Universal applications of mobile identities

Application of user profiles for identity based service interaction

Henning Olesen, CMI, Copenhagen Institute of Technology (AAU), Ballerup, DK
Josef Noll, UniK/UiO, Univ. Graduate Center/Univ. of Oslo, Kjeller, NO
Mario Hoffmann, Fraunhofer SIT, Darmstadt, GE

Introduction

- WWRF announced the “I-centric” approach back in 2000
- Some FP5, various FP6 and many FP7 projects address user preferences
  - Youngster, ePerSpace, E2R, SIMPLICITY, SMS, Daidalos, Spice, MobiLife, Magnet Beyond, PRIME, PrimeLife....
- Early implementations are available from various research labs
- User profile closely related to ID management, context awareness, device environment
- Now is the time for coordination and standardisation

User profile

What is a user profile?

"The total set of user-related information, preferences, rules and settings, which affects the way in which a user experiences terminals, devices and services" [ETSI 2005a]

Main types of user interaction:

Interaction with other users (peer-to-peer, communities, etc.),

Interaction with a "system" or a device

Interaction with an external service provider offering services to the user

The user profile (together with context information) can facilitate this interaction: An enabler for service adaptation and more relevant and user-friendly services.

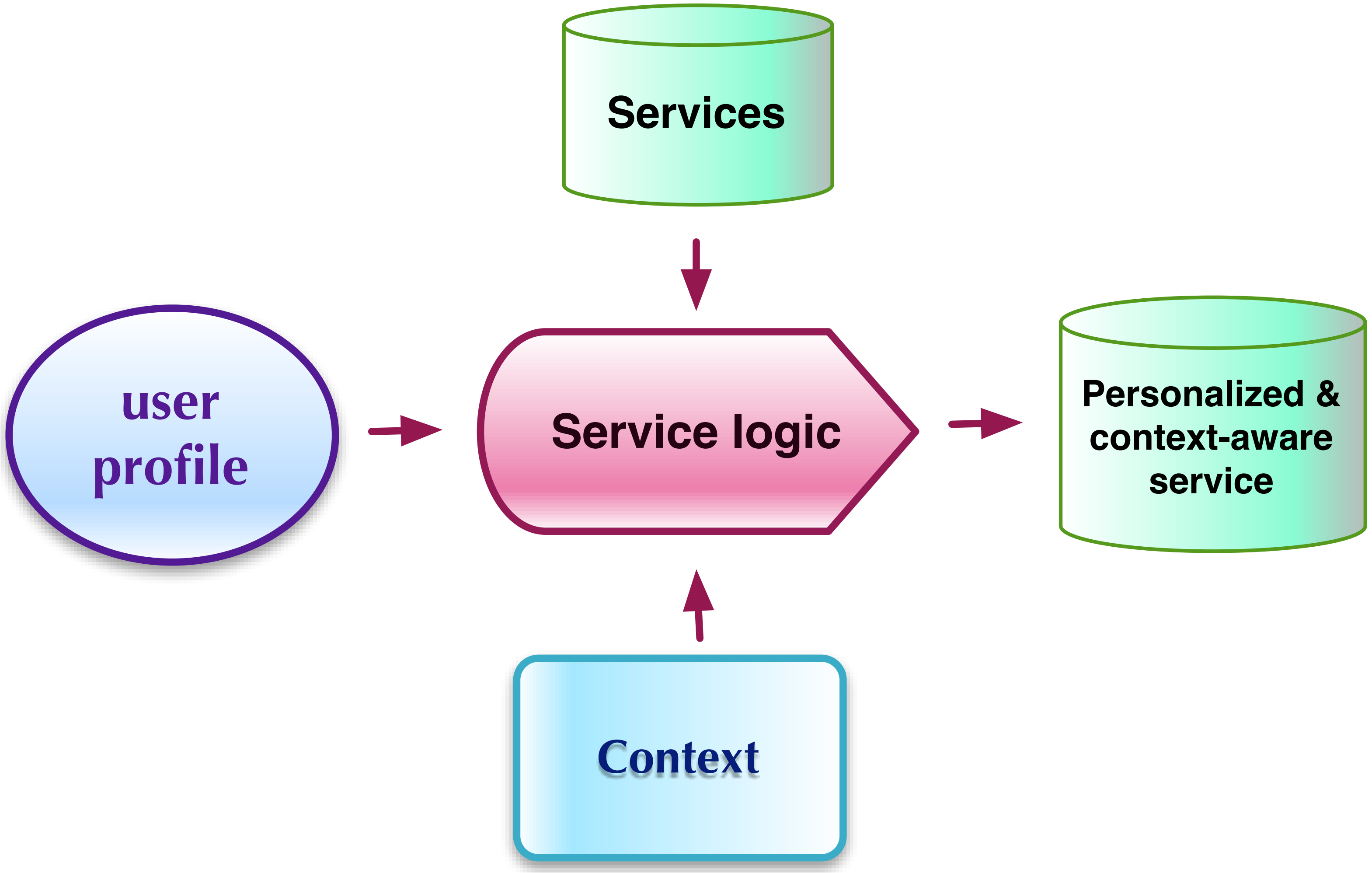
Scenario

- A full scenario
  - With focus on transport and home situations
  - With a special scenario element verbally supported with a car-to-car high level technical description
  - Covering the daily life for a normal user in Germany
- Scenario elements (to focus on special themes and geographical differences)
  - Social networking (nomadic business man in Sydney)
  - Traffic issues (man in Chennai, India, to get through a traffic jam)
  - Car-to-car high level technical description of one element in the full scenario
  - Private/public issues (Rural China)
- Editors: Lene Sørensen, Knud Erik Skouby (WG1)

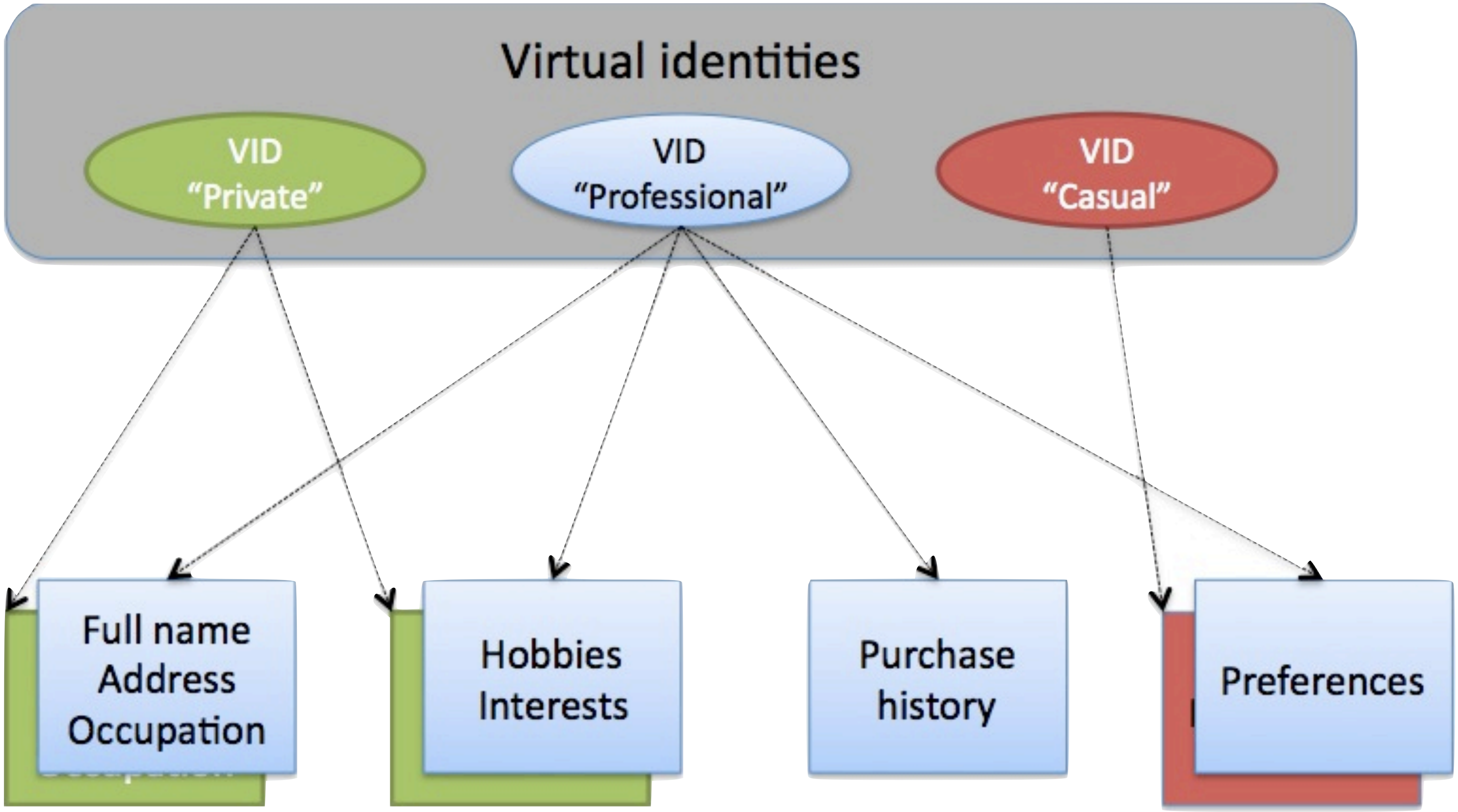
Table of Content

- Introduction
- Service Scenarios
  - Identifying the parts, where user profiles are important
- Applicability of user profiles
  - Virtual identities, role-based service selection, prioritisation
- Process description
  - I-centric, set-up, service selection, service usage
- Structure of profile
  - Communities and Identities, context and communication
- Enhancing the user profile
  - User input, learning, community input
- Privacy-enhanced personalisation
- Vision: Identified areas of research
- Conclusions

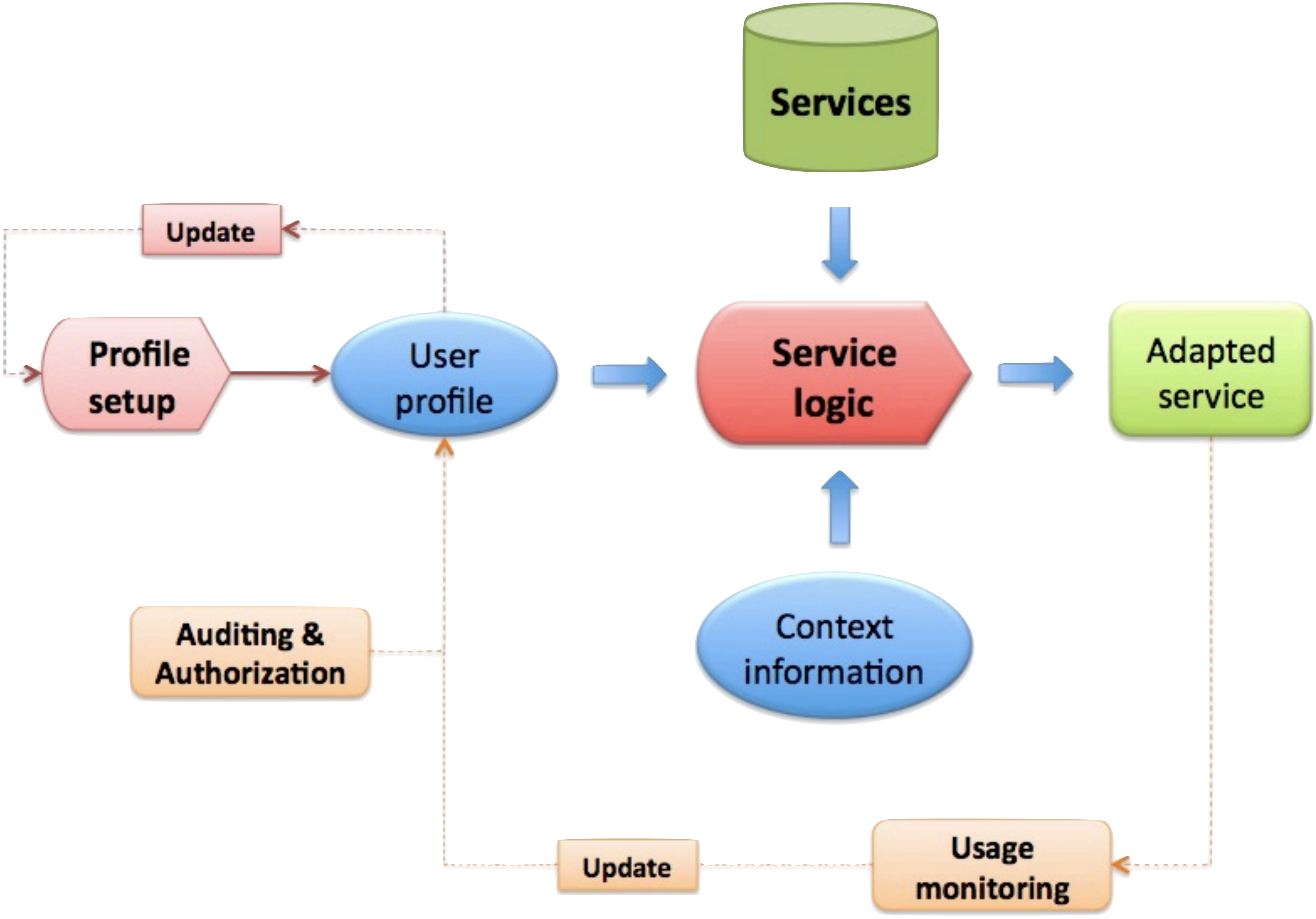
Service adaptation



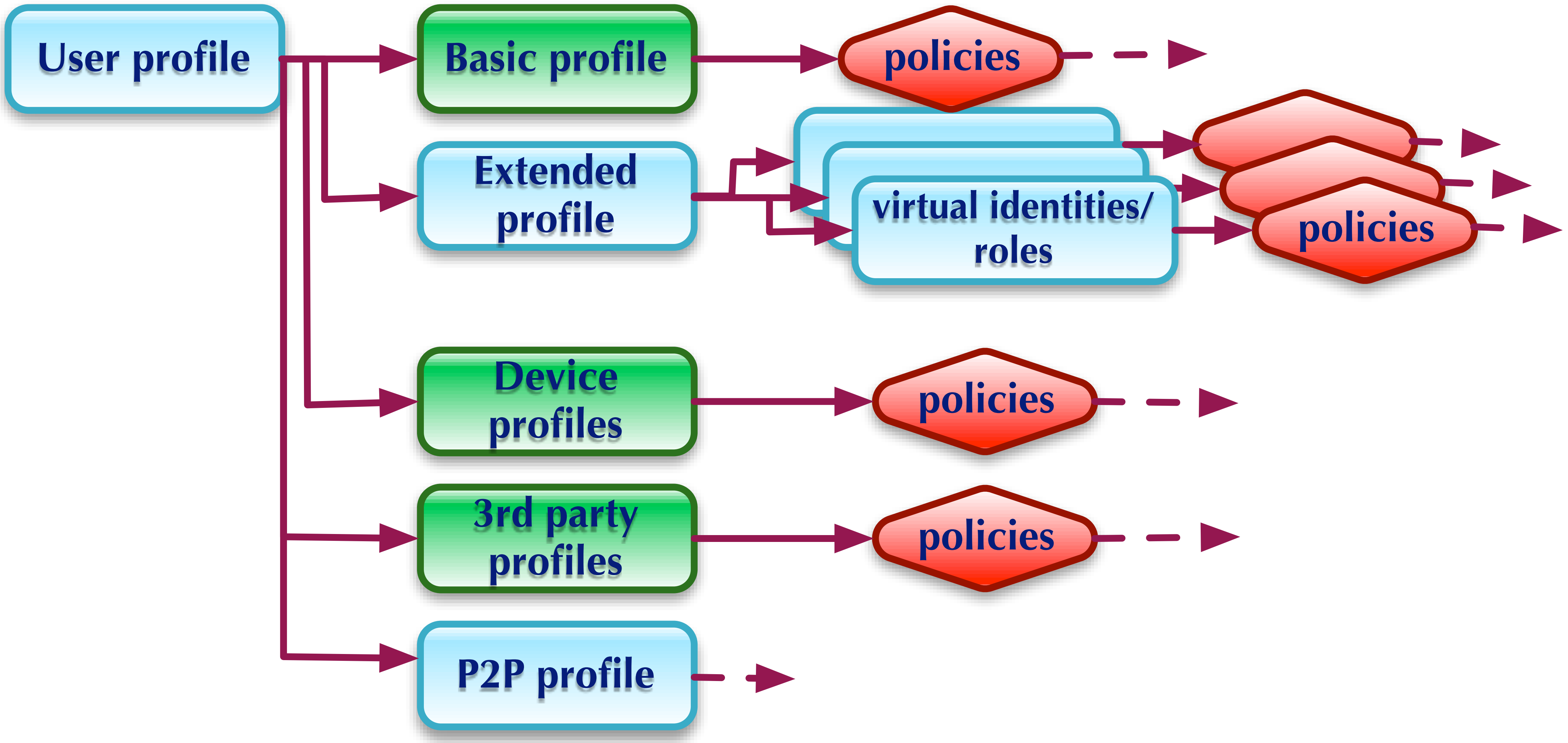
Service adaptation



Service adaptation



Profiles and policies



🟩 x defined by 3GPP/ETSI/W3C

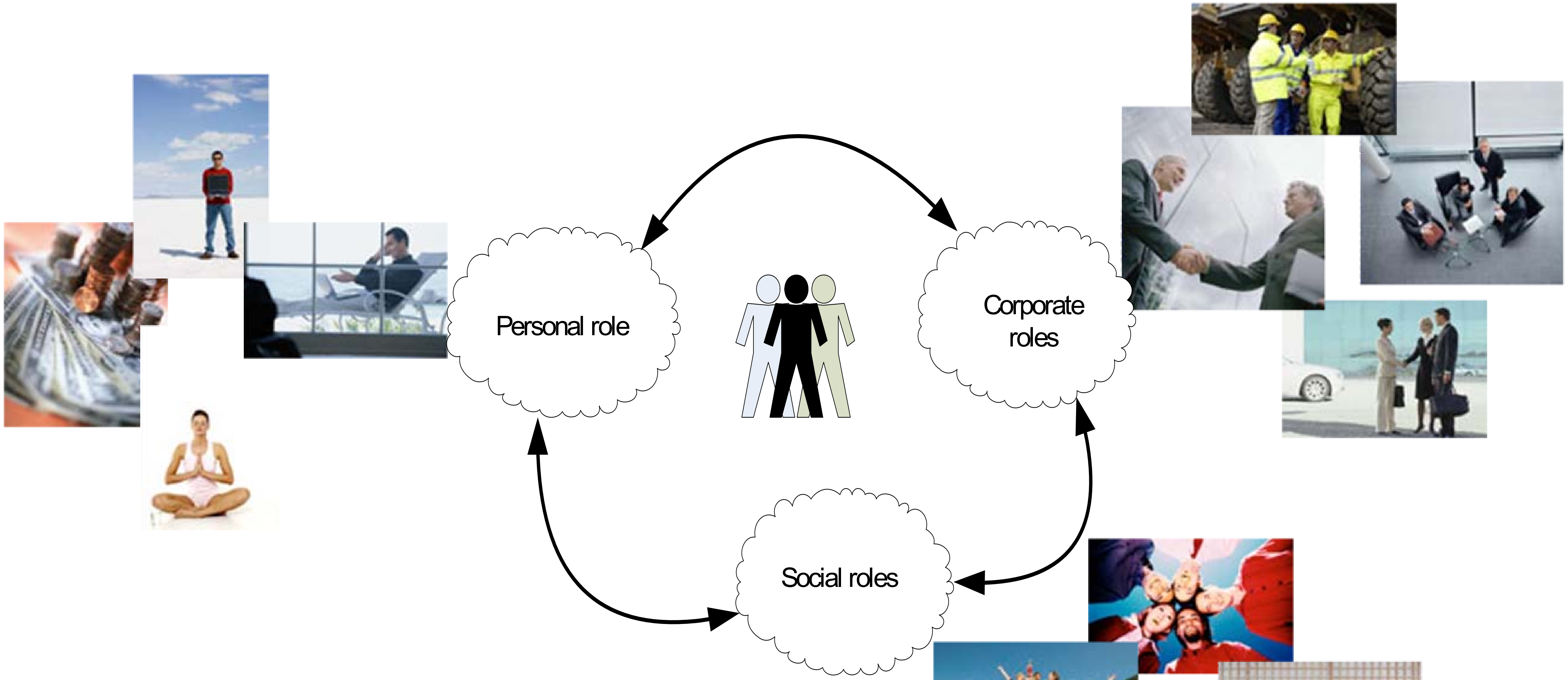
🟦 y defined by Magnet Beyond, Daidalos, Liberty Alliance

Example application:

Role based access

NFR Swacom project, http://www.swacom.org

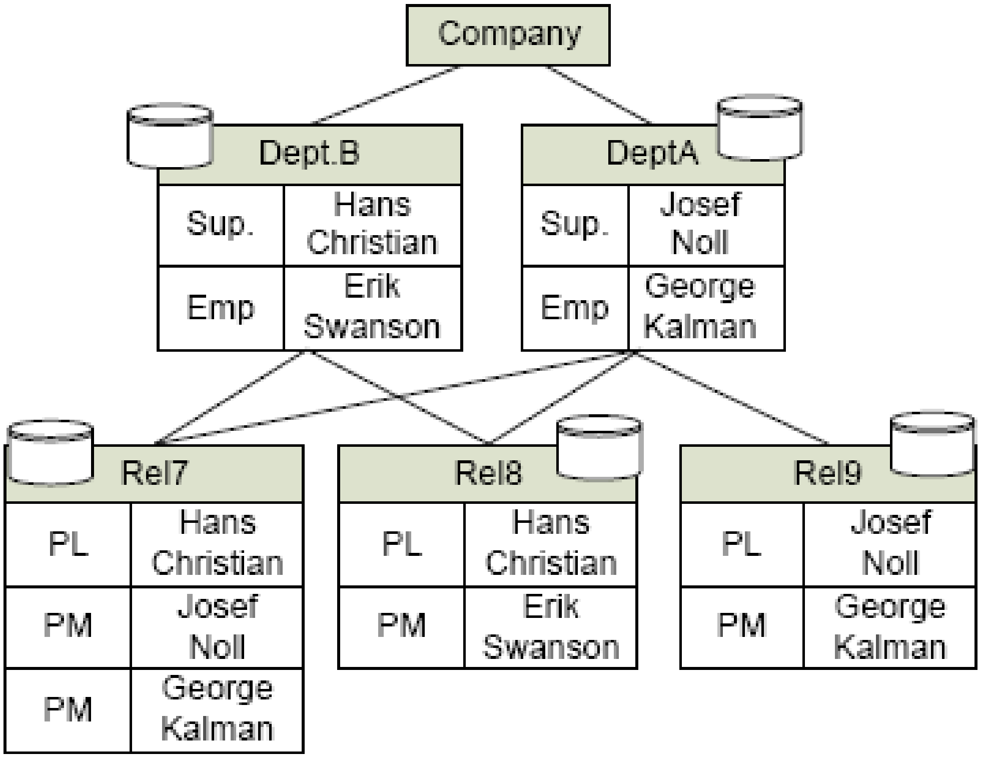
Human roles and relations



- Used to define virtual identities
  - Social Identity (SID)
  - Corporate Identity (CID)
  - Personal Identities (PID)

source: Mohammad M. R. Chowdhury, UNIK

Scenario: Corporate access



Company

Dept.B	
Sup.	Hans Christian
Emp	Erik Swanson

DeptA	
Sup.	Josef Noll
Emp	George Kalman

Rel7	
PL	Hans Christian
PM	Josef Noll
PM	George Kalman

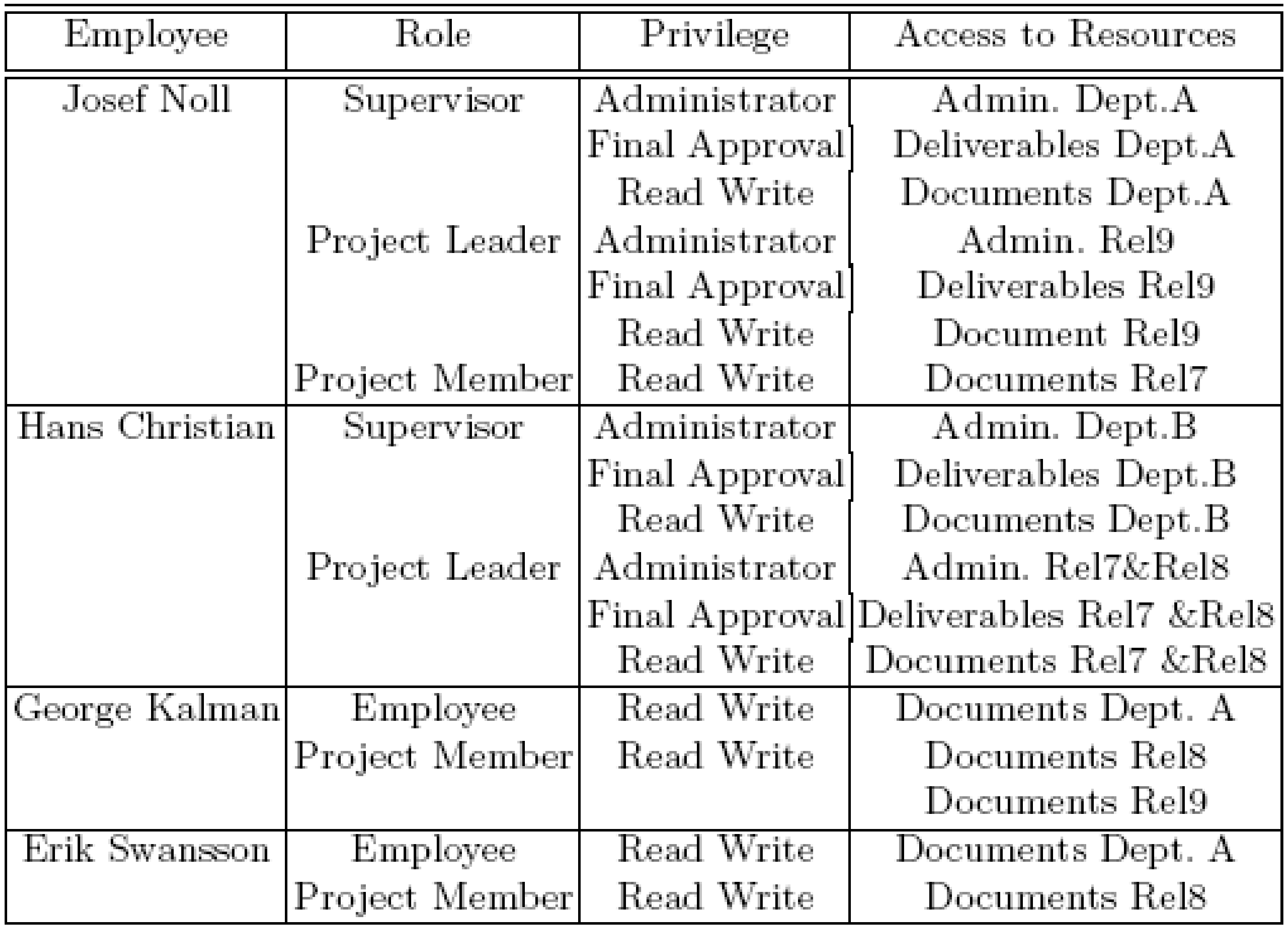
Rel8	
PL	Hans Christian
PM	Erik Swanson

Rel9	
PL	Josef Noll
PM	George Kalman

Assumptions: All the users are authenticated

Requirements: users having specific roles can access relevant resources belong to the project/department they involve in with right privileges.

Table 1. Roles and privileges to access corresponding resources



Employee	Role	Privilege	Access to Resources
Josef Noll	Supervisor	Administrator Final Approval Read Write	Admin. Dept.A Deliverables Dept.A Documents Dept.A
	Project Leader	Administrator Final Approval Read Write	Admin. Rel9 Deliverables Rel9 Document Rel9
	Project Member	Read Write	Documents Rel7
Hans Christian	Supervisor	Administrator Final Approval Read Write	Admin. Dept.B Deliverables Dept.B Documents Dept.B
	Project Leader	Administrator Final Approval Read Write	Admin. Rel7&Rel8 Deliverables Rel7 &Rel8 Documents Rel7 &Rel8
George Kalman	Employee	Read Write	Documents Dept. A
	Project Member	Read Write	Documents Rel8 Documents Rel9
Erik Swansson	Employee	Read Write	Documents Dept. A
	Project Member	Read Write	Documents Rel8

Access depends on –

- Roles
  - Multiple Roles by a user in different work unit
- Role plays in which dept./project
- Role contains which privileges
- Resources need which privileges

source: Mohammad M. R. Chowdhury, UNIK

Architectural overview

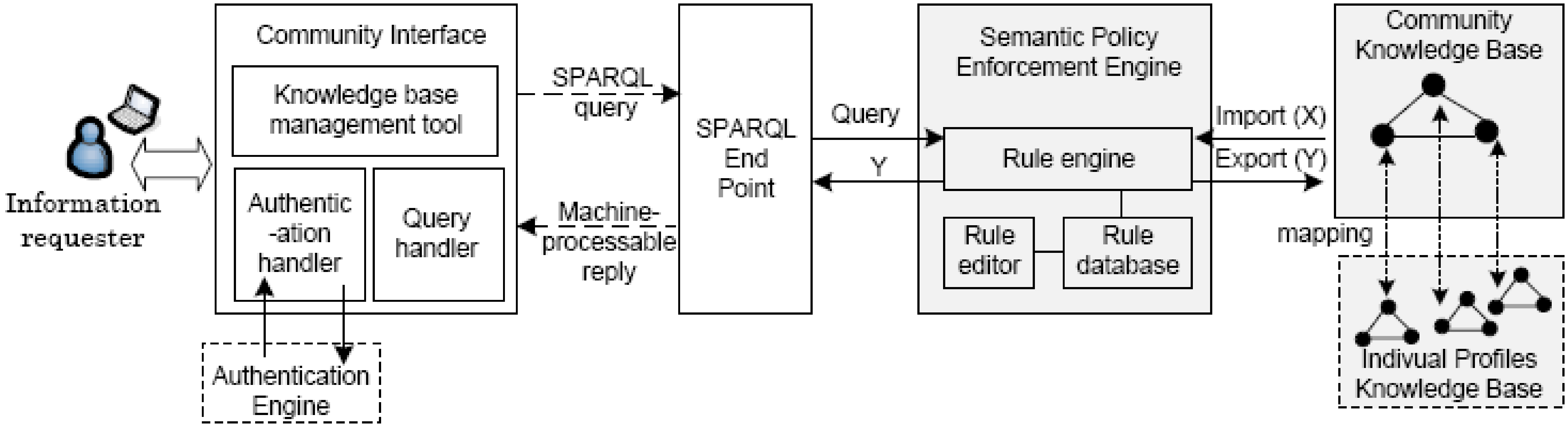


Figure 4 Detailed functional architecture of the proposed social community framework.

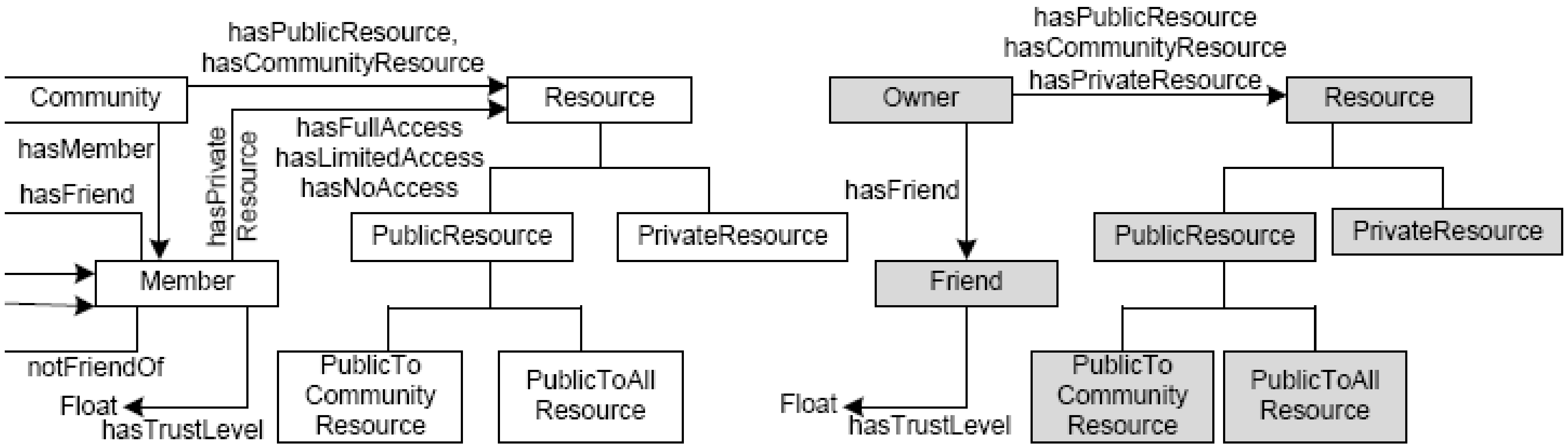


Figure 5 The classes and the properties of community and individual ontologies.

Mapping required to represent the correspondence between the elements of the ontologies

Limitations:

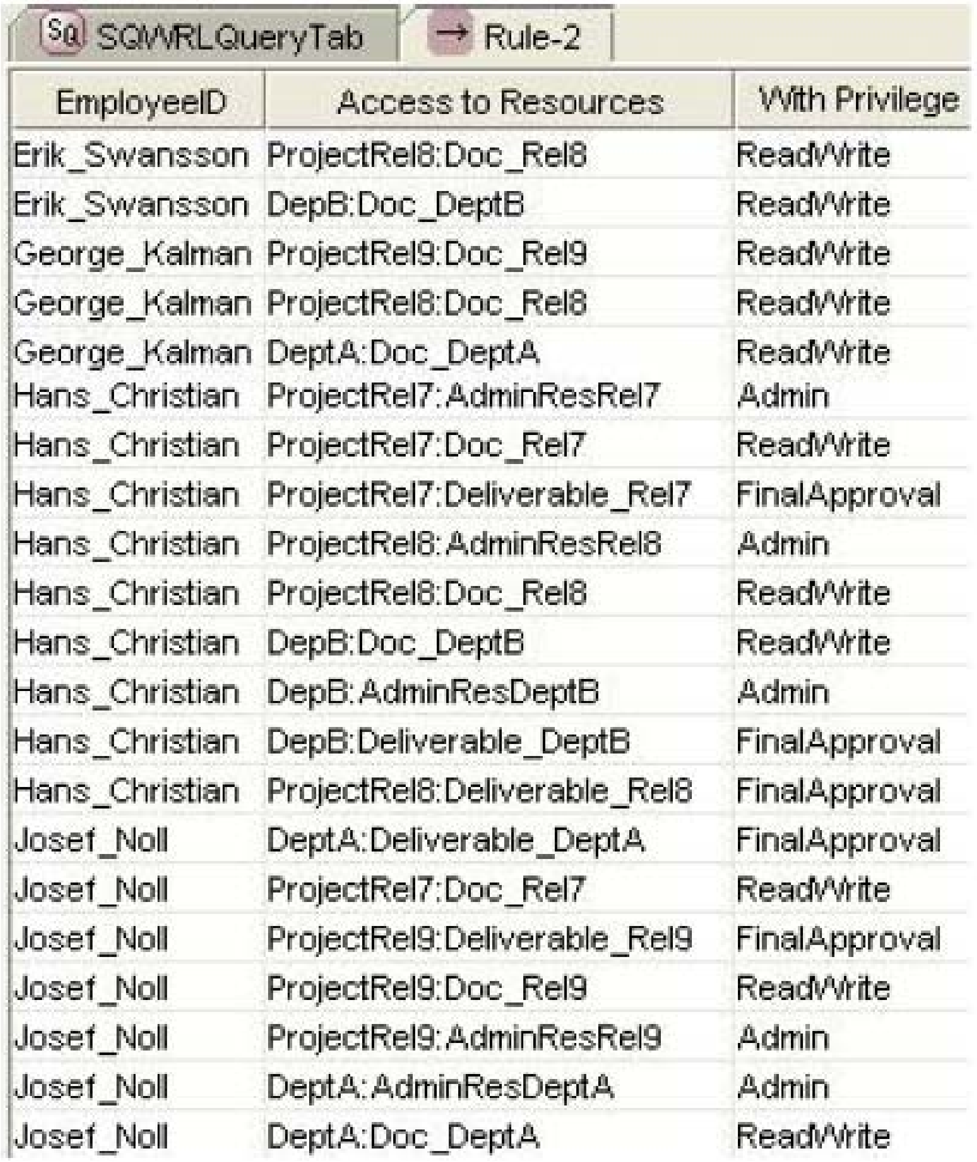
Manual mapping (complex and tedious)

source: Mohammad M. R. Chowdhury, UNIK

Implementation using OWL-DL and SWRL

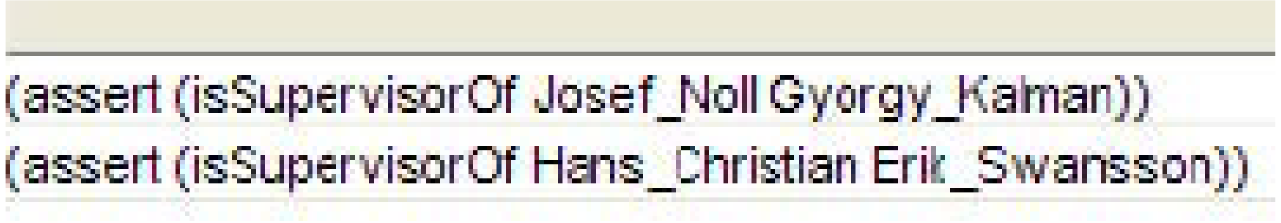
$$EmployeeID(?ID) \wedge hasRole(?ID,?R) \wedge Privilege(?PR) \wedge hasPrivilege(?R,?PR) \wedge needPrivilege(?Z,?PR) \wedge hasAccessTo(?R,?Z) \longrightarrow sqwrl:select(?ID) \wedge sqwrl:select(?Z) \wedge sqwrl:select(?PR) \wedge sqwrl:columnNames(``EmployeeID'', ``AccesstoResource'', ``WithPrivilege'') \wedge sqwrl:orderBy(ID?)$$

- Used rule based reasoner for the neccessary deductions
  - SWRL + SQWRL + Jess Rule Engine



EmployeeID	Access to Resources	With Privilege
Erik_Swansson	ProjectRel8:Doc_Rel8	ReadWrite
Erik_Swansson	DepB:Doc_DeptB	ReadWrite
George_Kalman	ProjectRel9:Doc_Rel9	ReadWrite
George_Kalman	ProjectRel8:Doc_Rel8	ReadWrite
George_Kalman	DeptA:Doc_DeptA	ReadWrite
Hans_Christian	ProjectRel7:AdminResRel7	Admin
Hans_Christian	ProjectRel7:Doc_Rel7	ReadWrite
Hans_Christian	ProjectRel7:Deliverable_Rel7	FinalApproval
Hans_Christian	ProjectRel8:AdminResRel8	Admin
Hans_Christian	ProjectRel8:Doc_Rel8	ReadWrite
Hans_Christian	DepB:Doc_DeptB	ReadWrite
Hans_Christian	DepB:AdminResDeptB	Admin
Hans_Christian	DepB:Deliverable_DeptB	FinalApproval
Hans_Christian	ProjectRel8:Deliverable_Rel8	FinalApproval
Josef_Noll	DeptA:Deliverable_DeptA	FinalApproval
Josef_Noll	ProjectRel7:Doc_Rel7	ReadWrite
Josef_Noll	ProjectRel9:Deliverable_Rel9	FinalApproval
Josef_Noll	ProjectRel9:Doc_Rel9	ReadWrite
Josef_Noll	ProjectRel9:AdminResRel9	Admin
Josef_Noll	DeptA:AdminResDeptA	Admin
Josef_Noll	DeptA:Doc_DeptA	ReadWrite

$$Dept\_Employee(?DepEm) \wedge hasRole(?Y,?DepEm) \wedge Department(?Dep) \wedge rolePlaysIn(?DepEm,?Dep) \wedge Corporate\_Identity(?ID) \wedge Supervisor(?Sup) \wedge hasRole(?ID,?Sup) \wedge rolePlaysIn(?Sup,?Dep) \longrightarrow isSupervisorOf(?ID,?Y)$$



```
(assert (isSupervisorOf Josef_Noll Gyorgy_Kalman))
(assert (isSupervisorOf Hans_Christian Erik_Swansson))
```

source: Mohammad M. R. Chowdhury, UNIK

Conclusions

- User profiles supporting virtual identities
- Providing privacy and allow for personalised service access
- SWACOM project focusses on role-based identities
- Using ontologies and rules (OWL-DL and SWRL) for access control policy descriptions
- Issues
  - Limited expressiveness - “Open world reasoning”
  - Interworking of ontologies (mediation)
  - “privacy” of parts of ontologies
- Implementation with focus on document access policies