



# **Cross Layer Linking of names and Identifiers**

**19/11/2007, Heidelberg, Germany**

**Telma Mota (PT Inovação)**

**Alfredo Matos (IT Aveiro)**





# Overview

- ▶ Daidalos Virtual Identity Approach
- ▶ Privacy in the Daidalos architecture
- ▶ Identifiers: Linkage and Correlation
- ▶ Daidalos Approach to Namespaces
- ▶ Daidalos Approach to Identifiers





# The Daidalos Identity Approach

- ▶ VID Framework
  - Fragmented Identity Model
  - Privacy Oriented
  - Virtual Personae
- ▶ Basic Support
  - **Identity Broker**
  - **Identity Manager**
  - Addressing Mechanisms





# Identity Referral

- ▶ Identity Pointer – VIDID
  - 64 bit public Identifier
  - Realm (Home Domain)
  - Identifier (Index)
- ▶ Implicit pointer
  - Embeddable in addressing structures
    - IPv6 addresses, SIP Addresses, etc.
  - Easily resolvable





# Privacy in the Daidalos Architecture

- ▶ No two identifiers belonging to different (virtual) identities can be correlated at any point in the network stack
- ▶ Two Virtual Personae must not be linked or correlated
- ▶ They may exist on the same terminal





# Identifiers: Linkage and Correlation

- ▶ Linkage
  - Two identifiers are mapped to the same Identity if they appear linked
    - Packet inspection in an Access Network
      - **Mac Address Linked to the IP Address**
- ▶ Correlation (or indirect linkage)
  - Two identifiers are mapped together if they are correlated by linked identifiers
    - Packet inspection in an Access Network
      - **Virtual persona uses two different IP addresses, with the same MAC Address**





# The Daidalos Approach

- ▶ Two virtual identities must have a distinct set of identifiers
- ▶ That means
  - Never use the same identifiers on every layer
    - MAC Addresses
    - IP Addresses
    - Home Addresses
    - SIP Addresses
    - ... or even data... EPPs
    - ...





# Bottom Up Approach

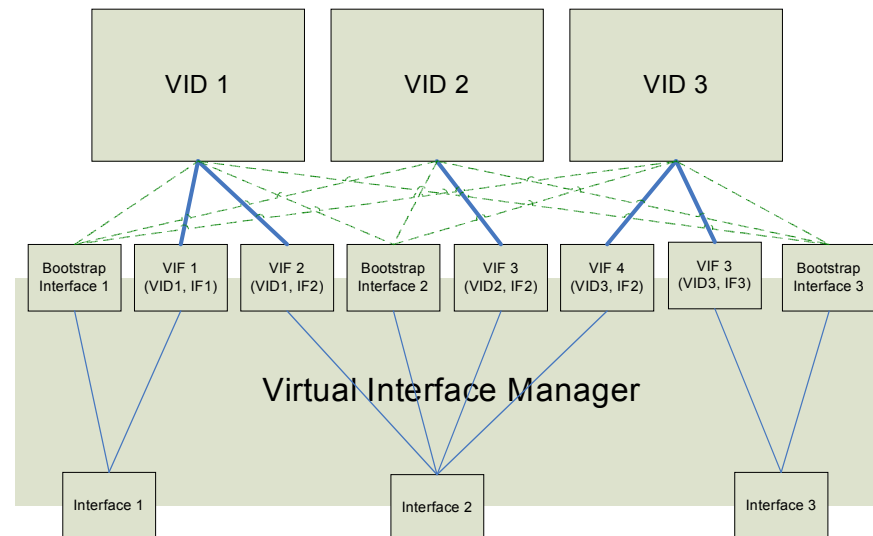
- ▶ Link Layer
  - Mac Addresses, 802.21
- ▶ IP Layer
  - IP address : Care-of Address
- ▶ Transport
  - IP Address: Home Address
- ▶ Application
  - SIP URI





# Link Layer

- ▶ Different Identities different MAC addresses
- ▶ Virtual Interface Proxy (VIP)
  - Generate (virtual) network devices (on the host) for each virtual Identity
  - Each Virtual device has a different hardware address





# IEEE 802.21

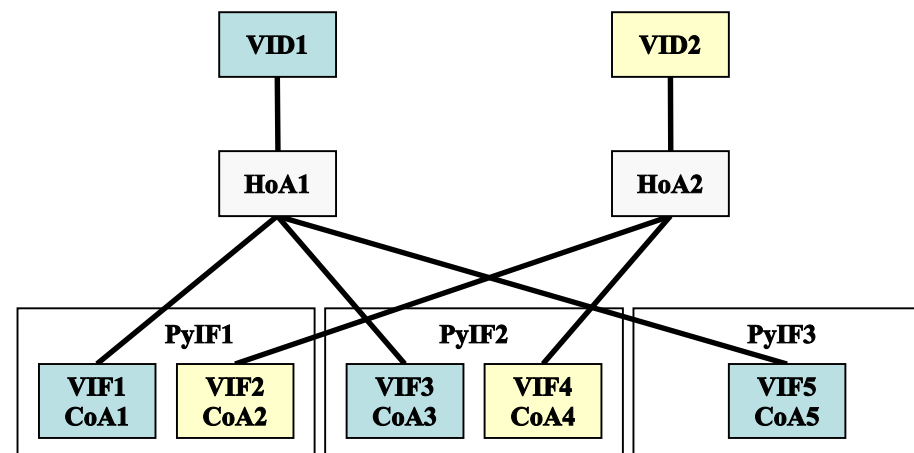
- ▶ Different Identities, different Media Independent Handover Functions (MIHF)
  - Per Identity MIHF registration at the Access Router
  - Per Identity Commands and Events
- ▶ Each (virtual) MIHF Function has a different MIHF\_ID





# Network Layer

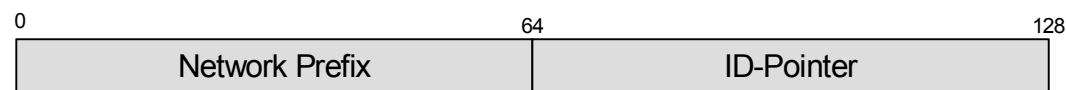
- ▶ Different IPv6 Addresses for each Virtual Interface (VIF)
- ▶ That means:
  - One MIPv6 Care-of, for each VIF, belonging to a particular Identity
  - Multiple MIPv6 registration per terminal
    - As many as virtual identities





# Transport Layer

- ▶ Transport Bindings use MIPv6
- ▶ Different Identities, different Home Addresses
  - For one terminal must manage several HoA's
  - At least one HoA per Virtual Identity
  - Multiple Entries at the home agent
- ▶ HoA is more an Identifier than a Locator
  - Embedded VIDID in the suffix
  - Points to relevant Identity Information
    - User profile, QoS capabilities, Authorization material (detailed in the Identity model)





# Application<sup>↑</sup>

## ▶ SIP URI

- Leads to Identity
- SIP Address  $\Leftrightarrow$  VIDid = Index@realm
- Direct mapping between the HoA and the SIP Address
- Separation between SIP Public and Private identities does not make sense in Daidalos. All identities are private!
- Session Mobility/Portability -> Several Terminals must have the have the same HoA





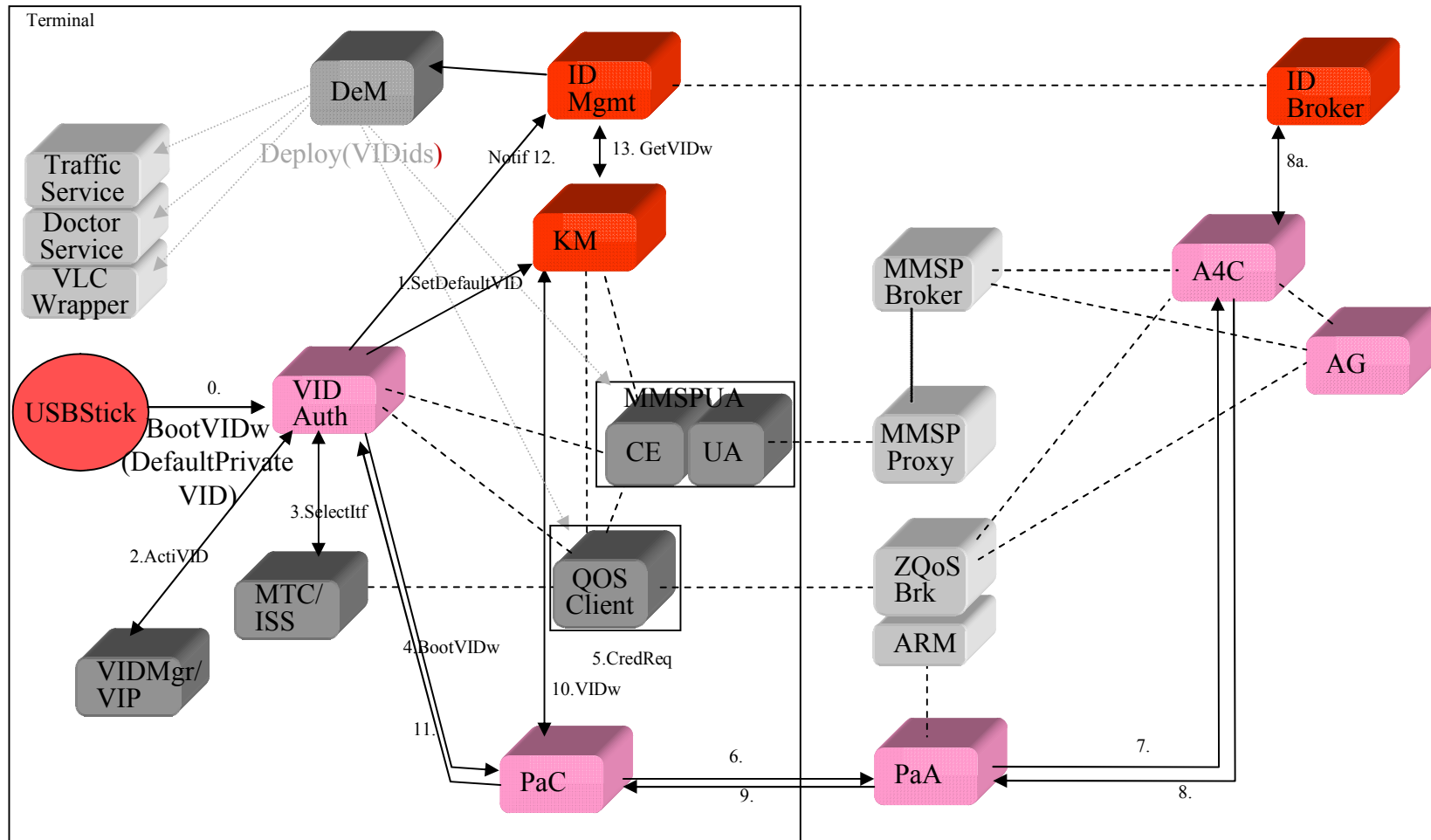
# Daidalos Virtual Terminal

- ▶ The network doesn't see different Identities
  - It sees different terminals
- ▶ Virtual Terminal Concept
  - Each Virtual Identity leverages it's own set of Identifiers
  - The Network relates to different sets, and treats them as different Terminals
  - There is no information on the network that enables the mapping between identities





# Daidalos Privacy Architecture





# Key Benefits

- ▶ Privacy Protection
  - Two identities remain unrelated
  - Actions are not linked together
  - User empowered to leverage different contexts
- ▶ Identity relationship
  - Strong Identity Integration
  - Enhances the Identity Model





# Drawbacks

- ▶ Network Overhead
  - Requires managing extra identifiers sets
  - Each Identity behaves as a virtual terminal
    - Duplicated effort
    - Multiple L2 Associations
    - Multiple IPv6 address configuration
    - Multiple registration at the Home Agent
    - Multiple Handover signaling flows
- ▶ There is no way around this
  - Aggregating signalling flows means linkage
  - The price of privacy





# Conclusions I

- ▶ Privacy is possible but expensive.
- ▶ Limited number of Identities should be available.
- ▶ Unlimited number of “Service Ids” can be available as part of of the VID (EPPs) but very limited privacy is guaranteed in this case.





# Conclusions II

- ▶ No component will be able to easily co-relateVIDs execept the user/terminal and the VIDid Provider  
(exception can be the charging entity – in case of explicit request of the user)
- ▶ Profiles, Preferences, Context, Learning may compromise the concept -> Privacy.

