ITU-T

International Telecommunication Union

Virtual Identities in a Heterogeneous Environment

Joao Girao

NEC Europe Ltd.

on behalf of Daidalos

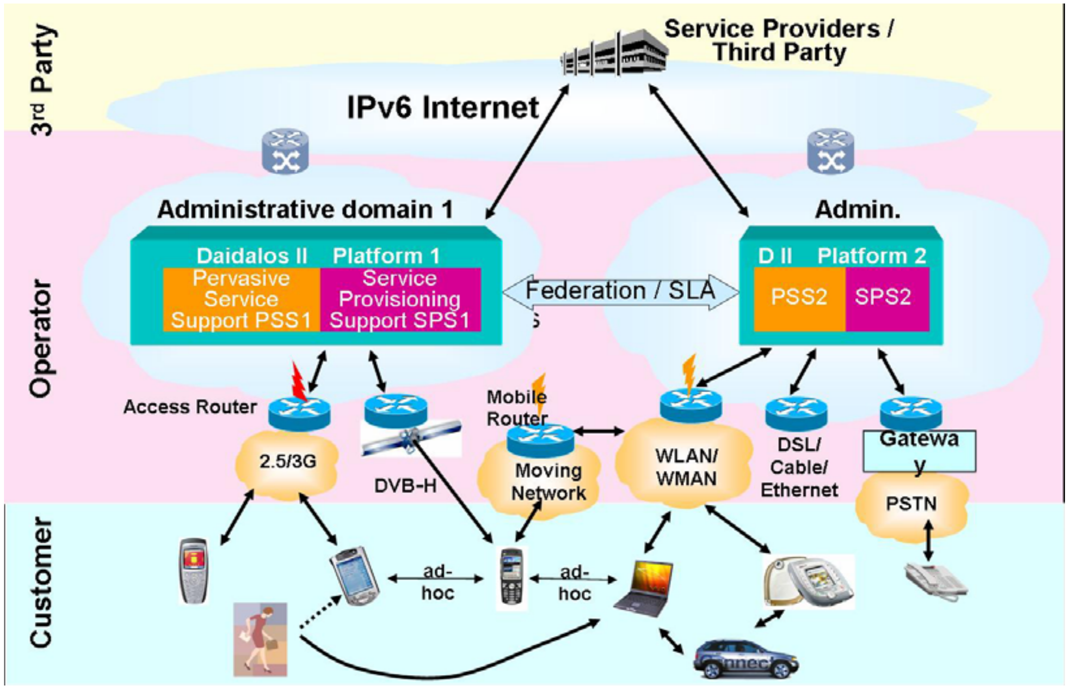
Overview

- Introduction to Daidalos
- Virtual Identities (VIDs)
  - Motivation
  - Concept
- So, how does VID relate to ID management?
- Cross layer design
- Some focus areas in the project
  - Identity Brokerage and Access Control
  - Mobility / Location privacy
  - Privacy in Context (ex. through obfuscation)
- Take home ideas

Introduction to Daidalos (1) - Overview

- EU IST 6th Framework Research Project
  - Beyond 3G Area
- Volume ~ 50 M€ over 5 years and 2 phases
  - November 2003 – December 2008
- Currently 36 Partners
- Lead: Deutsche Telekom AG
- Goal: Integrate mobile and broadcast communications following a scenario-based approach to deliver ubiquitous end-to-end services across heterogeneous technologies
- Contributions to standards an important aspect

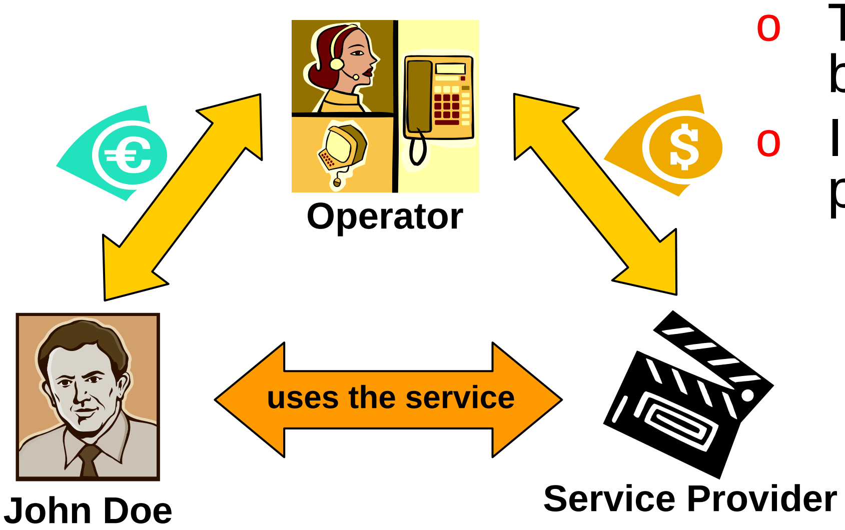
Introduction to Daidalos (2)
- Daidalos 5 Key Concepts



- MARQS (Integrating Mobility Management, AAA, Resource Management, QoS and Security)
- VID (Virtual Identities – personalisation at all levels)
- USP (Ubiquitous and Seamless Pervasiveness – includes context awareness),
- SIB (Seamless Integration of Broadcast – both technology and service levels)
- Federation (in terms of multiple market players, "*comperation*": competitors in cooperation")

Virtual Identities (VIDs) (1) - Motivation

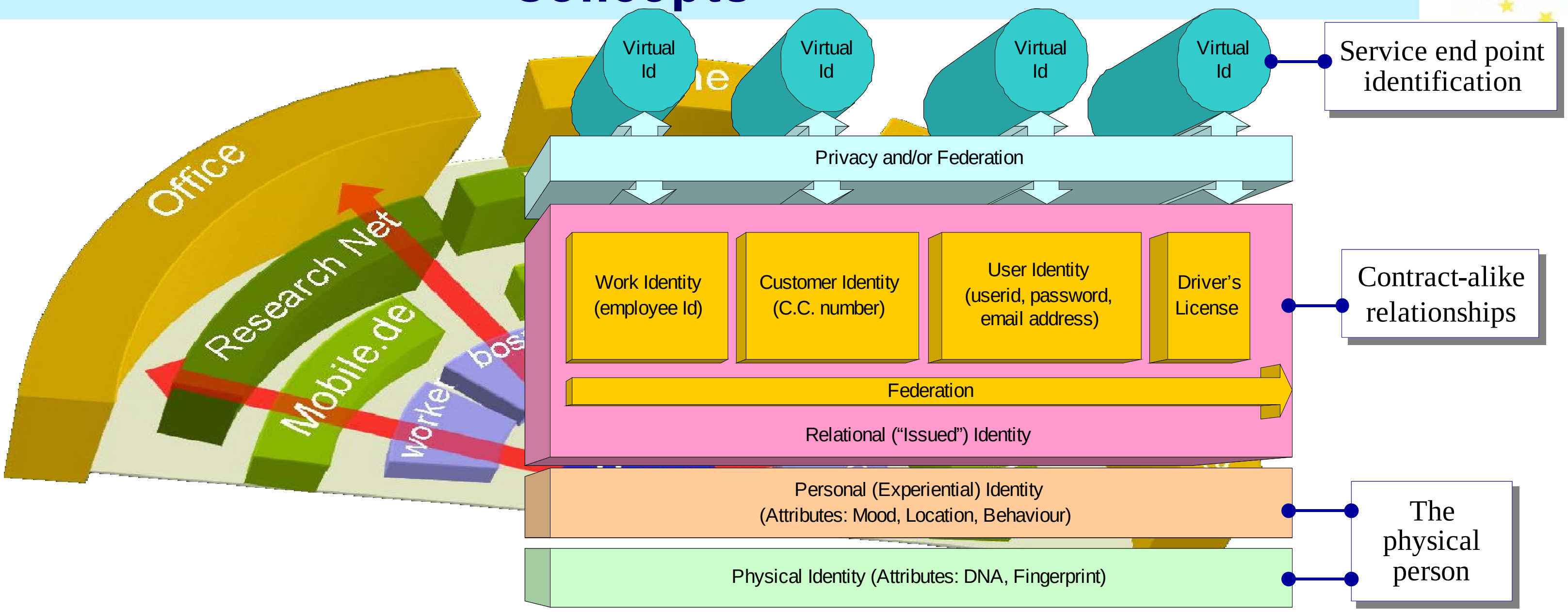
- Growing numbers of communication services burden users with increasingly complex authentication effort
- Users want a limited number of operators enabling universal access to everything – ideally “single sign-on”
- Identity solutions need to support multiple (virtual) identities for several profiles, roles and contexts, the maintenance of these identities, respecting privacy, and all available services, networks, content, … wherever the user may be.



- The trusted operator becomes a proxy for billing which is a business in itself.
- Improved security through VIDs acting as pseudonyms
  - the service provider delivers without knowing the user.
  - the trusted operator (e.g. operator or bank) knows the user but not the service.

ITU-T

Virtual Identities (VIDs) (2) - Concepts



Virtual Id
Virtual Id
Virtual Id
Virtual Id

Service end point identification

Privacy and/or Federation

Work Identity (employee Id)
Customer Identity (C.C. number)
User Identity (userid, password, email address)
Driver's License

Contract-alike relationships

Federation

Relational ("Issued") Identity

Personal (Experiential) Identity (Attributes: Mood, Location, Behaviour)

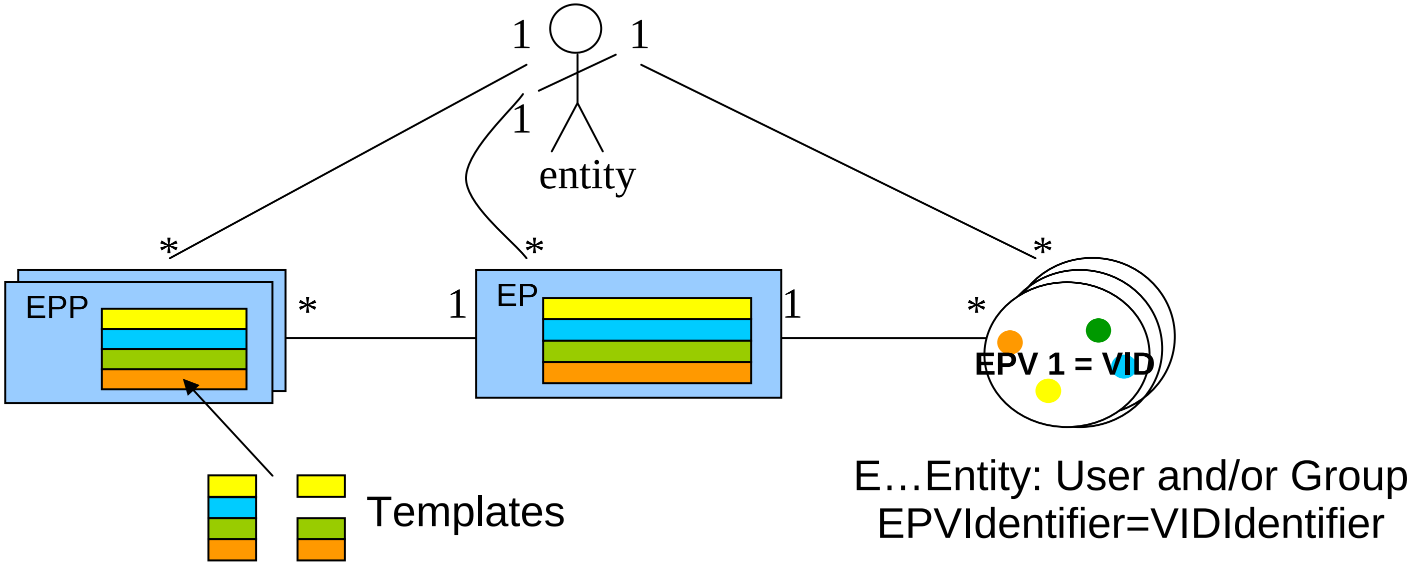
Physical Identity (Attributes: DNA, Fingerprint)

The physical person

- Privacy
- Unified and Uniform Namespaces
  - Contractual
  - Context
  - Personalization
- Access Control
- Billing and Charging
- Lawful Interception

- Linking the real world with the digital world
- User's data should be under his control
- Service providers must make use of federation to enhance the user-experience but this should be a user-oriented mechanism

Virtual Identities (VIDs)? (3) - Concepts



E…Entity: User and/or Group
EPVIdentifier=VIDIdentifier

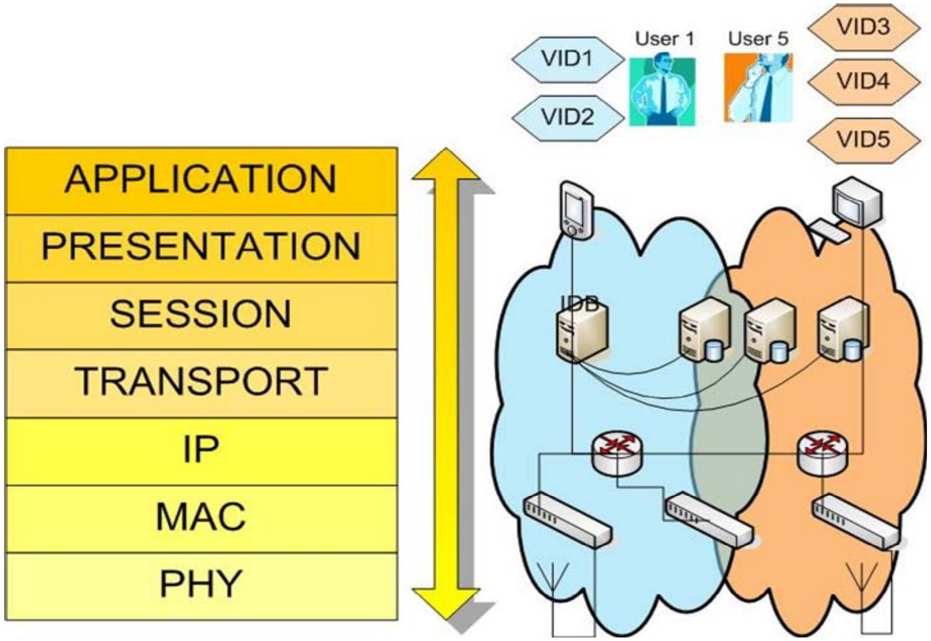
- Entity: Any body capable of performing a legal binding (individual, company, service provider, etc).
- Entity Profile Part (EPP): The minimum coherent piece, part of the entity's data (contractual, context, network related, personalization).
- Entity Profile (EP): The union of all EPPs knowledge coming directly from the entity. EP is an abstract concept which does not exist in the network.
- Entity Profile View (EPV) or Virtual Identity: The result of the entity's selection and aggregation of some of its EPPs. Provides a limited view on the profile of the entity.

So, how does VID relate to ID management?

- VID is a framework which abstracts from the entity information management mechanism
- It makes use of the hooks provided by IDm platforms and integrates its functionality with that already present in lower layers
- VID also enforces an analysis on where entity data can be correlated at different layers and network domains
- It is based on the fact that a user may want to show different unrelated faces to the network and services. (the same holds for the service, groups, …)

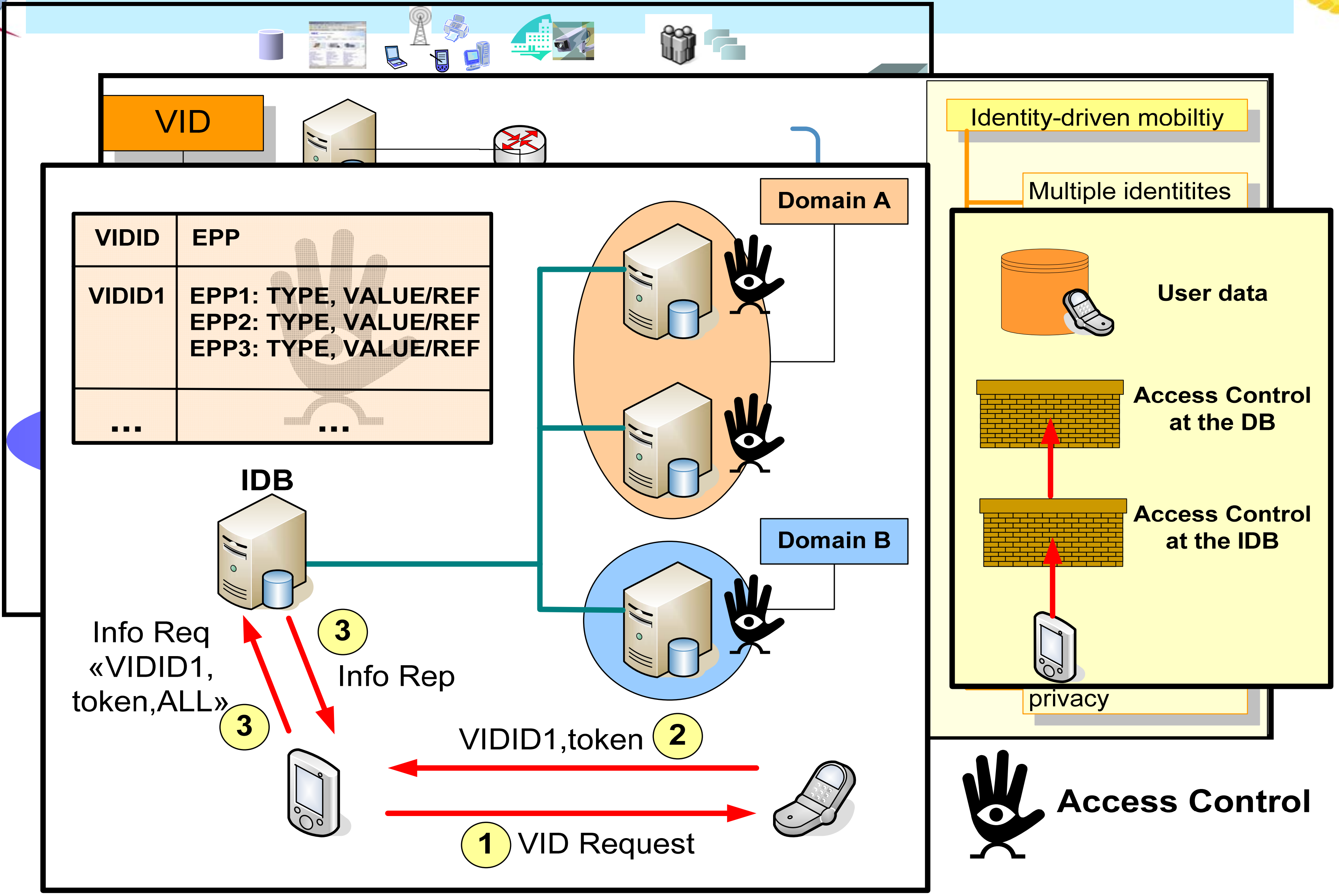
ITU-T

Cross layer design



- Uniform namespaces (one ID for all purposes)
  - For network identification
  - To obtain information about a user/service/group
  - Under which to authenticate to the network and to the services
- To maintain pseudonimity at a higher level, a top-down protocol design is required
- ID must be independent of the application, service, interface and even terminal

Some focus areas in the project



VIDID	EPP
VIDID1	EPP1: TYPE, VALUE/REF EPP2: TYPE, VALUE/REF EPP3: TYPE, VALUE/REF
...	...

Take home ideas

- Identity Management is maturing quite fast, however we need to pay more attention to **how identity affects the lower layers**
- The **information** on the user/service should be **handled consistently** and **integrated** into **Internet** management and transport **protocols**
- The potential of a **digital identity** goes far beyond services, it can be used to **enhance network protocols** such as mobility or QoS
- Identity Management permeates the complete network architecture. Understanding the SDO's role and reaching consensus is essential to achieve a **single** solution

END