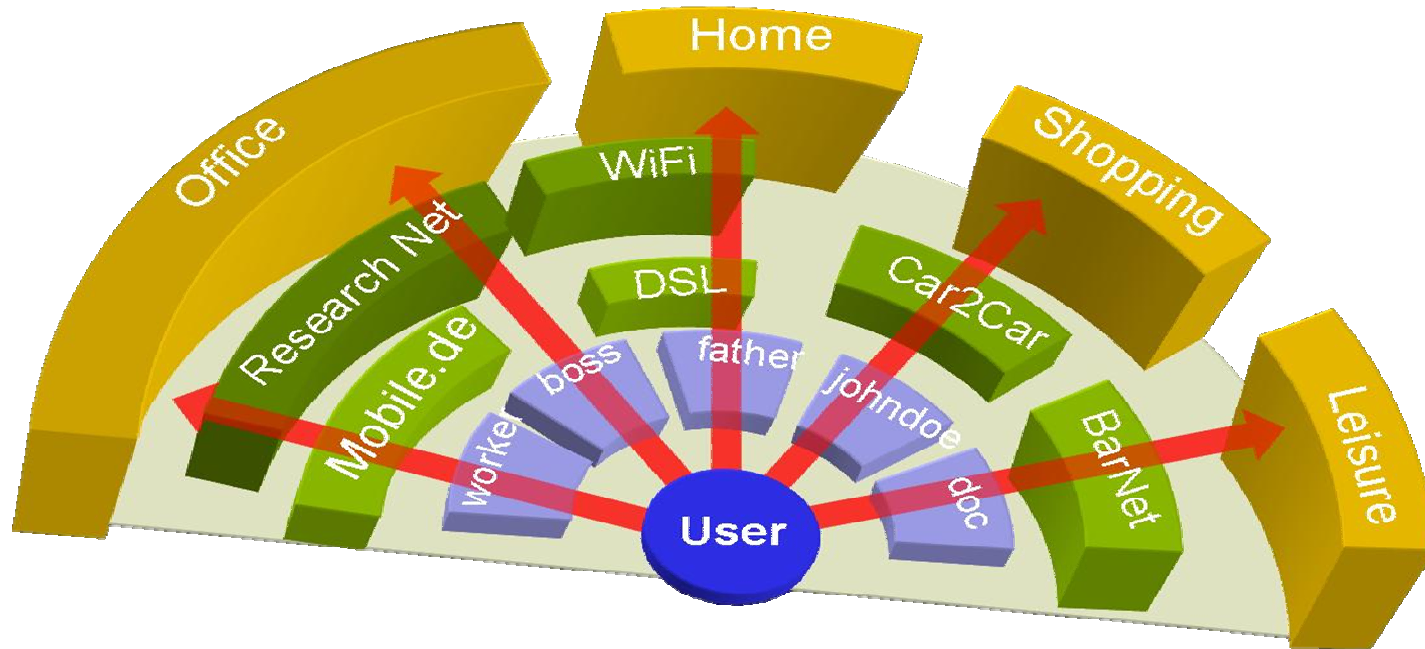




Daidalos VID Summary



Summary (1 of 2)

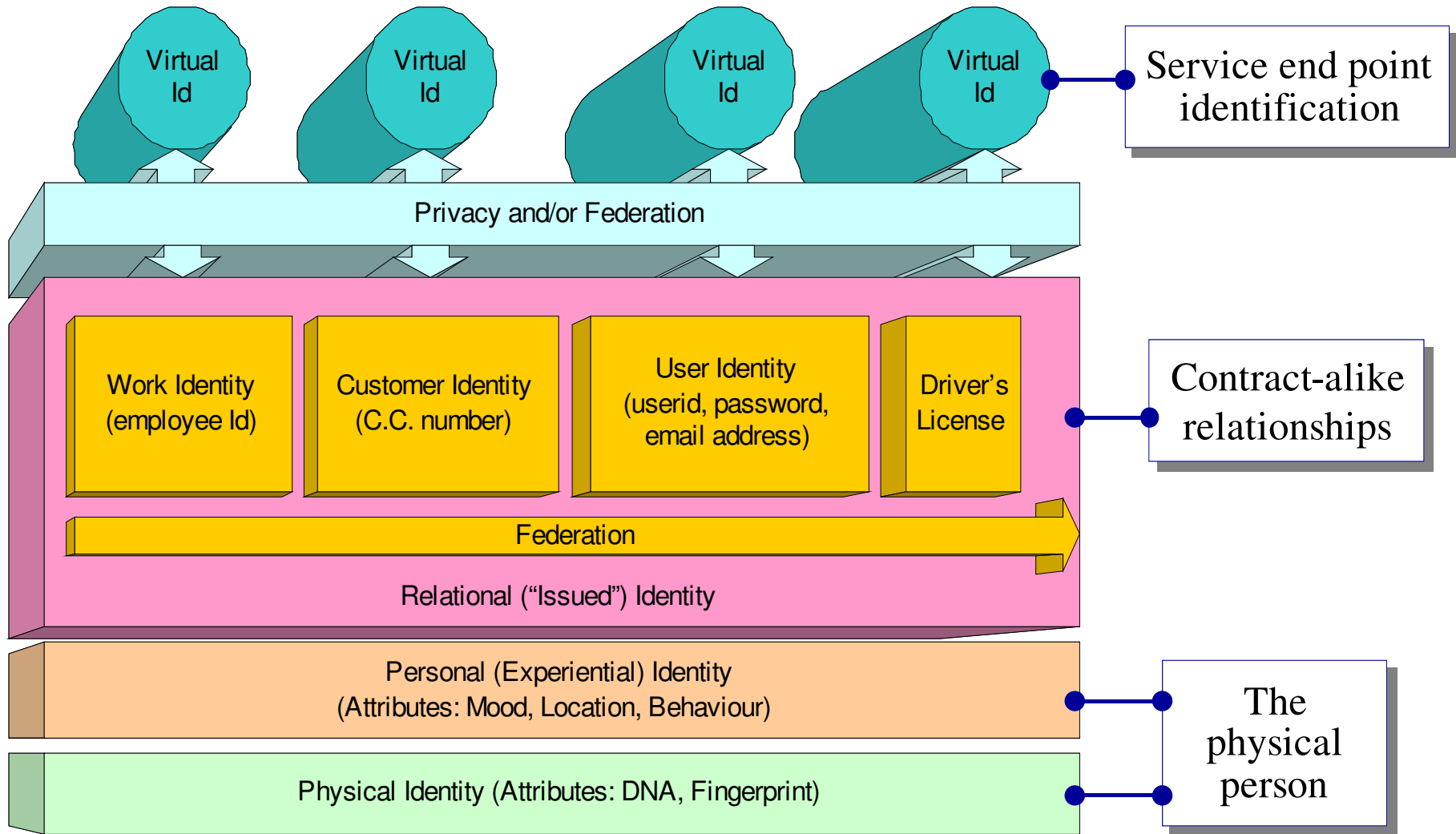


- ▶ Privacy
- ▶ Unification and Uniformity of Namespaces
 - Contractual
 - Context
 - Personalization
- ▶ Access Control
- ▶ Billing and Charging
- ▶ Lawful Interception



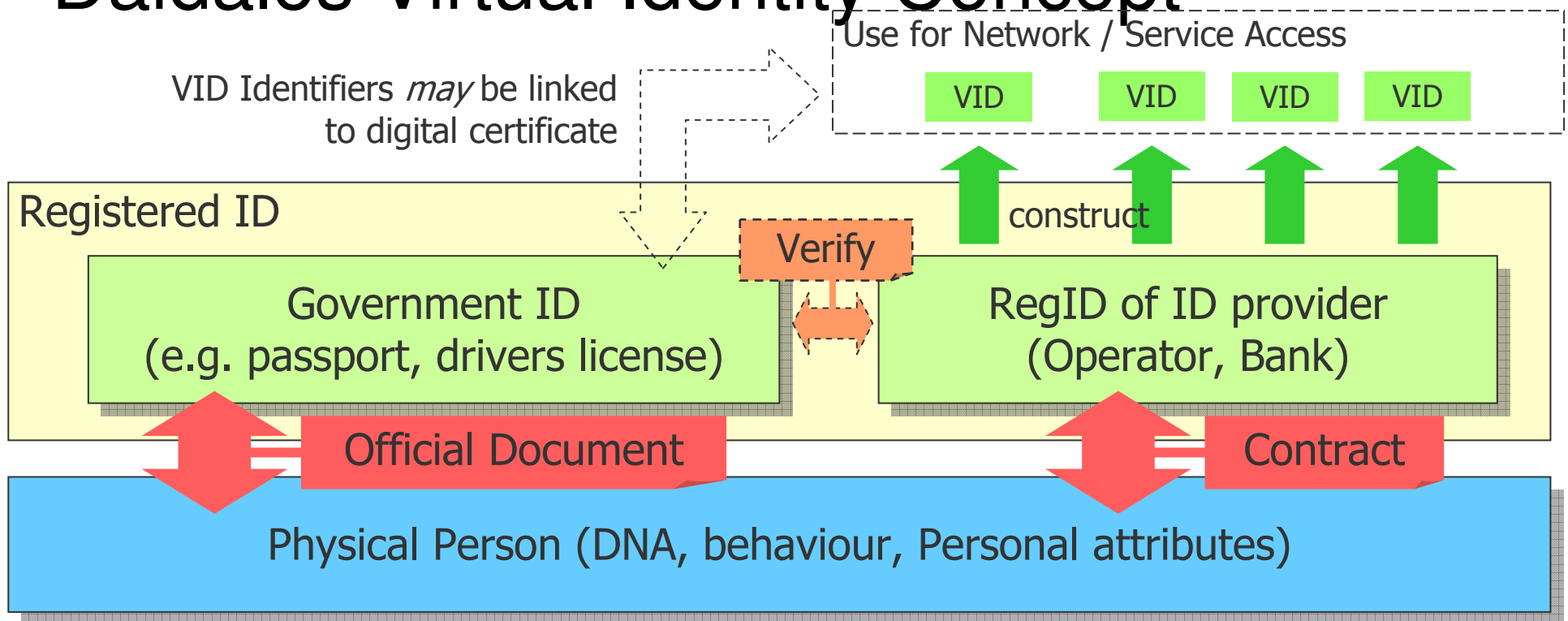


Summary (2 of 2)





Daidalos Virtual Identity Concept

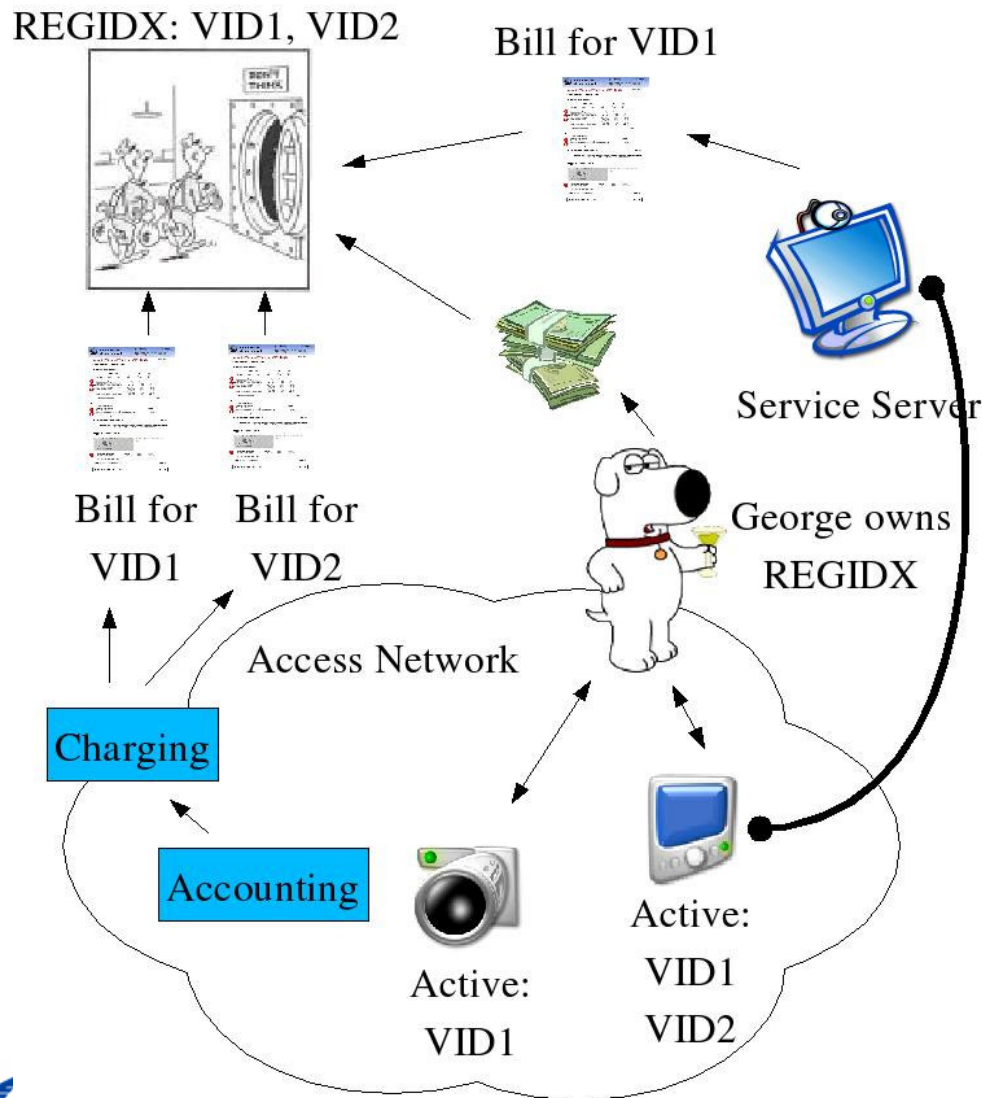


- VIDs are used for federation between domains as provider identifiers
- VIDs are used for both network and service access, as well as content
 - May be extended to other domains, e.g. gaining entrance to building
 - ID token that contains VID Identifier + encrypted artefact for A4C is used





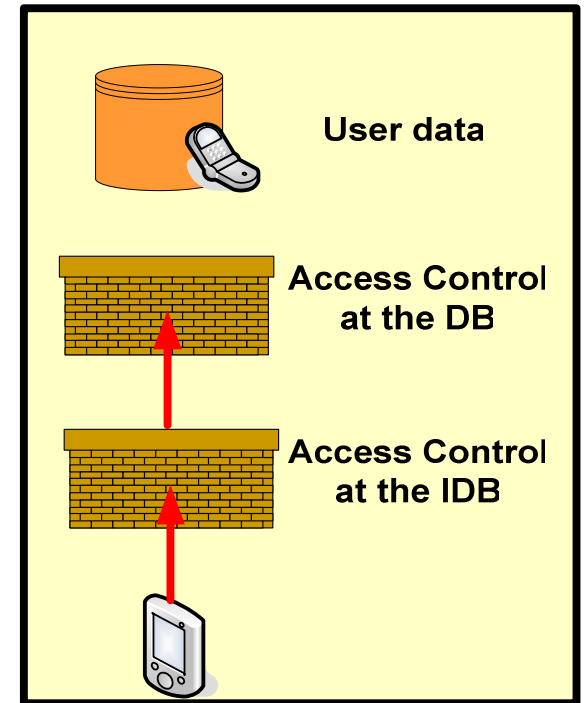
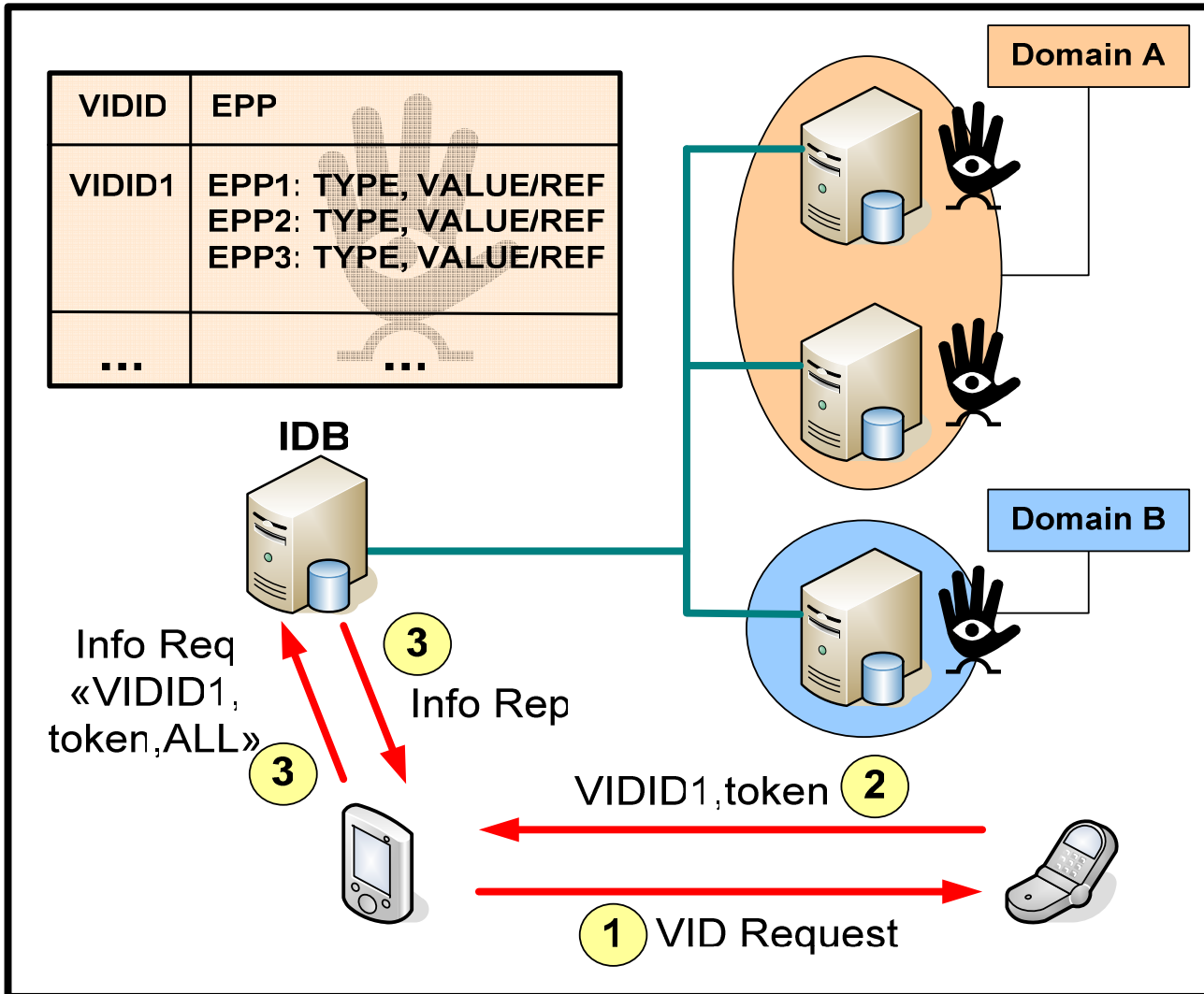
Billing and Charging



- ▶ The user can use the operator as a proxy for billing.
- ▶ The service provider knows the service but not the identity of the user.
- ▶ The billing entity (e.g. bank) knows the user but not the service.
- ▶ Allows setting up a cascade of contractual relations by proxying responsibility in an authorized way.



ID Broker + Access Control





Mobisplit in a Virtualized, Multi-Device environment

J. Abeillé, J. Giraó, T. Melia, P. Stupar, NEC Europe Laboratories, Germany, R. L. Aguiar, IT Aveiro, Portugal, I. Soto, UC3M, Spain



Outline



- ▶ Introduction
- ▶ Traditional mobility / identity approaches
- ▶ A new paradigm in mobility
- ▶ Instantiation



Outline



- ▶ Introduction
- ▶ Traditional mobility / identity approaches
- ▶ A new paradigm in mobility
- ▶ Instantiation





Introduction

- ▶ Increasing complexity in next generation mobile networks
 - Multimode device with several access technologies
 - User has multiple device and ubiquitous access
 - Public / shared device available to the user
- ▶ Mobility influenced by
 - User context
 - User preferences
- ▶ -> New paradigm in mobility supported by a novel architecture



Outline



- ▶ Introduction
- ▶ Traditional mobility / identity approaches
- ▶ A new paradigm in mobility
- ▶ Instantiation





Traditional Mobility schemes

- ▶ Inside a device
 - Host based mobility: MIPv6, CIP
 - Network based mobility: GTP, PMIPv6
 - > mobility bound to an interface
- ▶ Multihoming
 - MONAMI6 IETF WG
 - Several HoAs/CoAs
 - often visible from the outside
- ▶ Session mobility (across device)
 - Seen as a session layer issue, supported with SIP
 - > application dependant





Traditional identity architectures

- ▶ 3G separates identity from terminal by means of a SIM card
 - Usable over several device
 - One device can support several SIMs
- ▶ HIP splits identifier from locator
 - But user over multiple device not supported



Outline

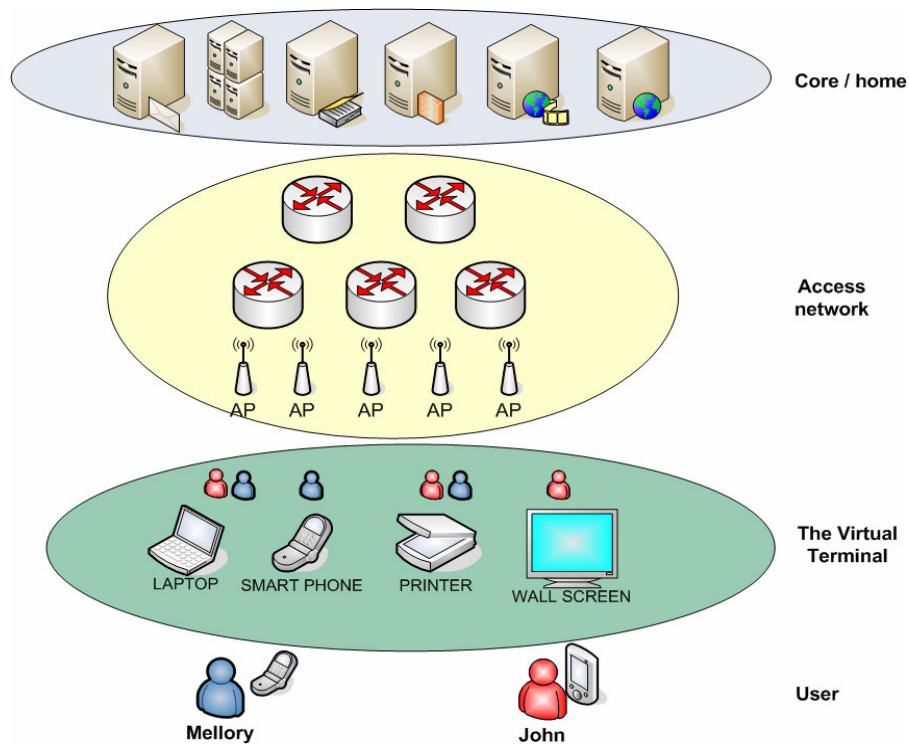


- ▶ Introduction
- ▶ Traditional mobility / identity approaches
- ▶ A new paradigm in mobility
- ▶ Instantiation





Mobility with Virtual Identity



▶ The **User** and his **Virtual Terminal** are mobile

▶ A user has several device / interfaces, public device, operators, all bound to one common VT

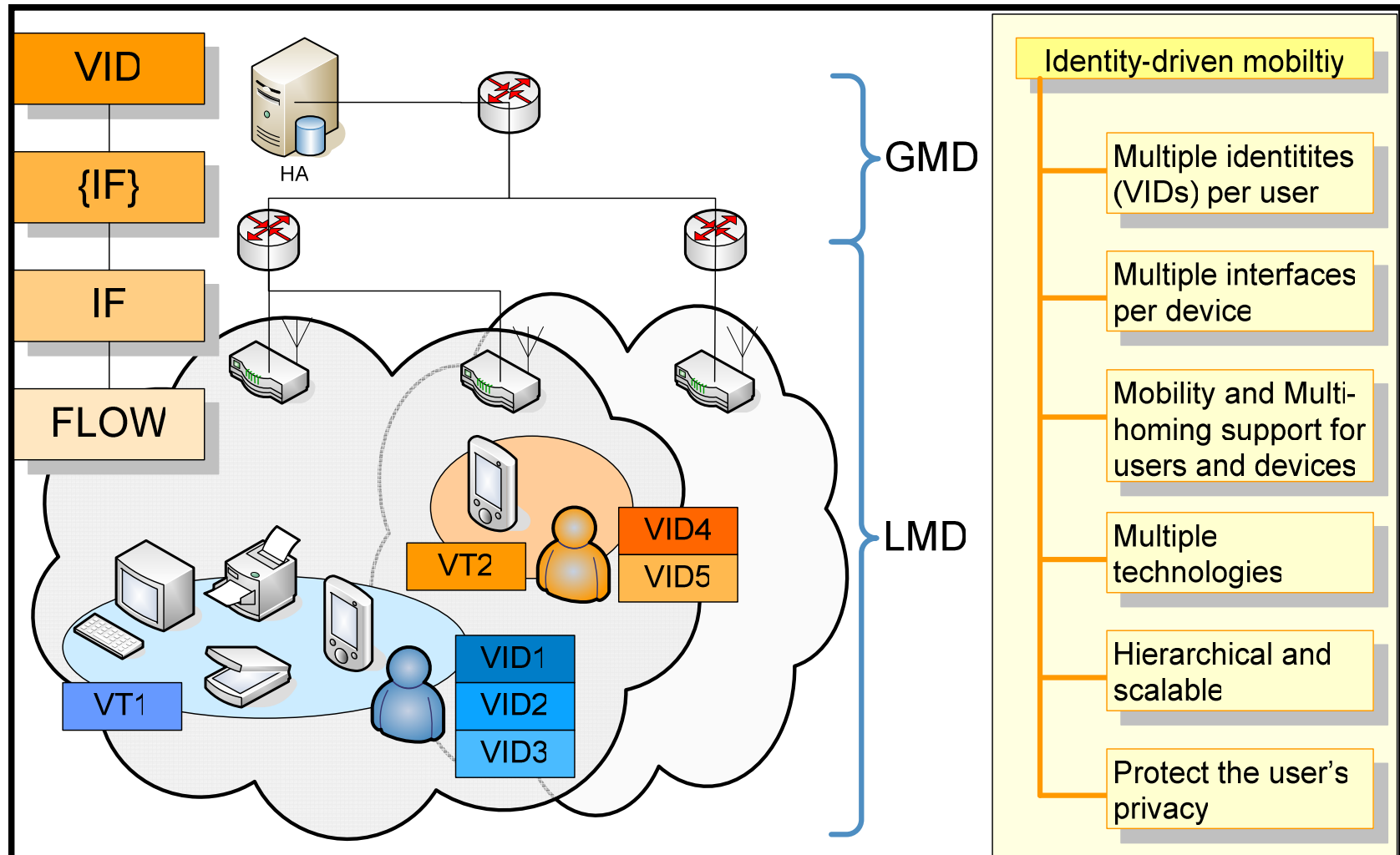
▶ The peers outside the access network do not see the interfaces at any layer.

▶ Interface / session mobility handled at network layer.





Identity-driven Mobility



Outline

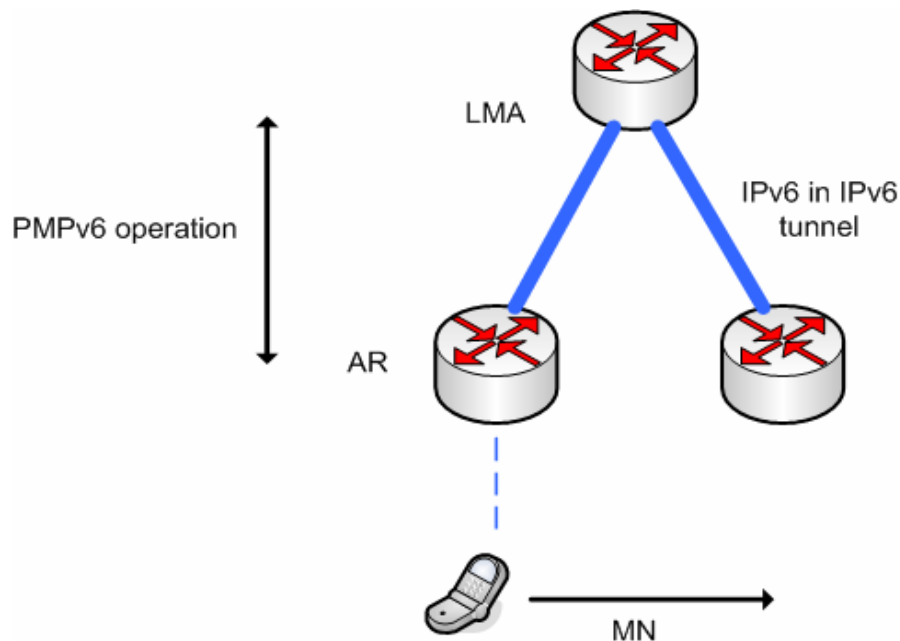


- ▶ Introduction
- ▶ Traditional mobility / identity approaches
- ▶ A new paradigm in mobility
- ▶ Instantiation





Background - NetLMM



- ▶ Goal 1: MN implements a vanilla IPv6 stack
- ▶ Functional entities = LMA, AR
- ▶ Signaling to handle registration, deregistration, handover
- ▶ Tunneling between LMA and MAG
- ▶ MN keeps the same IP address



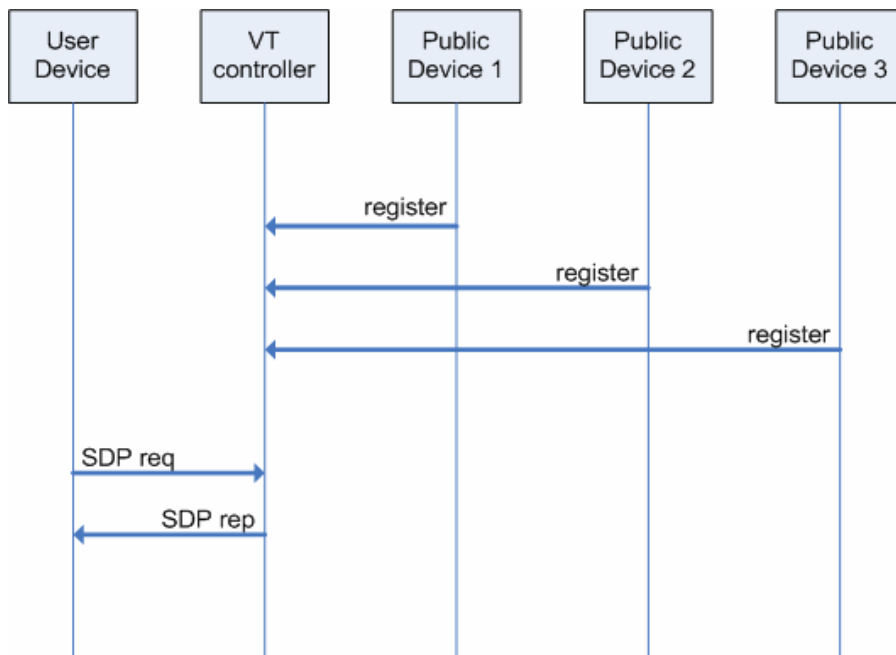
Background - MobiSplit

- ▶ Hierarchical scheme according administrative boundaries
 - Host based mobility in the global domain (MIPv6 as an example)
 - Network based mobility in the local domain (PMIPv6)
 - > operators independence, flexibility
- ▶ Multihoming / multi – device
 - All interfaces get the same IP address while roaming inside an access network
 - > transparent to the core, applications
- ▶ Anchor inside the Local Mobility Domain = User ID + interface ID
- ▶ Identifier in the core = user ID





Phase 1 - Device discovery



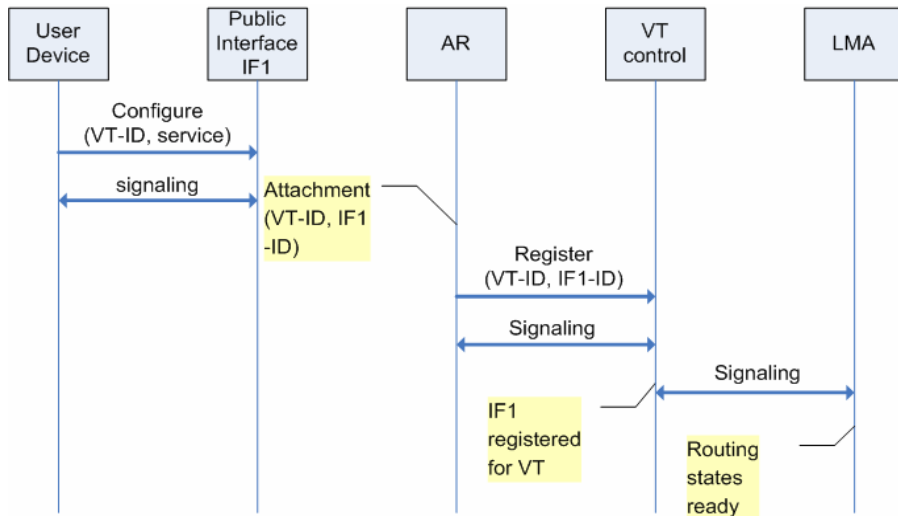
- ▶ We assume the user has one device registered
- ▶ Can be achieved by means of existing protocols, i.e. IETF Simple Service Discovery Protocol





Phase 2 – device configuration

- ▶ Public / user owned device
- ▶ Registration using VT ID and interface ID
- ▶ Configuration to be ready to receive / send traffic
- ▶ Can be done with existing protocols, e.g. CORBA



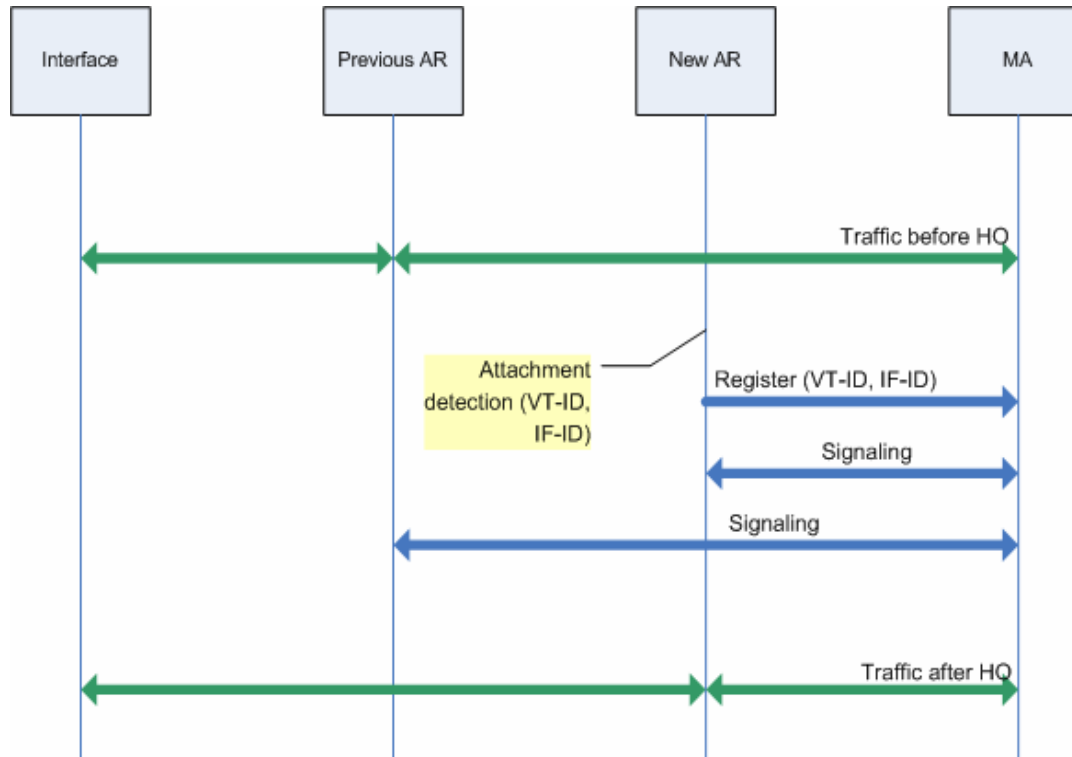


Phase 3 - Policy control

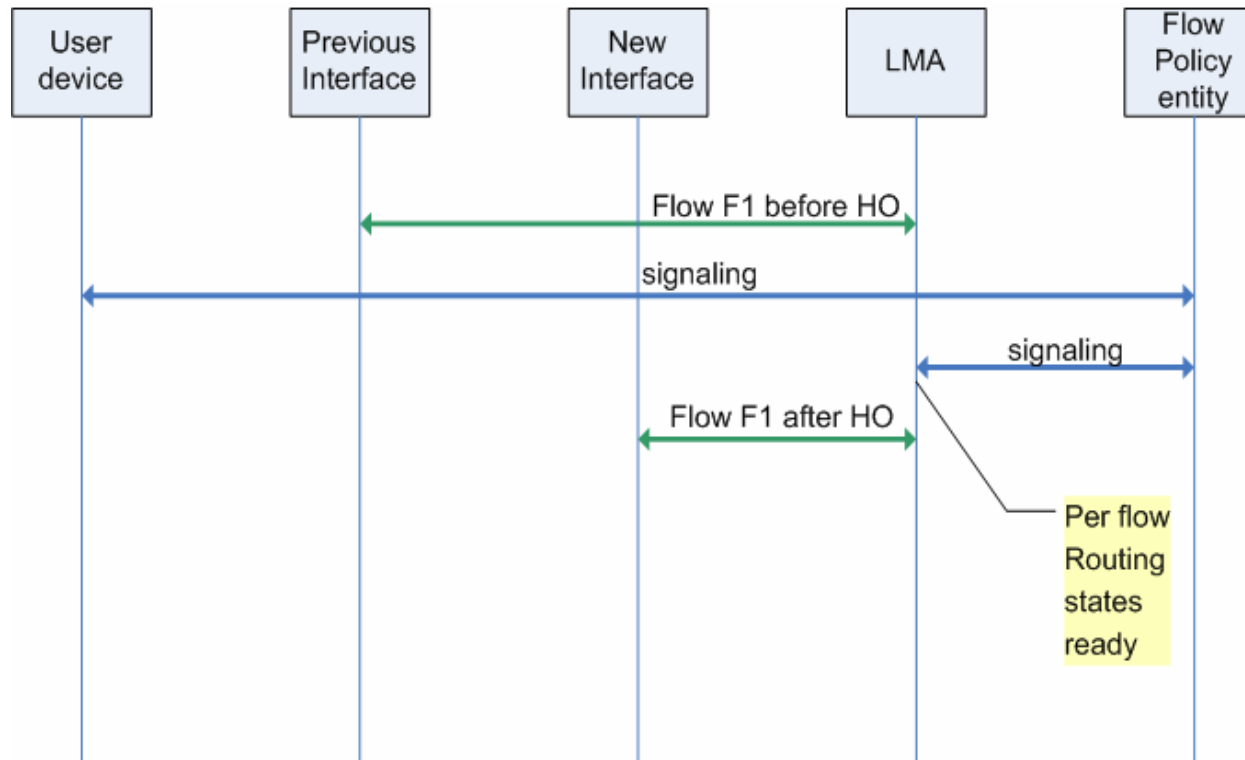
- ▶ Routing policy
 - Per flow routing (e.g. IP and transport 5- tuple)
 - Routing policy uploaded from the user main device towards the LMA
 - Uplink routing handled locally on each device
- ▶ Routing update
 - Interface handover
 - Flow handover



Interface handover



Flow Handover





Security considerations

- ▶ Location privacy
 - NetLMM inherent protection
- ▶ Network security
 - Credentials on several device -> more chances of attacks -> signaling must be bound to the user
- ▶ Several users on the same device
 - OS specific issue





Thank you



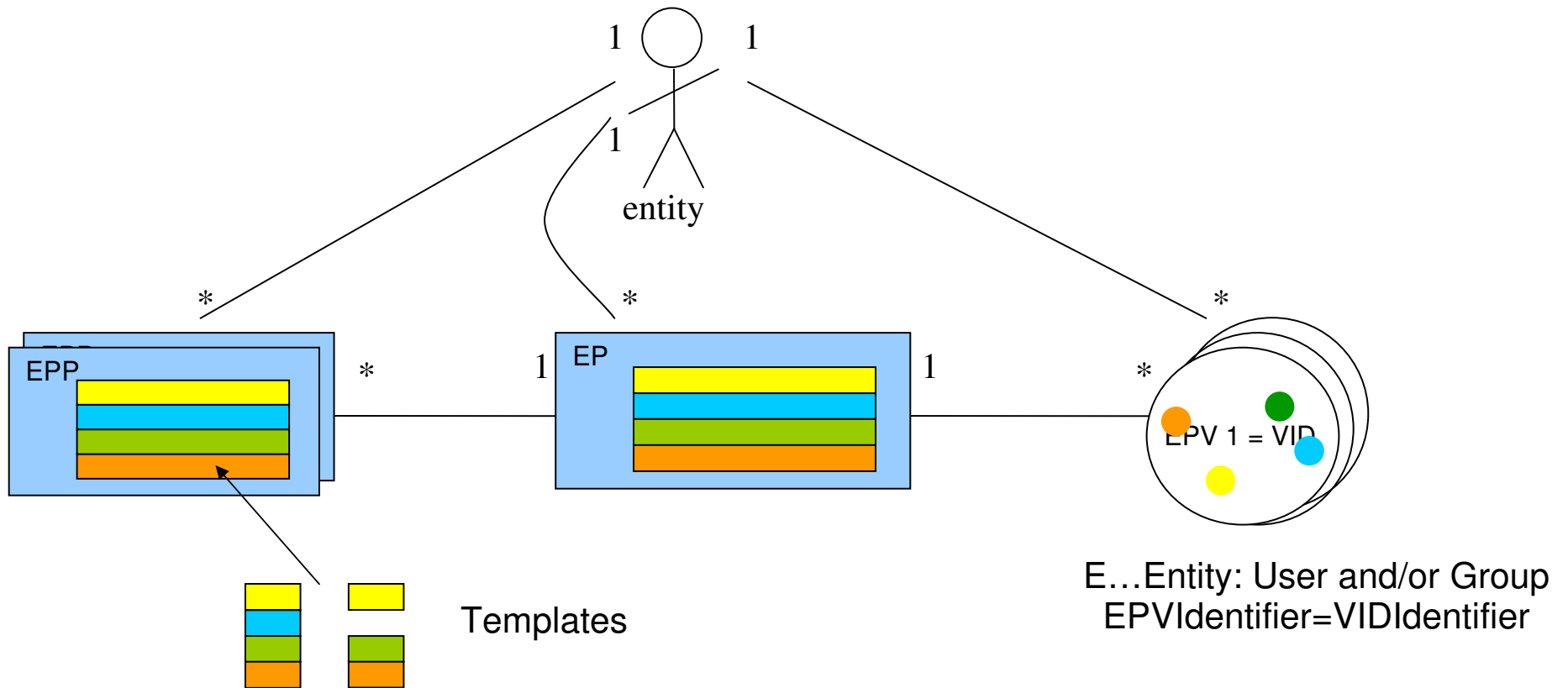


Daidalos VID Details



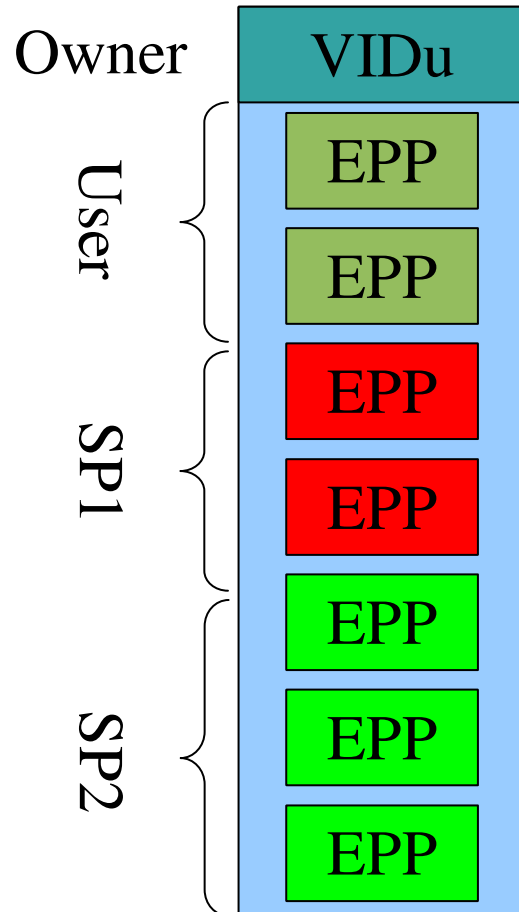


The Model





Ownership

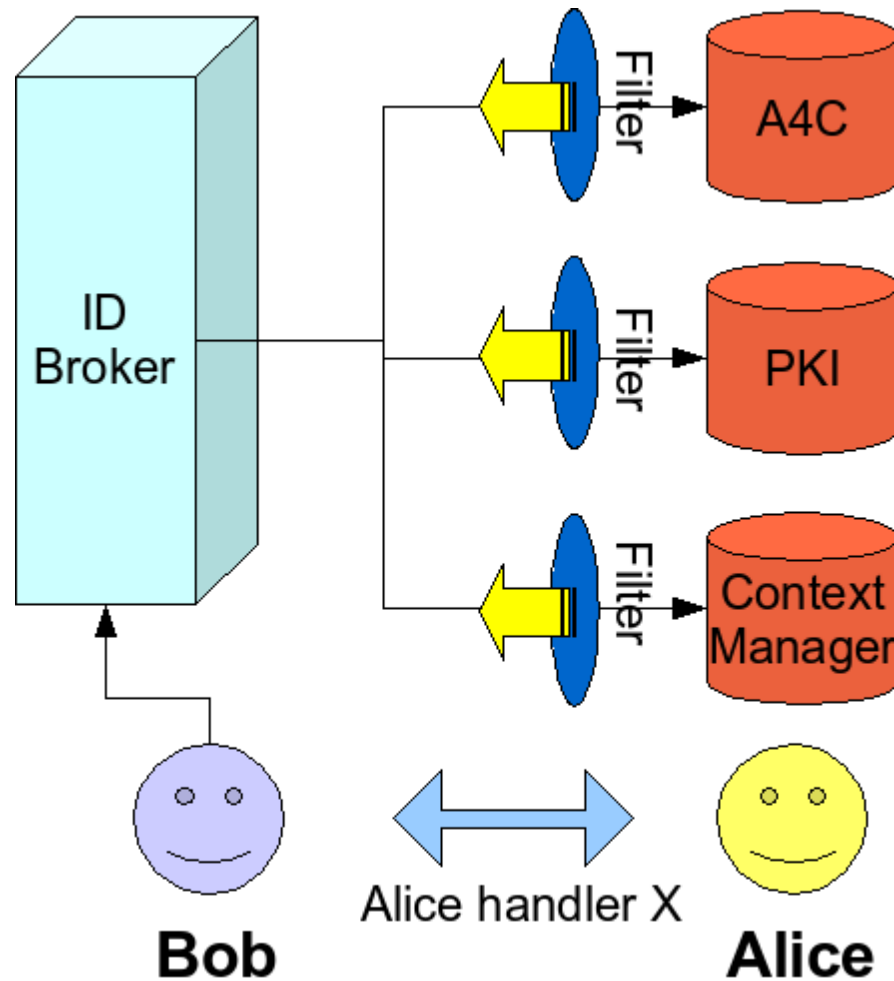


- ▶ The VID can contain EPPs, which are owned by different entities, but relevant to the same VID.
- ▶ Even though the user u “owns” VID u , it does not own all EPPs in it.
- ▶ The user should not be able to modify, for example, metering information related to his network usage.
- ▶ Only the owner of an EPP can set access control rules which affect that EPP.
- ▶ The control of the VID is also under Access Control rules.





Access Control



- ▶ Performed at EPP Attribute granularity
- ▶ Rules
 - Requester
 - Service
 - Context
 - Can be stored as part of the VID
- ▶ Actions
 - Read/Write x Owner/Other/Group
 - Obfuscation
- ▶ FEPV
 - the view the service has of the values contained in the VID



Privacy of Context Information

▶ Activity within Daidalos WP4 A4.5 Security and Privacy

▶ Motivation

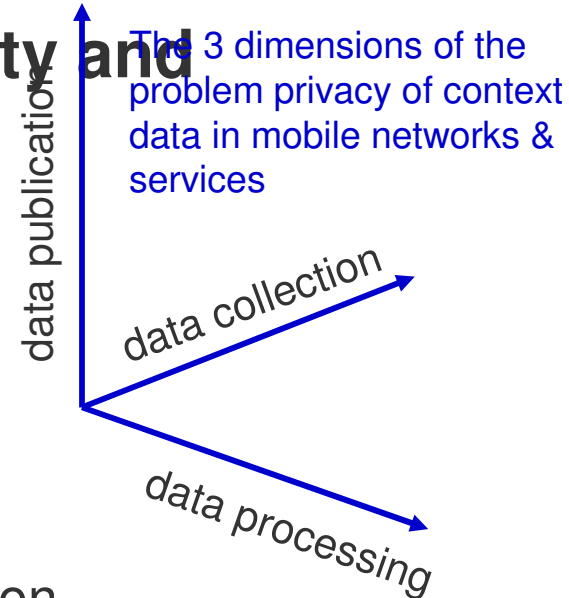
- avoid misuse of context information
- protect privacy
- increase user acceptance

▶ Requirements

- Adequate concealment mechanisms
- give user control to **block or blur** context information

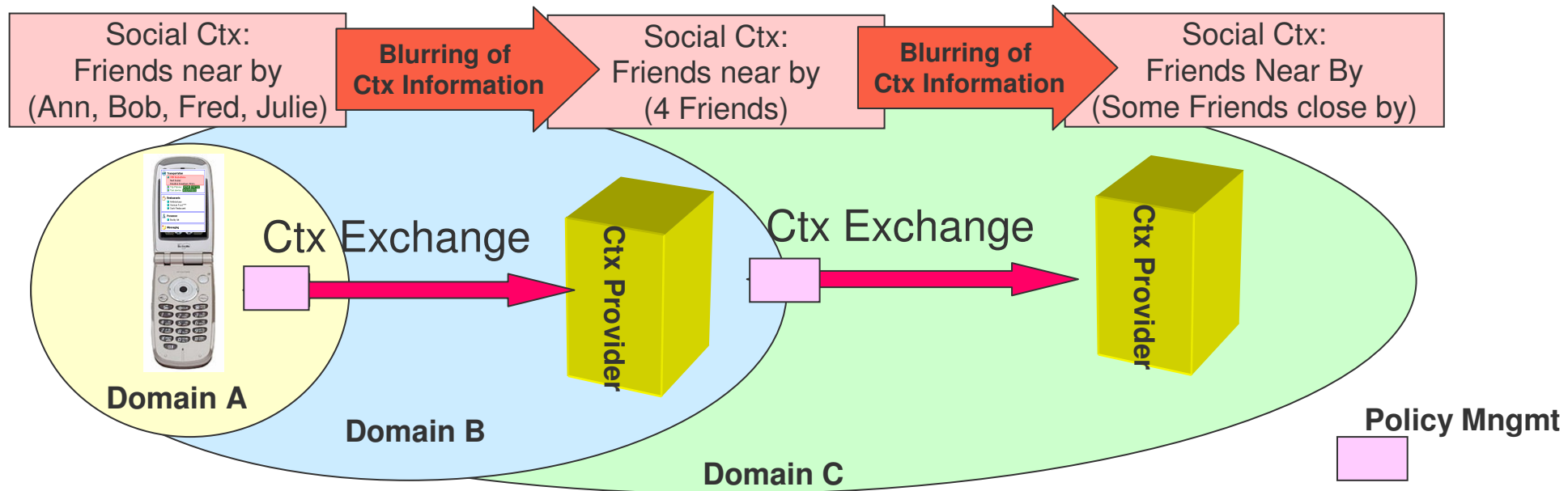
▶ Implications

- privacy policy management to control
 - use of VIDs
 - context exchange within and across domains (Federation)
- Definition of adequate blurring categories and filters
 - which blurring function is available and how to apply (semantics, storage, association with VIDs)





Context Obfuscation



- ▶ **Support privacy of context information based on user preferences**
- ▶ **Incorporate VID concept to support context exchange especially across domains**
- ▶ **Context Obfuscation Challenges**
 - Context does not have any inherent structure that naturally translates to a unified blurring mechanism
 - Semantics (blurring parameters for location distortion may differ in urban or rural areas)
 - Define adequate blurring functions, context filters, translation of relevance values
 - User Interface: Decision support in dynamic environments, trust management, simplicity





Services

▶ VID Wallet

- Encrypted network or local storage of all or part of the information on the user's VIDs.
- Comprises of:
 - VID List
 - VID History
 - VID Credentials

▶ VID Tracking

- Allows a user to submit his VID for tracking in order to understand the associations between his VID and others.

▶ VID Selection

- Choose automatically which of the user's VIDs is best suited for the service he is accessing.





Mobility Management

- ▶ Mobility management framework which takes into consideration:
 - mobility addressing
 - identity as a concept which unites devices, interfaces and flows
 - a hierarchical structure
 - cross-layer relations (link, network, transport and session mobility)
 - cross-layer optimizations
 - scalability
- ▶ Top-down approach to mobility management
 - reactive vs proactive mobility management
 - movement can be correlated across layers (for optimization)

