



IdM for insurance companies

Pekka Hagström

Agenda

- Introduction
 - RM5 Software Oy in brief
 - Current IAM situation in financial organizations
 - Identity and Access Management sub-systems
- Identity and Access Management challenges
- Solution model

RM5 Software Oy in brief – selected customers

- Finnish State Railways
 - *Centralized Entitlement Management in the Core of e-Infrastructure*
- AREK & Pensionskyddscentralen
 - *The Employment Pension Information of Every Finn is protected with RM5 IdM*
- Pension Fennia
 - *“RM5 Identity Management Solution Supports our Business Goals and Needs.”*
- TeliaSonera
 - *New Business with Entitlement Management*

Current situation in many financial organizations

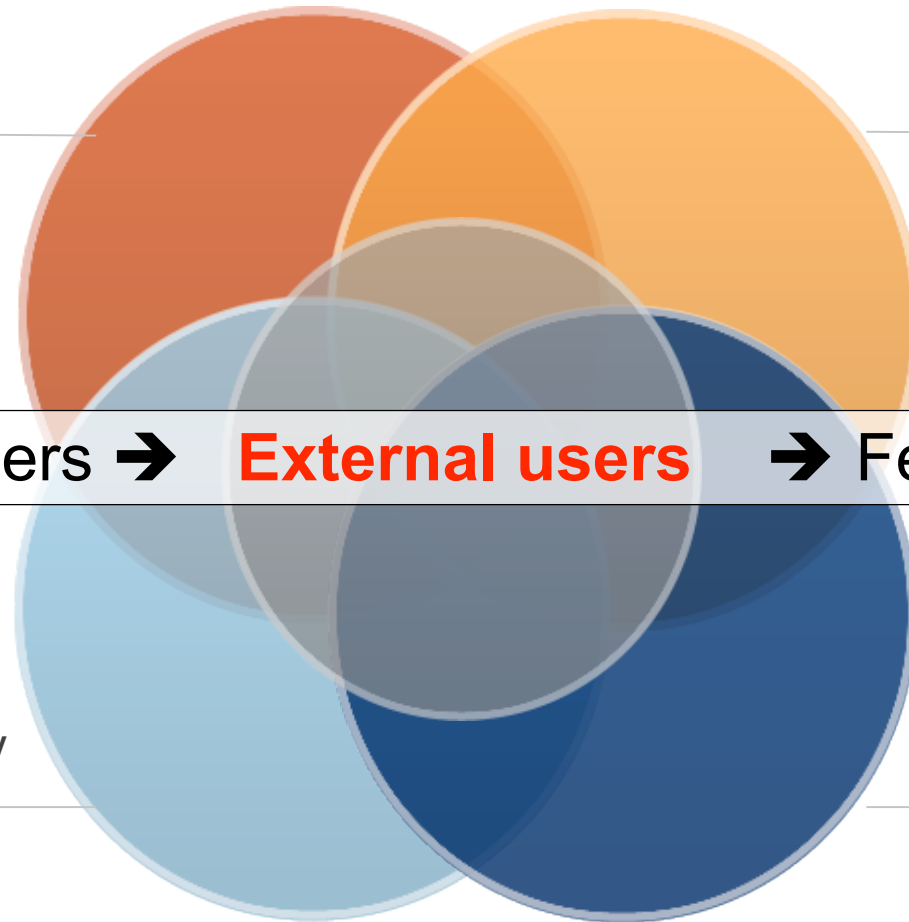
Large number of external stakeholders and users

Large number of services and confidential customer data

Internal users → **External users** → Federated identities

Complex entitlement policy requirements

Frequent change in entitlements



Identity and Access Management sub-systems

Identity Management

Administration

Propagation

Audit

IdM repository

Access Control

Login

Session
Management

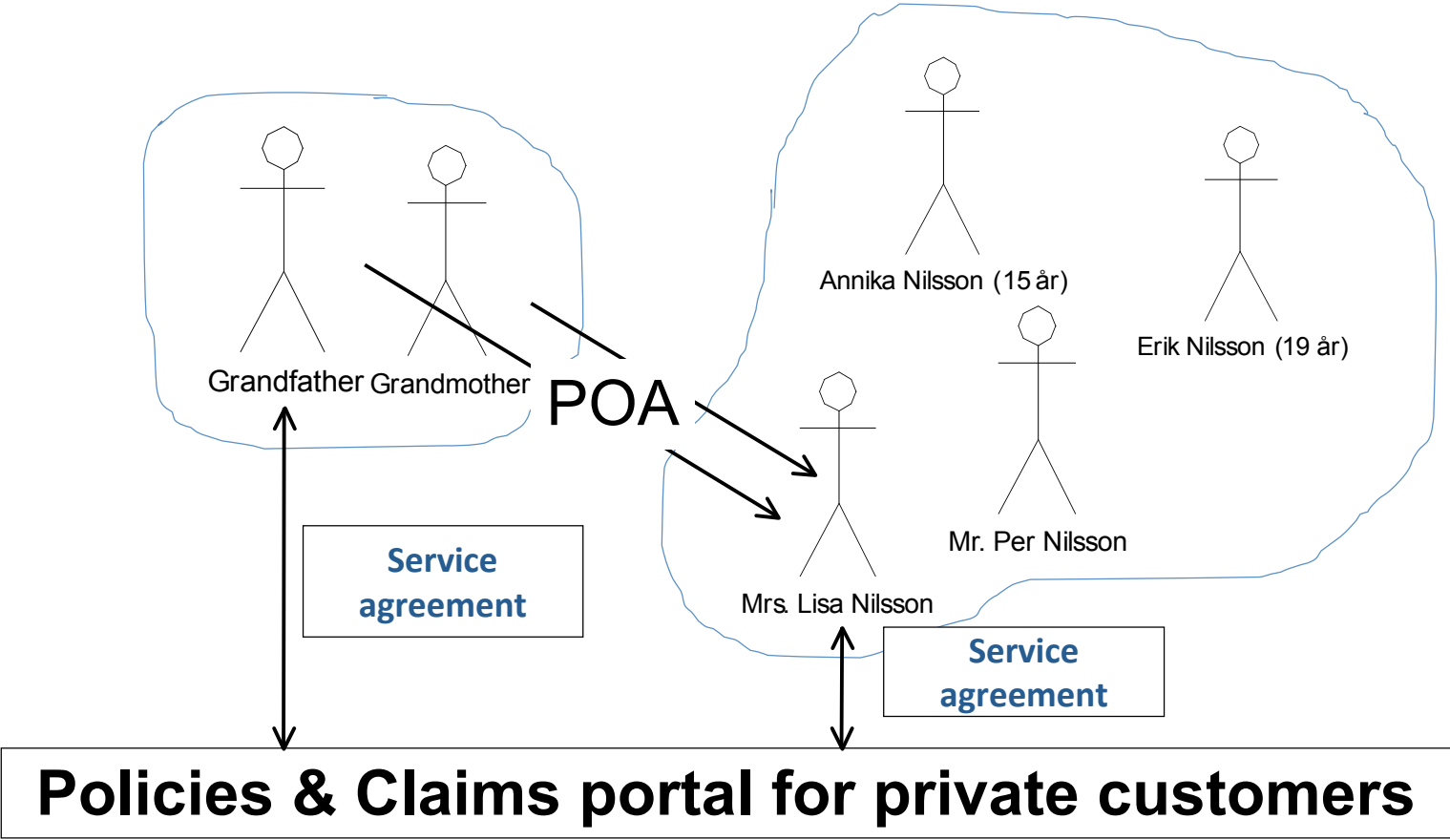
Authorization

Accounting

Agenda

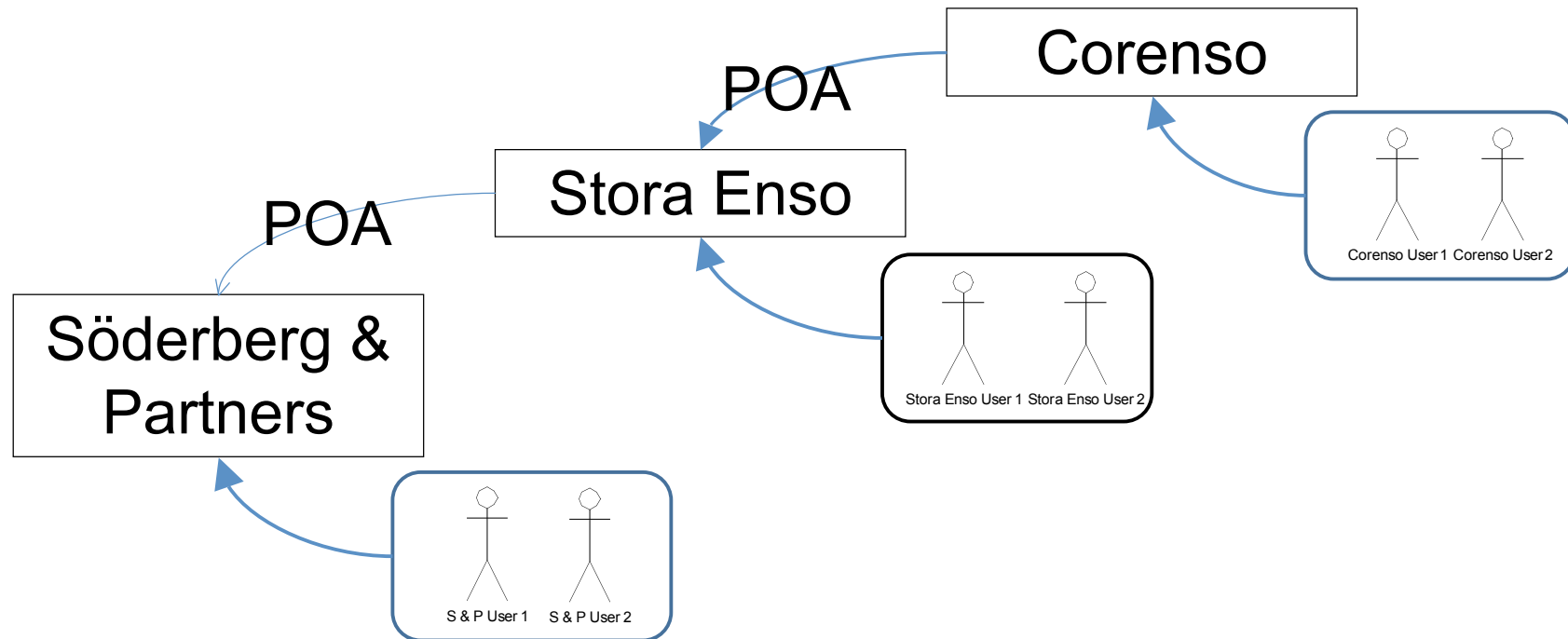
- Introduction
- Identity management challenges
 - Large number of external stakeholders and users
 - Large number of services and large amount of confidential data
 - Complex authorization requirements
 - Frequent changes in entitlements
- Solution model

Large number of external stakeholders and users



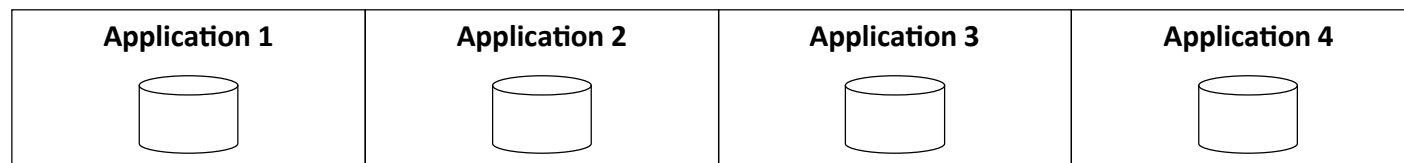
Large number of external stakeholders and users

- organizational customer



Policies & Claims portal for organizations

Base systems



Complex authorization requirements

- User entitlements must align:
 - With the service contracts
 - With the power of attorneys
 - With any other constraints
- Example:
 - Corenso grants a Power of Attorney to Stora Enso with the following constraints; policies 1, 2, 3 and 7 + 'Property'- and 'Liabilities'- line of businesses + allows Stora Enso to transfer the POA to a Broker.
 - Stora Enso transfers Corenso's POA to Söderberg & Partners for policies 1 and 2 + 'Property'-lob
 - Söderberg & Partners has a service agreement which includes 'policy admin role'. Thus, user may get an entitlement to administrate Corenso's policies 1 and 2 within 'Property'-lob

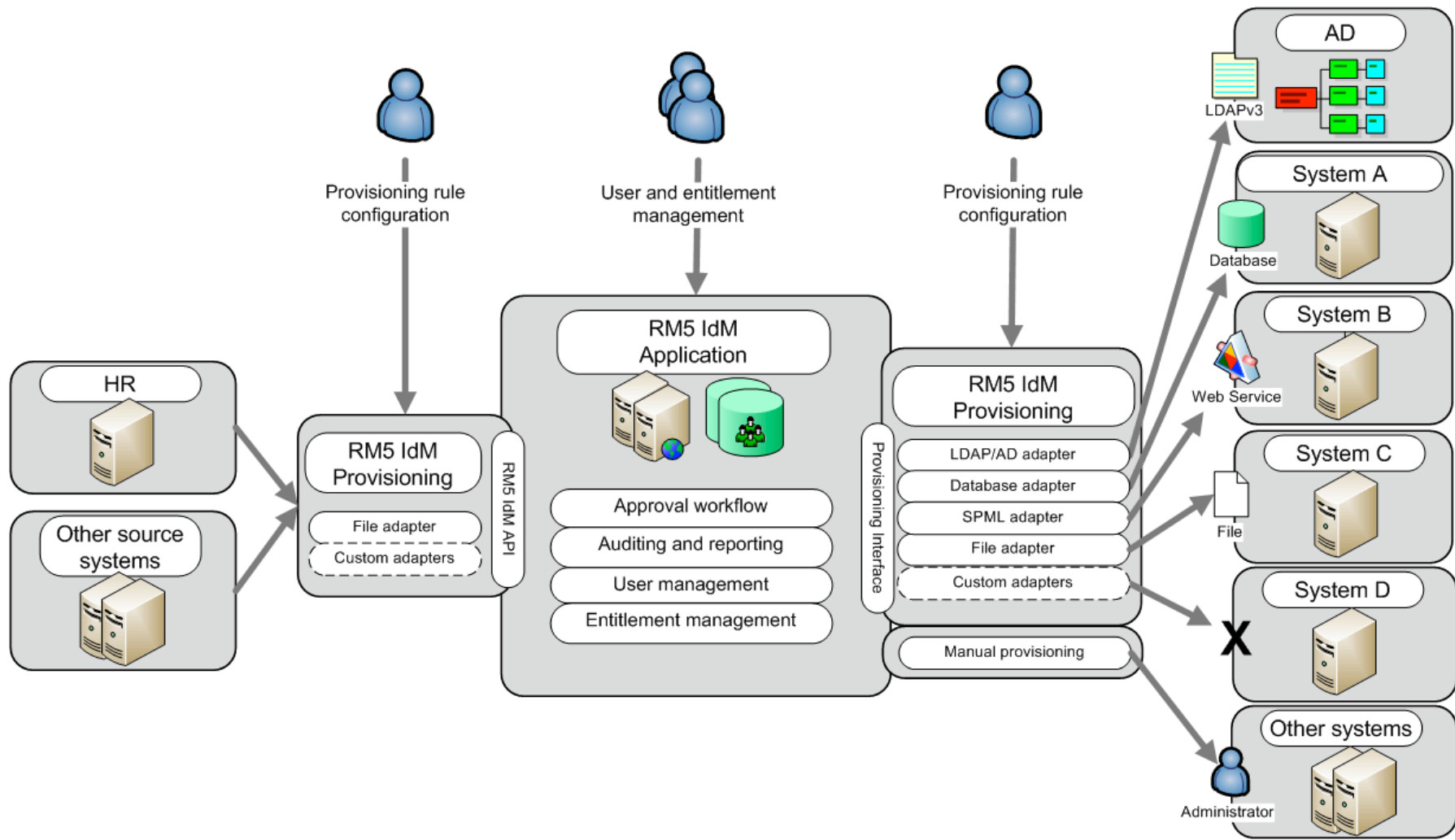
Summary

- **Power of attorneys** specify the scope within an agent can act on behalf of a principal.
- Principals can allow the agent to **transfer** a POA to another agent but the transferred POA cannot overrun the original POA's constraints
- Support for login with **BankIDs** and selection of user context
- Support for **Multiple service providers** (a financial organization is often a group of companies)
- Support for **Multiple customer ids** (as customers are created with different unique identifies in different base systems)
- Support for full **delegation** of entitlement administration

Agenda

- Introduction
- Identity and Access Management challenges
- Solution model
 - Reference architecture
 - Conceptual IdM data model
 - Authentication & Authorization services

Reference architecture



Business-centric IdM model

Service Consumer

Service Provider



(Customers, brokers, partners, resellers, etc)

(Parent company, subsidiaries, partners)

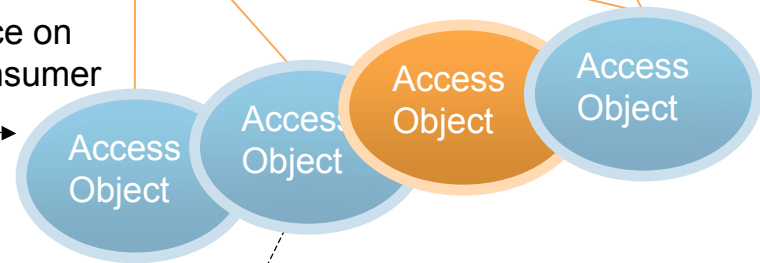
Delegation of permissions



Service agreement is a 'framework' within a stakeholder may delegate entitlements



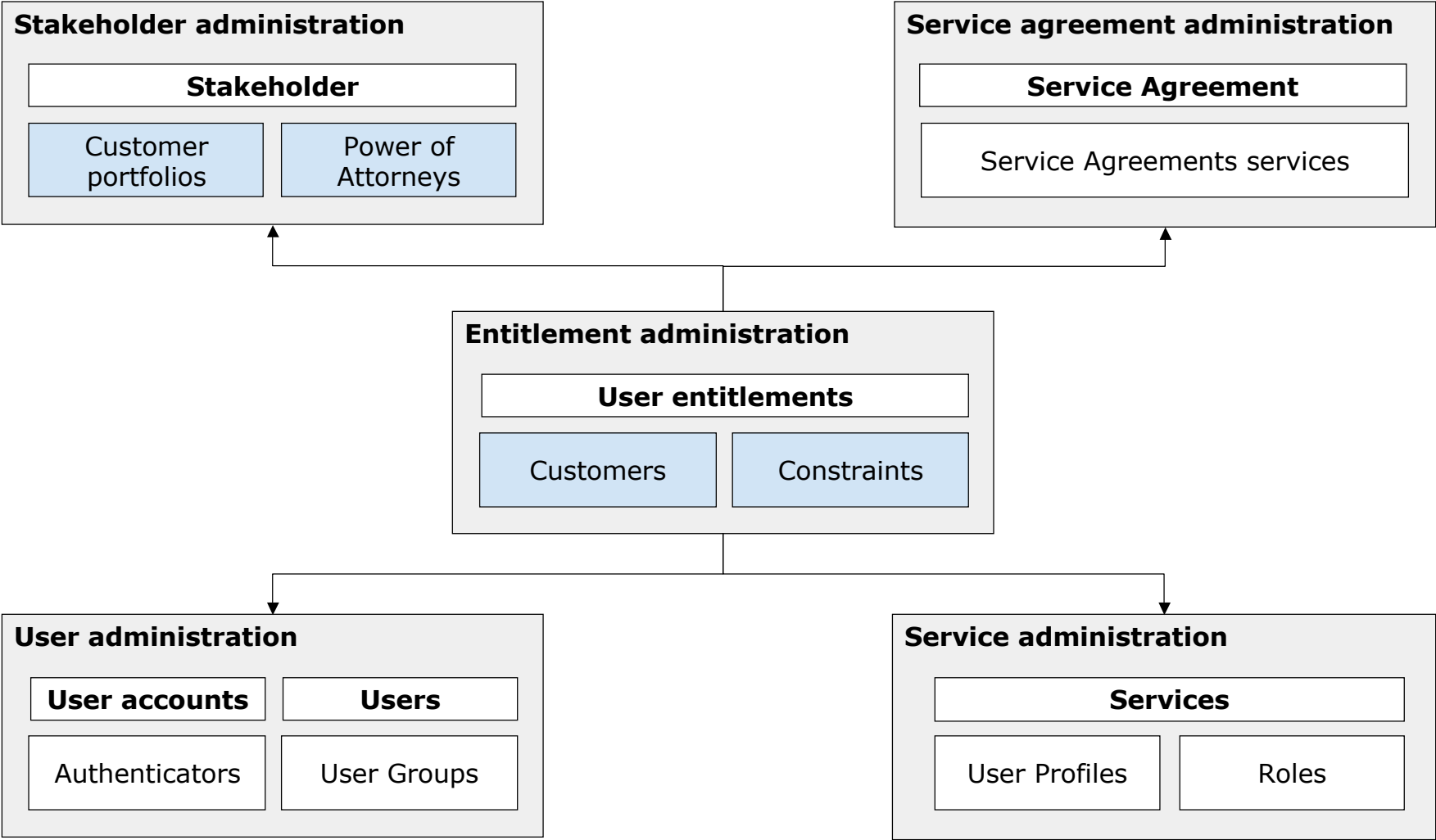
User operates a service on behalf of the service consumer



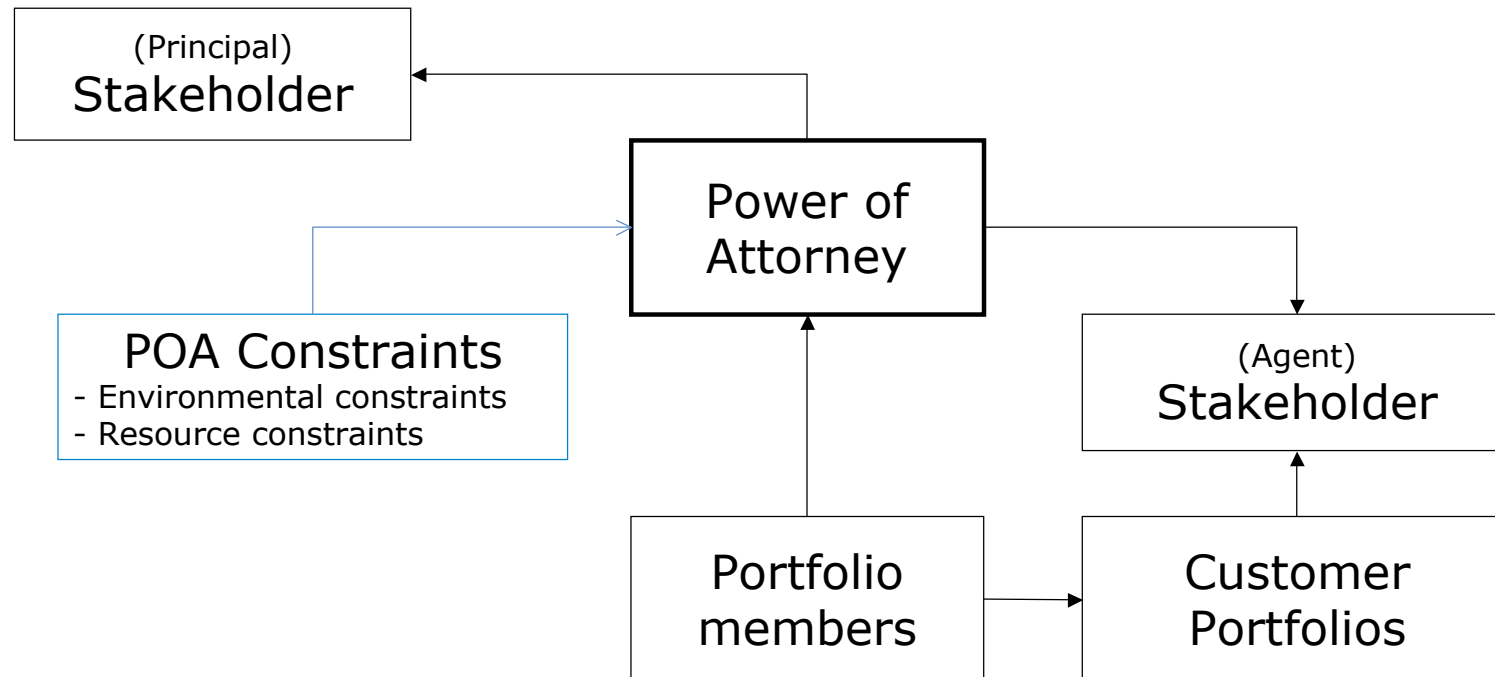
User (i.e. Agent)

Profiles, protection roles, applications etc

RM5 IdM – conceptual identity model



RM5 IdM – Stakeholder administration



(Principal) Stakeholders:

Brokers' customers, Subsidiaries, Private customers

(Agent) Stakeholders:

Brokers, Group companies, Private persons, 'partners'

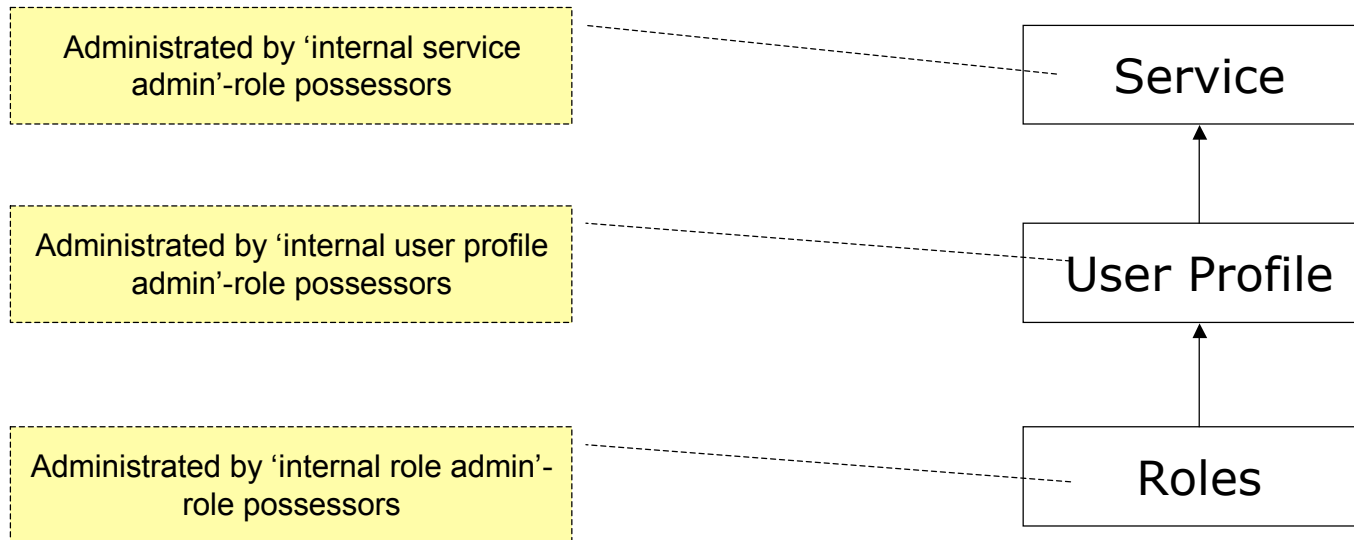
Power Of Attorneys:

Customer's POA to a Broker, Subsidiary's POA to mother Company, private persons POA to an other private person

Customer portfolios:

Broker's portfolios with customers, Group company's portfolio with subsidiaries

RM5 IdM – Service administration



Services:

Portal for private customers, Portal for Brokers, Portal for internal users, IdM for External stakeholders, IdM for Brokers, IdM for Internal administrators

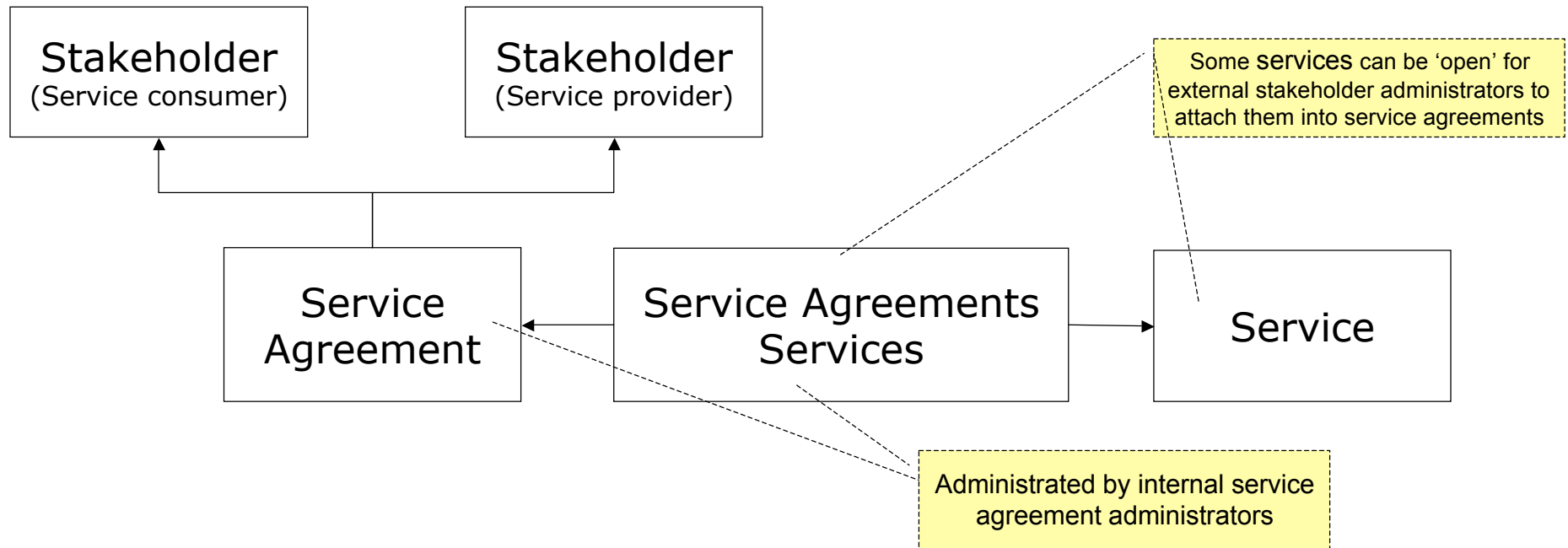
User profiles:

External risk manager, Brokers claims admin, External user admin, Internal POA Admin, Broker portfolio admin

Roles:

Broker claims reader, Internal claims reader, external claims reader, External entitlement admin, Internal service admin

RM5 IdM – Service agreement administration



Service providers:

Parent company & subsidiaries, External service providers (federated identities to external services)

Service consumers:

Internal & external stakeholders

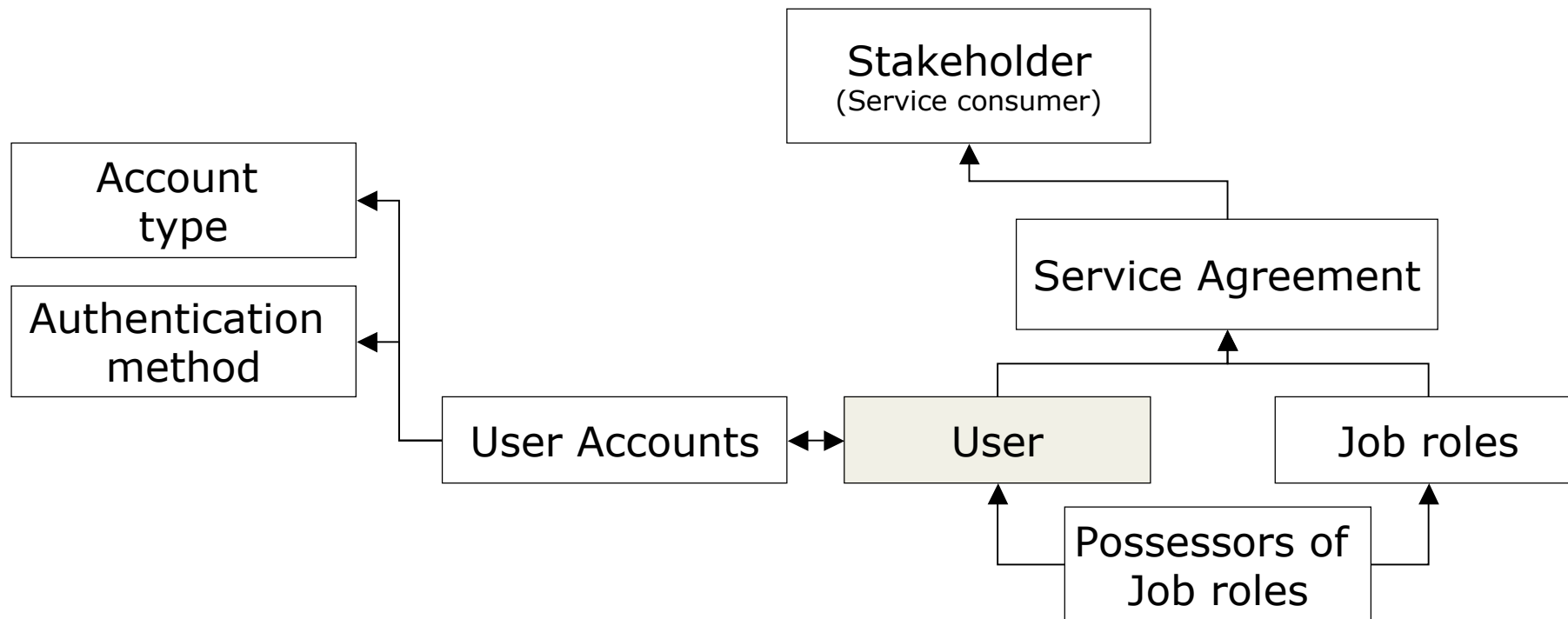
Service agreement:

Frame agreement between service providers and service consumers

Service Agreements services:

Services attached to service agreements, i.e. defines the services (user profiles and roles) the service consumer is allowed to use

RM5 IdM – User administration



User account:

Attachment of user credential to a user. Example, a person's BankID is attached to a user.

User account type:

External: BankIDs, certificates, etc
Internal: Active Directory, LDAP,s IdM, etc

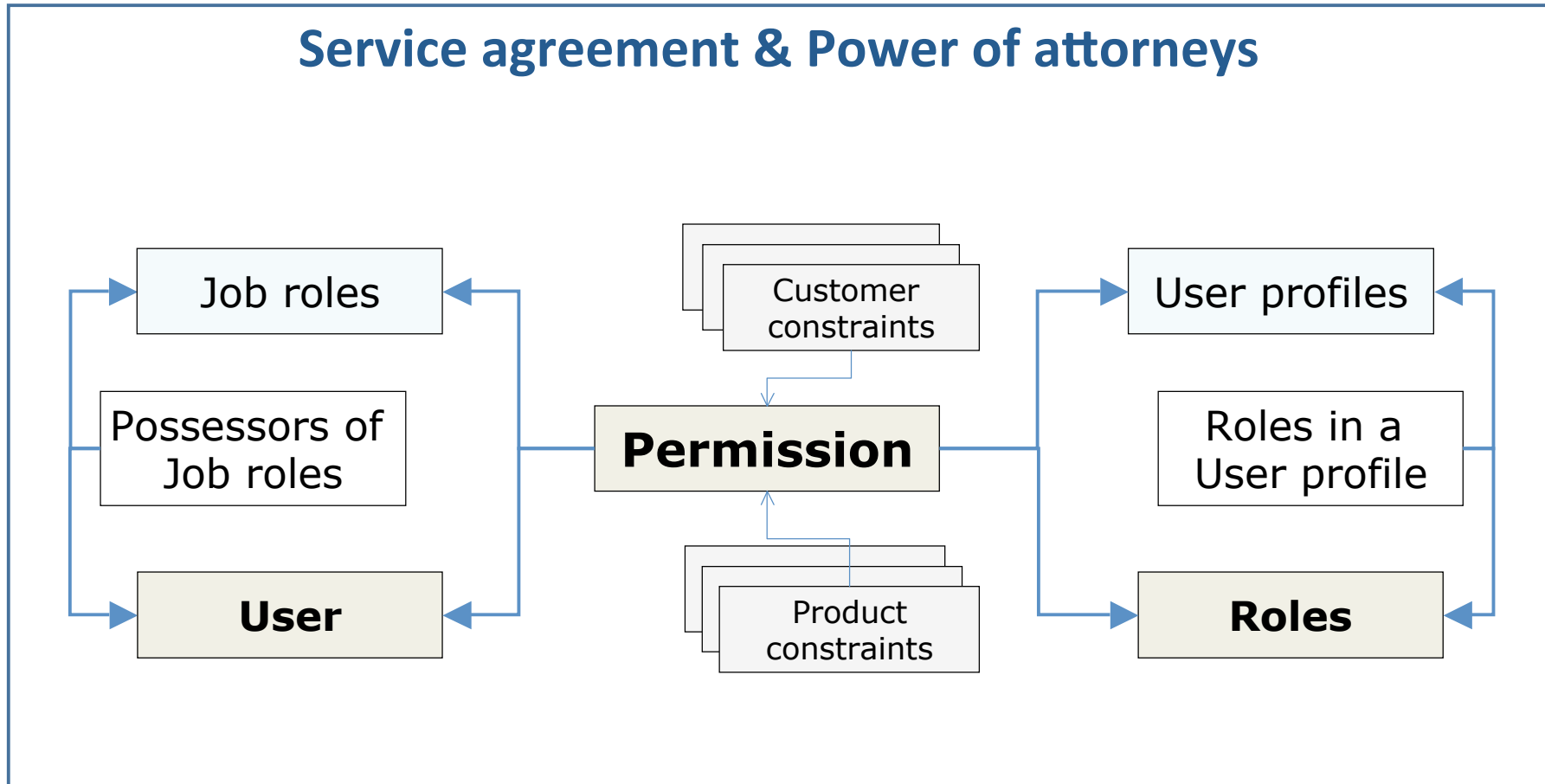
Authentication method:

Specifies the credibility of the user account authenticator – can be used at access control

User and User groups :

Individual users and groups of users within a service agreement. Service agreement is the framework for user entitlements – no user can have broader entitlements than the service agreement the user is attached to

RM5 IdM – permission administration



The End

- Business oriented challenges
- Reference architecture
- IdM entities

RM **5** software