legacy Identity Architecture



Cloud Identity Architecture



Challenges in the new world

A diverse and decentralized tech stack poses challenges for interoperability, governance and standardization

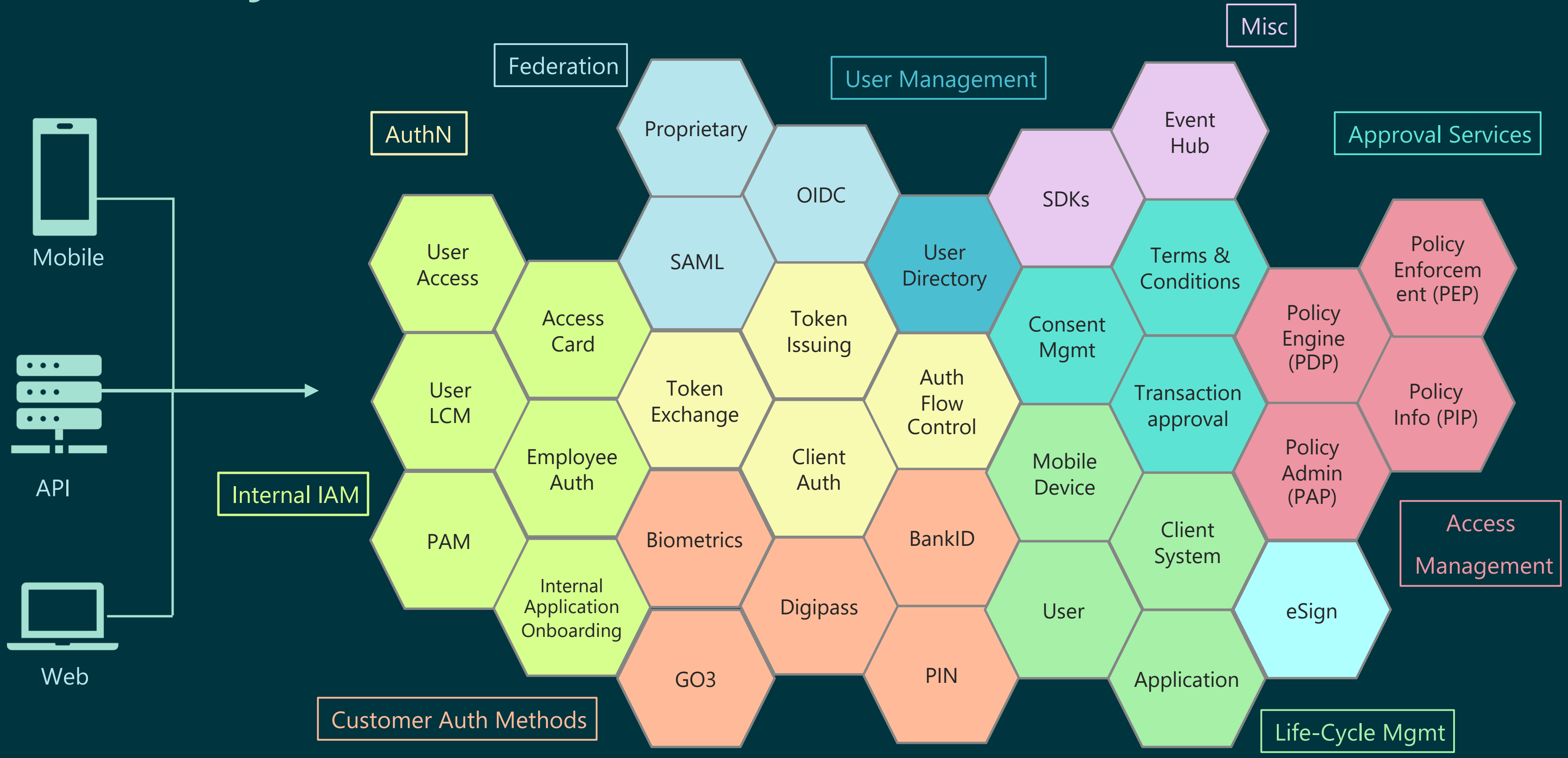
The only constant is change which means constant pressure for new use-cases and requirements

Different channels are created by different teams, but security and user journeys needs to harmonize across

Identity Architecture Principles

- Centralized - Decentralized
- Microservice architecture
- Composable capabilities that we can build use cases around
- Serve both users and machine identities
- Omni-channel
- Multi organizational
- Open standards
- Continuous change

Identity Fabric in DNB


Mobile

API

Web

AuthN

Federation

User Management

Misc

Approval Services

Internal IAM

Customer Auth Methods

Access Management

Life-Cycle Mgmt

User Access

User LCM

PAM

Access Card

Employee Auth

Internal Application Onboarding

Proprietary

SAML

OIDC

Token Exchange

Token Issuing

Client Auth

Auth Flow Control

Biometrics

GO3

Digipass

BankID

PIN

User Directory

SDKs

Event Hub

Consent Mgmt

Terms & Conditions

Transaction approval

Mobile Device

Client System

User

Application

Policy Engine (PDP)

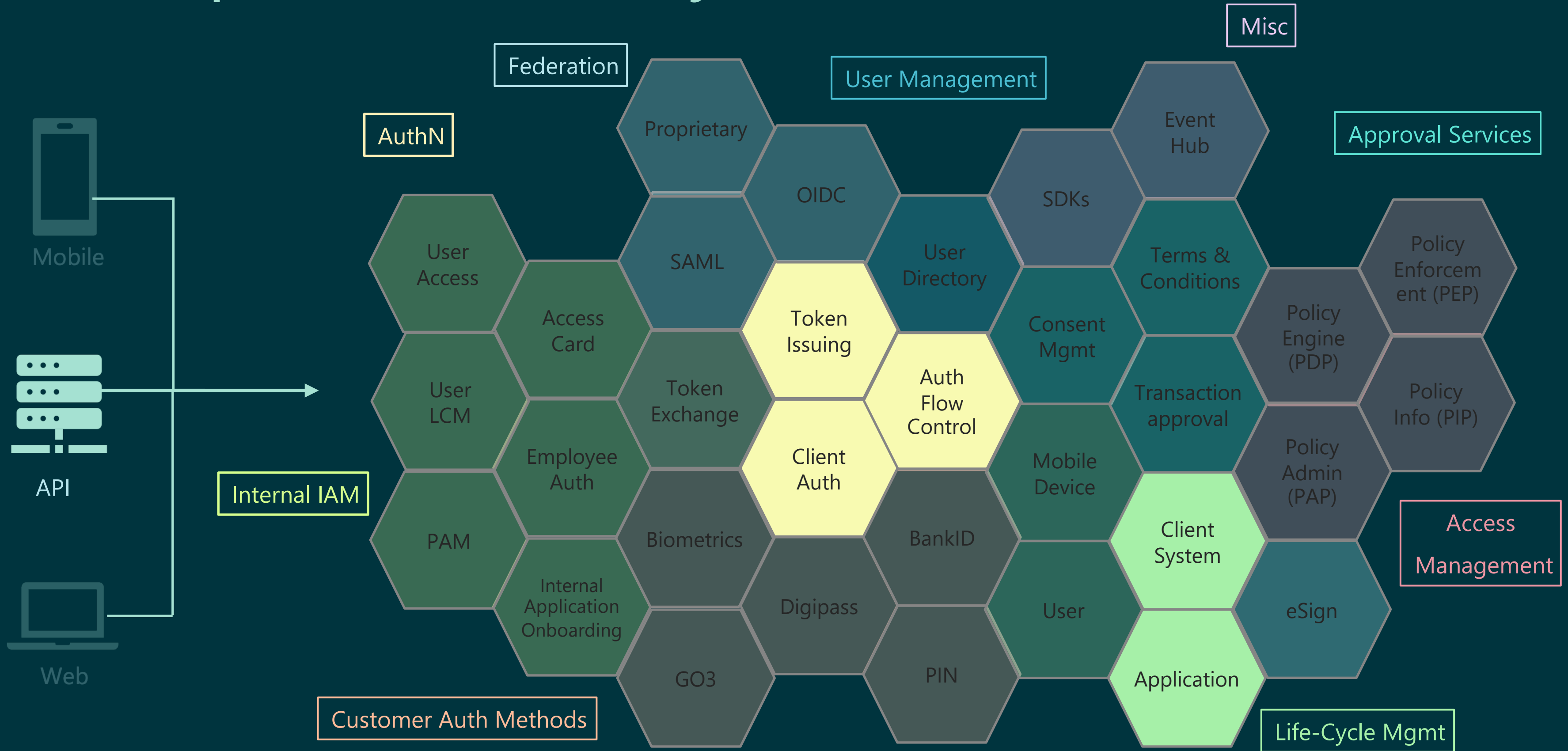
Policy Enforcement (PEP)

Policy Info (PIP)

Policy Admin (PAP)

eSign

Example use-case: system auth



Mobile

API

Web

AuthN

Federation

User Management

Misc

Approval Services

Internal IAM

Customer Auth Methods

Access Management

Life-Cycle Mgmt

User Access

Access Card

User LCM

Employee Auth

PAM

Internal Application Onboarding

Proprietary

SAML

Token Exchange

Biometrics

GO3

OIDC

Token Issuing

Client Auth

Digipass

User Directory

Auth Flow Control

BankID

PIN

SDKs

Consent Mgmt

Mobile Device

User

Event Hub

Terms & Conditions

Transaction approval

Client System

Application

Policy Engine (PDP)

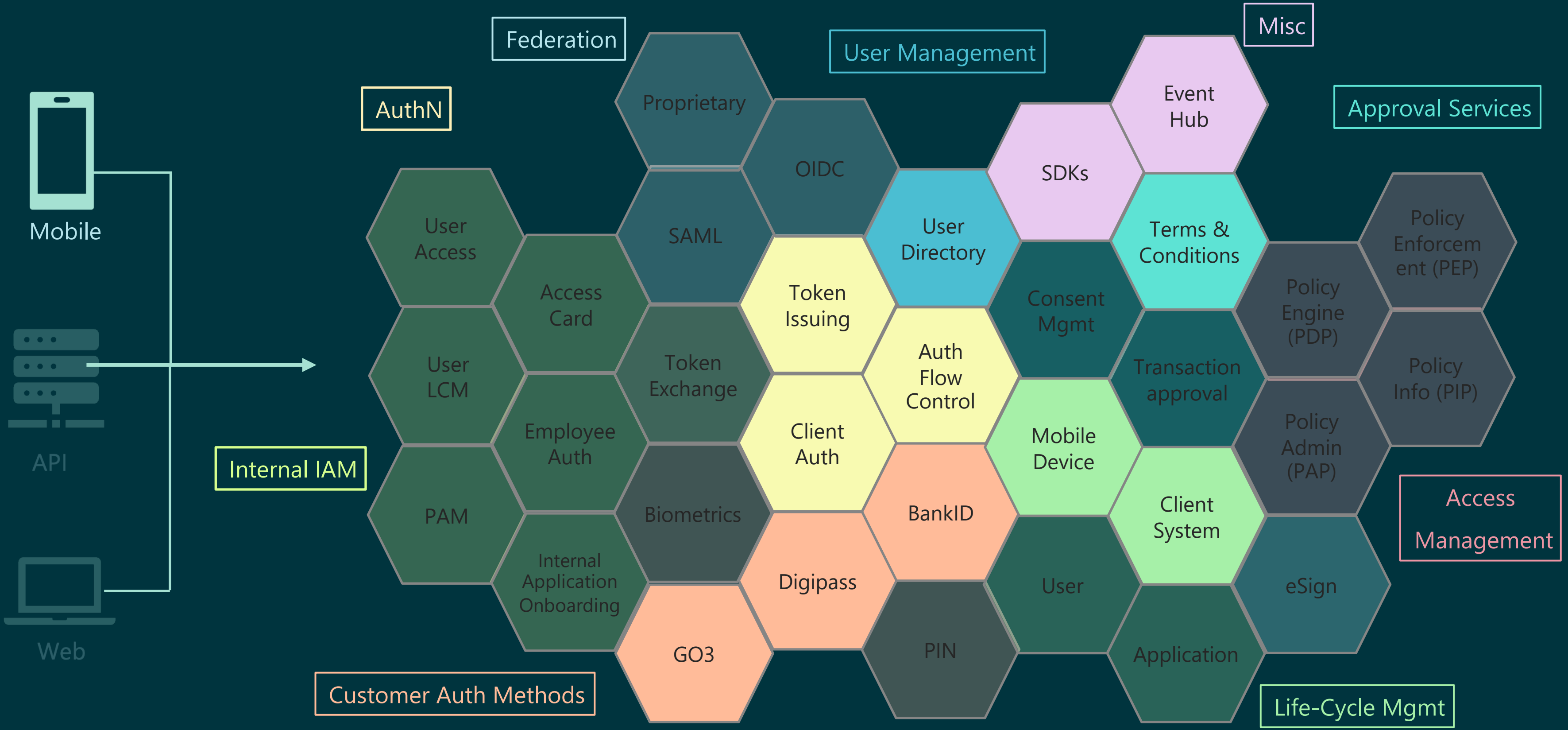
Policy Admin (PAP)

eSign

Policy Enforcement (PEP)

Policy Info (PIP)

Example use-case: mobile onboarding



Mobile

API

Web

AuthN

Federation

User Management

Misc

Approval Services

Internal IAM

Customer Auth Methods

Access Management

Life-Cycle Mgmt

Proprietary

OIDC

SAML

User Access

Access Card

User LCM

Employee Auth

PAM

Internal Application Onboarding

Token Exchange

Biometrics

GO3

Token Issuing

Client Auth

Digipass

User Directory

Auth Flow Control

BankID

PIN

SDKs

Event Hub

Terms & Conditions

Consent Mgmt

Transaction approval

Mobile Device

Client System

User

Application

Policy Enforcement (PEP)

Policy Engine (PDP)

Policy Info (PIP)

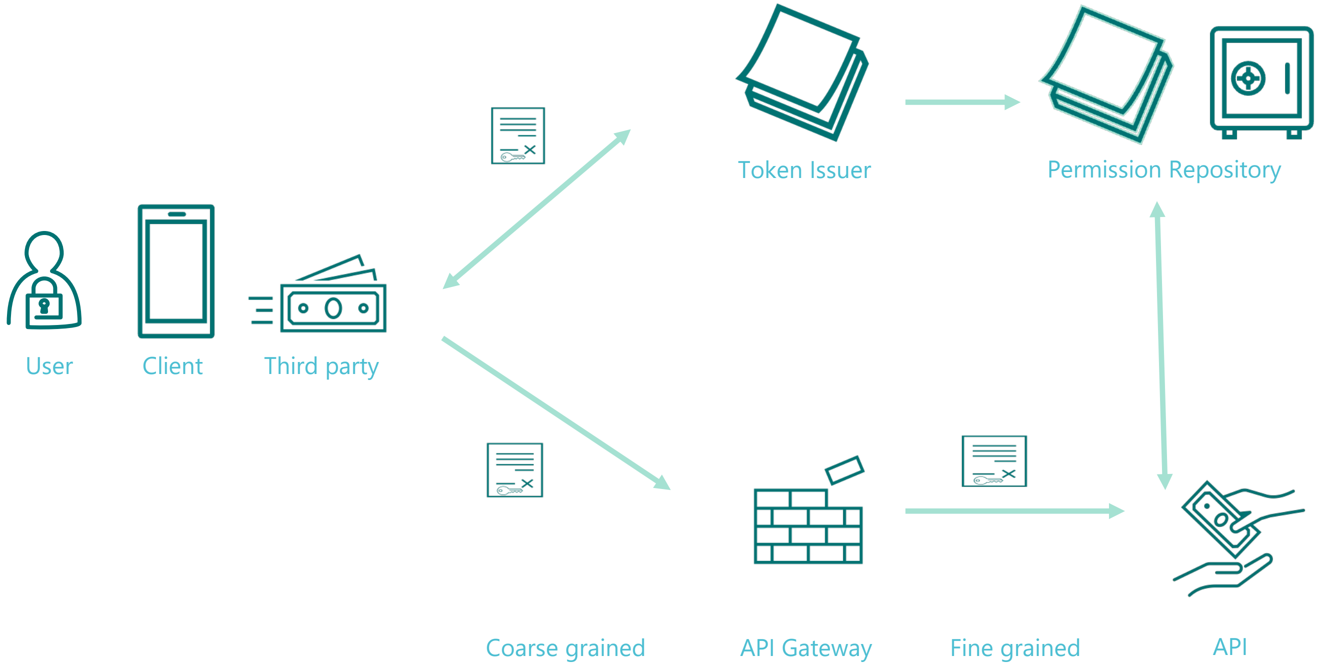
Policy Admin (PAP)

eSign

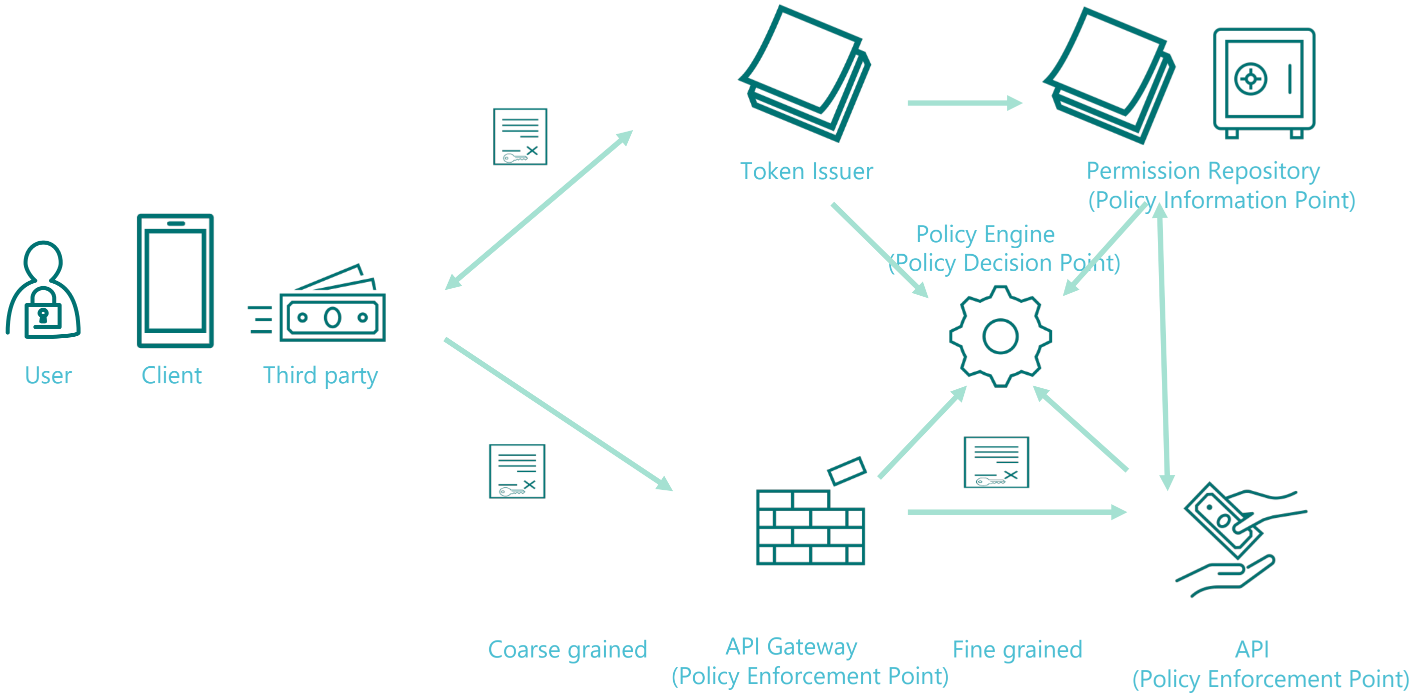
AuthZ - Standard OAuth 2.0

- Scopes (RFC6749)
  - Depends on client used and the request when tokens are issued
- Claims
  - Audience (“aud”)
  - Custom claims
- Token Exchange (RFC8693)
  - Embedded Access Token
  - Limits or increase access permissions
  - Add parties

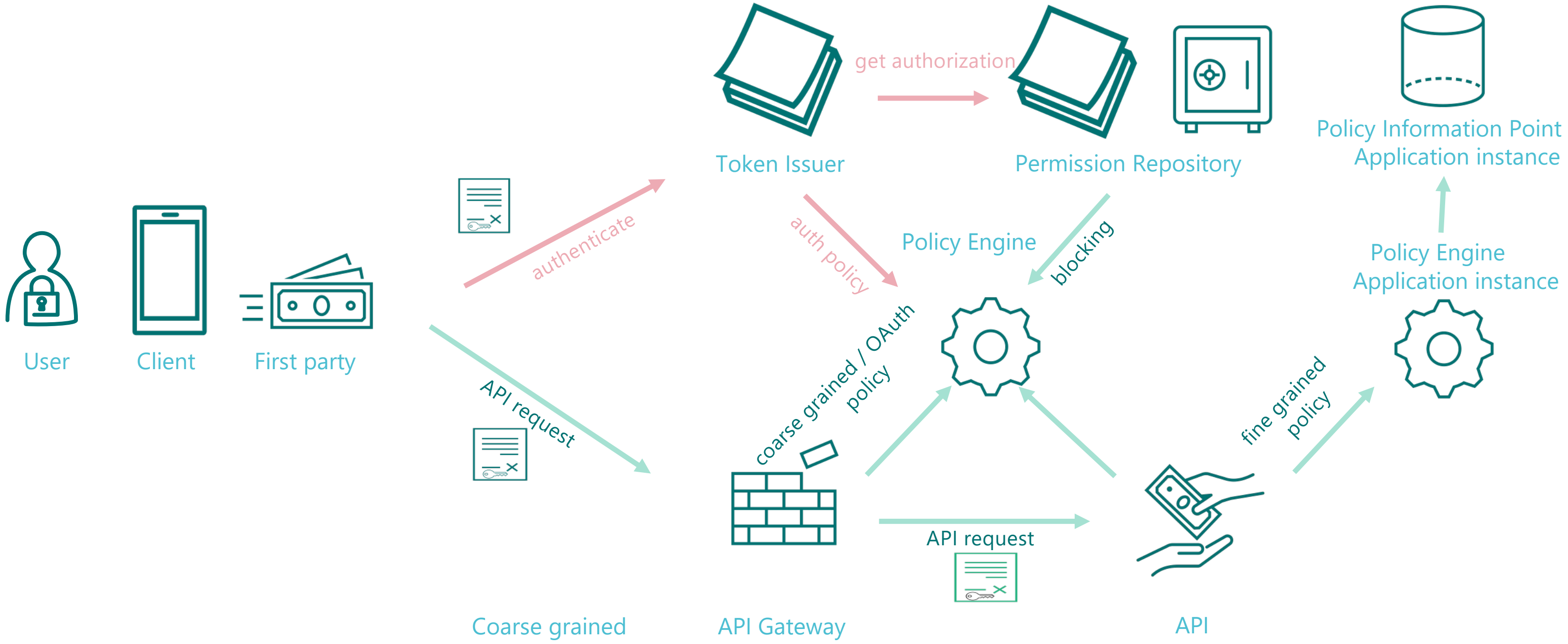
AuthZ - Multi-Layered



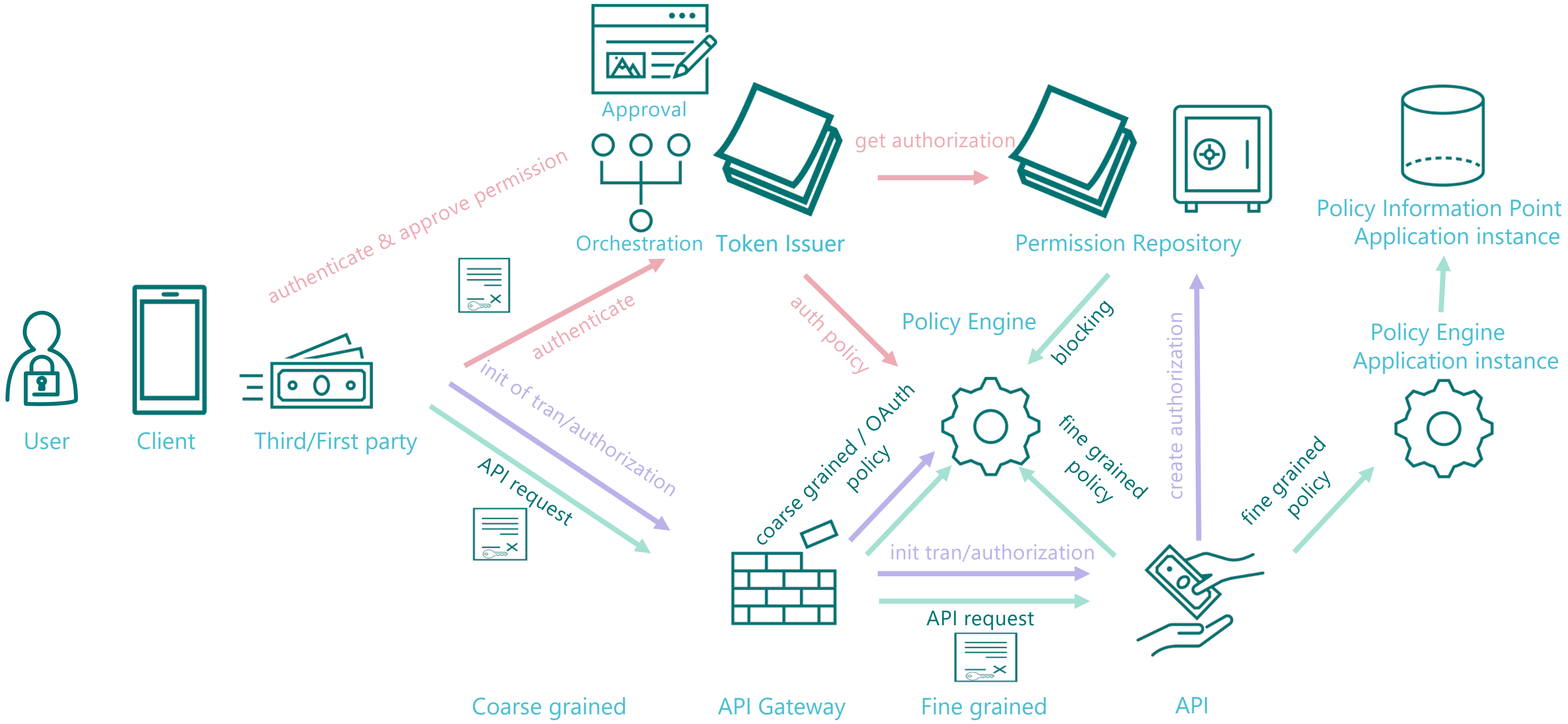
AuthZ - Policy Execution (PEP,PDP,PIP,PAP)



AuthZ – Application specific



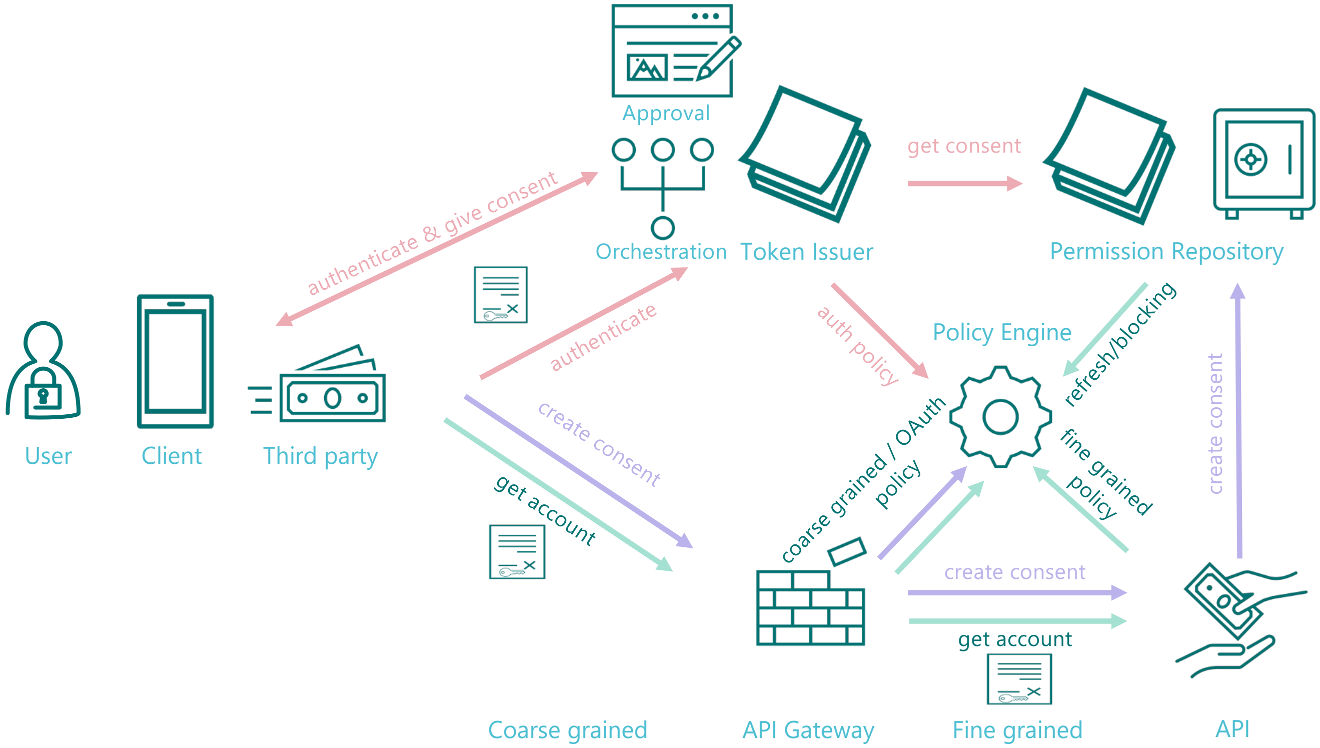
AuthZ – Combination of both Models (common/local)



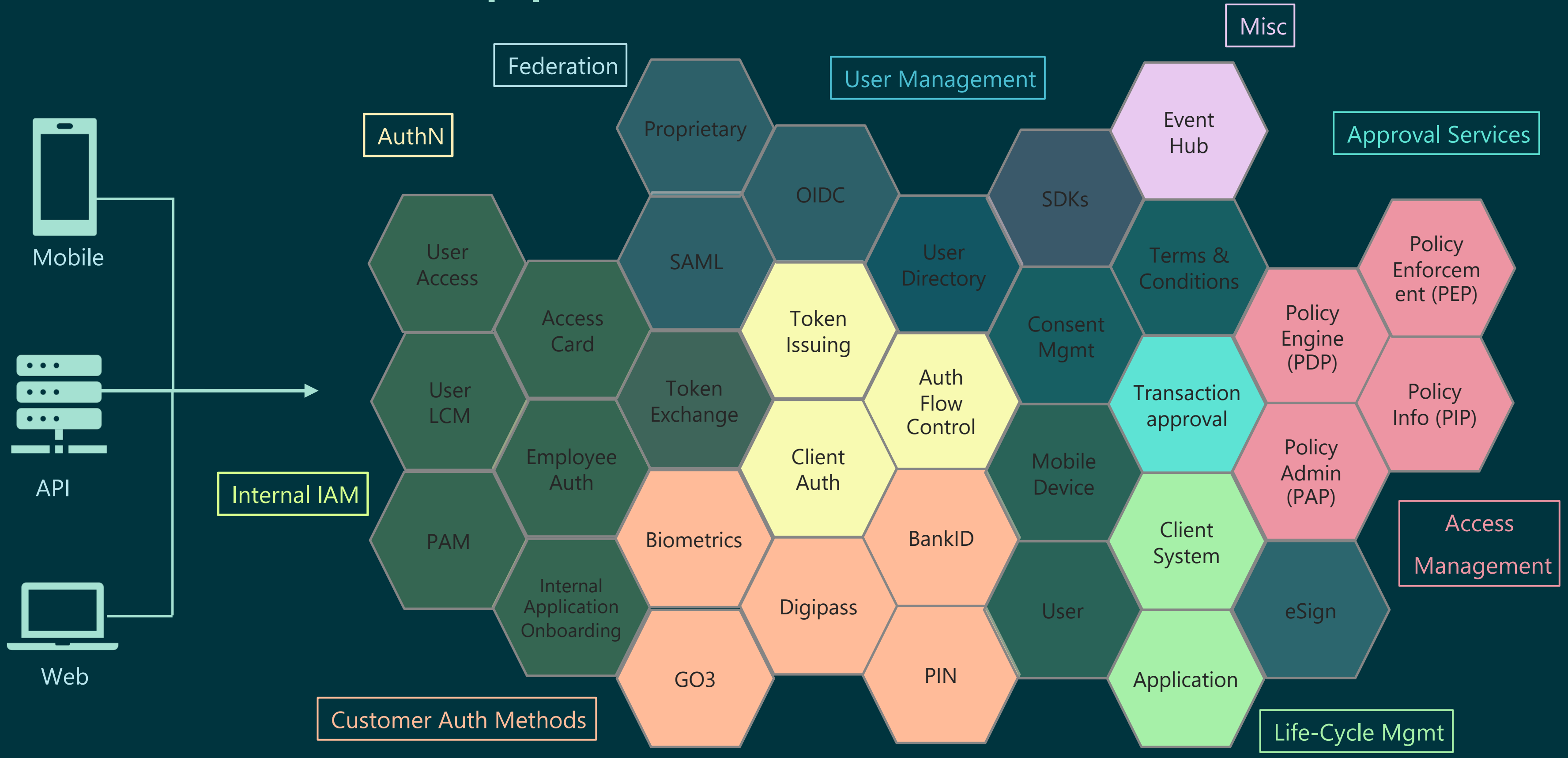
AuthZ - Permission Types (Policy Information Point)

- Generic delegation model – for delegating access to resources
- Consent – permission for (first/third) party to access user resources on behalf of the user
- Transaction Authorization – permission for (first/third) party to perform transactions on behalf of the user
- Impersonation – permission for a party (customer support) to impersonate the user and act on behalf of the user

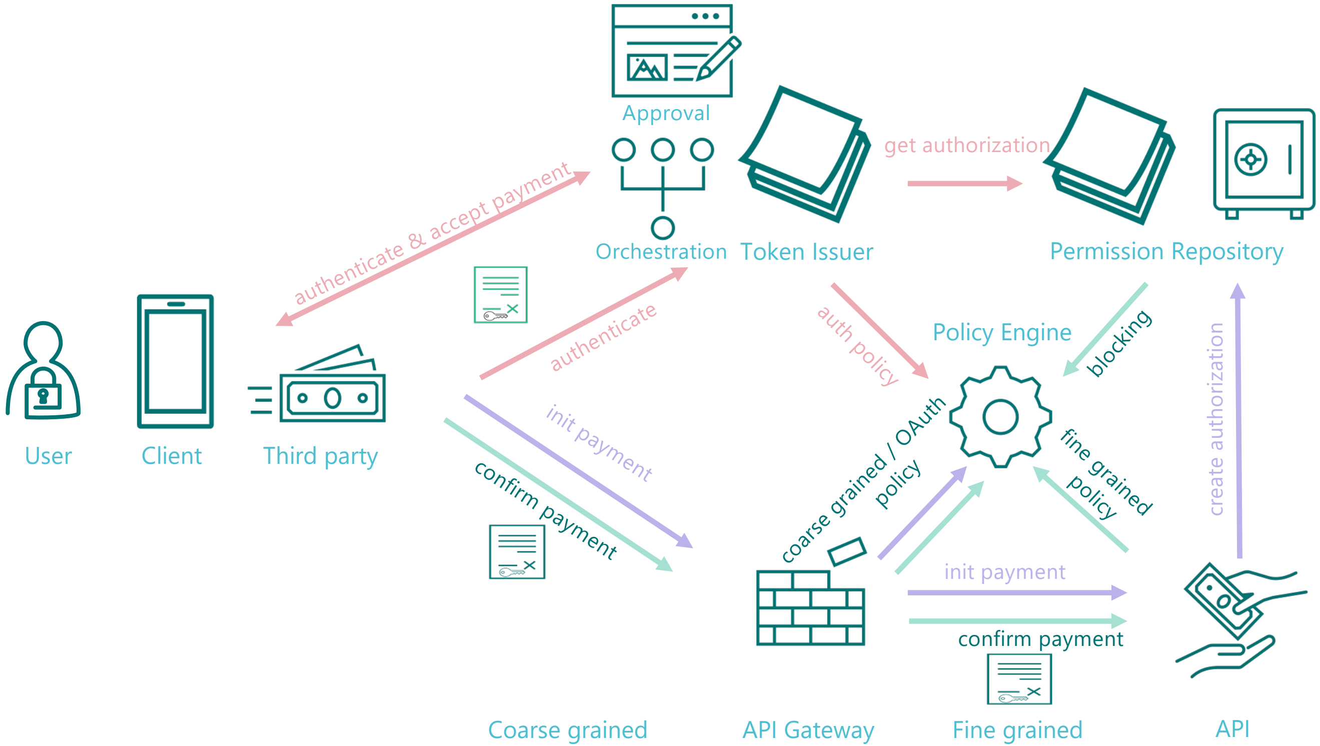
AuthZ – Consent (Account)



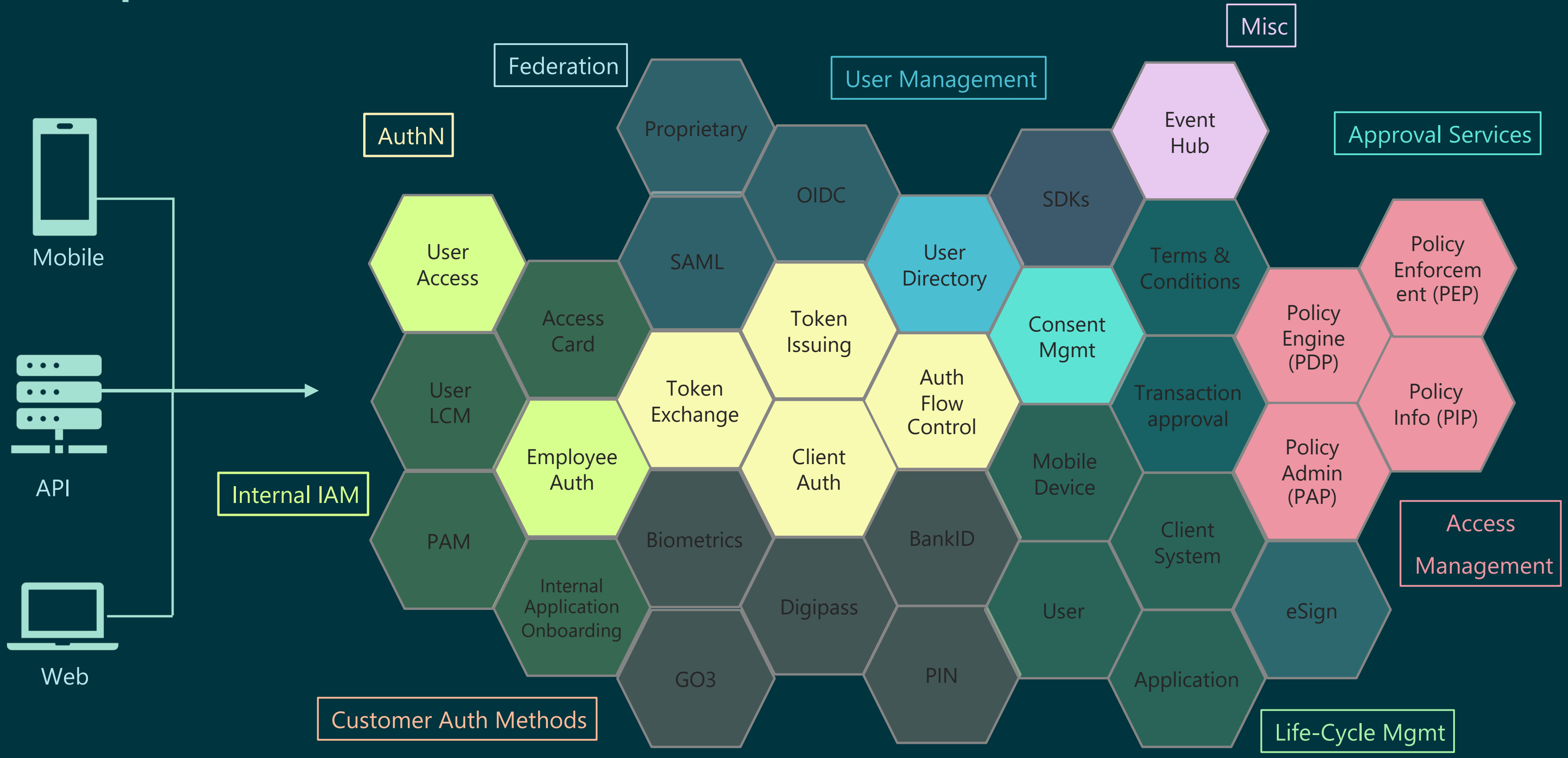
Transaction Approval



AuthZ – Transaction Authorization



Impersonation



Mobile

API

Web

AuthN

Federation

User Management

Misc

Approval Services

Internal IAM

Access Management

Customer Auth Methods

Life-Cycle Mgmt

Proprietary

OIDC

SAML

User Access

Access Card

Token Issuing

User Directory

SDKs

Event Hub

Terms & Conditions

Consent Mgmt

User LCM

Token Exchange

Auth Flow Control

Transaction approval

Policy Enforcement (PEP)

Policy Engine (PDP)

Policy Info (PIP)

Employee Auth

Client Auth

Mobile Device

Policy Admin (PAP)

PAM

Biometrics

BankID

Client System

Internal Application Onboarding

Digipass

User

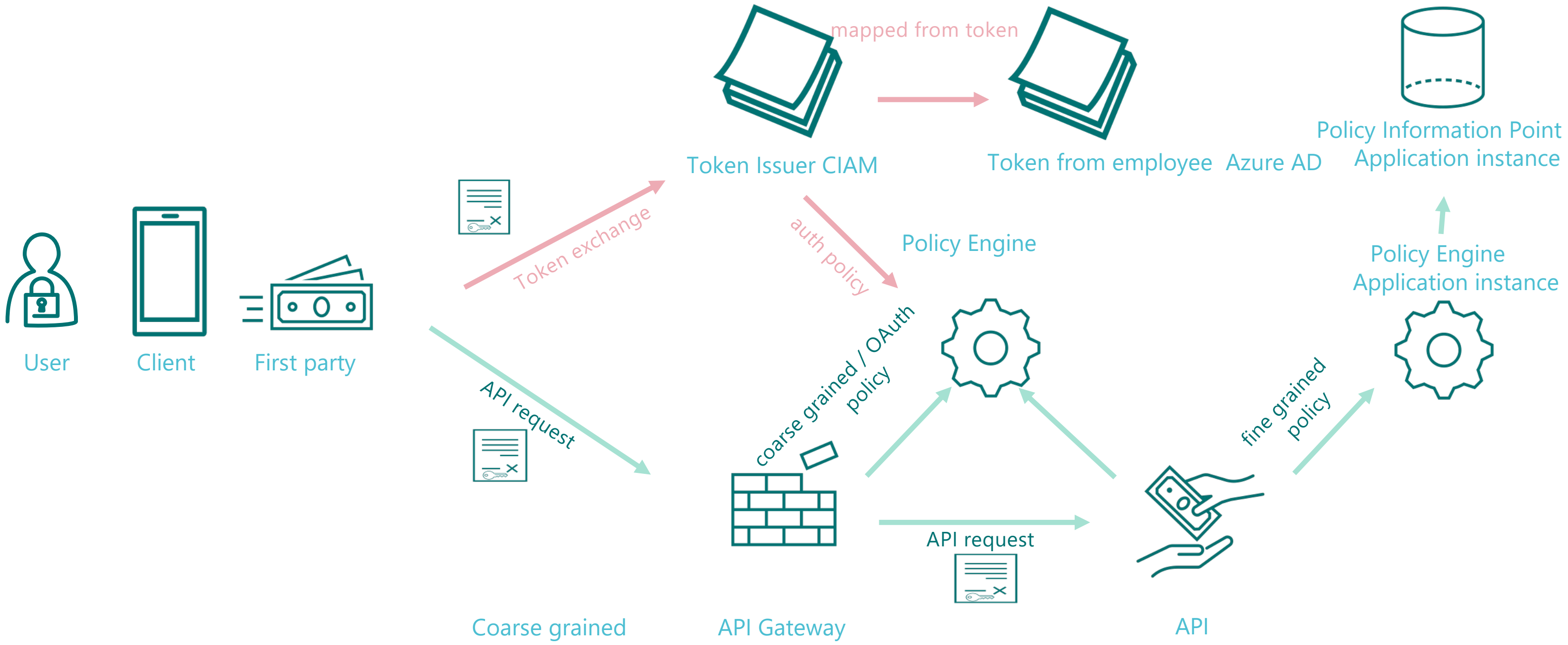
eSign

GO3

PIN

Application

AuthZ – Impersonation (employee)



Resources

- OAuth - https://oauth.net/2/
- OpenID Connect - https://openid.net/wg/connect/
- OpenID FAPI - https://openid.net/wg/fapi/
- OpenID Shared Signals - https://openid.net/wg/sharedsignals/
- OASIS XACML - https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml
- Open Policy Agent - https://www.openpolicyagent.org/

DNB