The Daidalos
Virtual Identity Concept
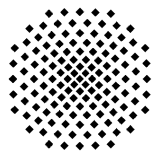
http://www.ist-daidalos.org/

ITG 5.2.4 Workshop
Darmstadt, 25 January 2007

Jochen Kögel

jochen.koegel@ikr.uni-stuttgart.de

Universität Stuttgart

Institute für Kommunikationsnetze und Rechnersysteme (IKR)

Agenda

- ▶ **Daidalos**
  - Project Overview
  - Architecture

- ▶ **Daidalos VID Concept**
  - Identity Model
  - Architecture building blocks

- ▶ **VID as a Vertical Concept**
  - Addresses and Privacy
  - IP address as part of VID

- ▶ **Summary**

Daidalos in FP6/IST

- ▸ EU IST 6th Framework Research Project
  - ● Area: "Mobile & Wireless Systems Beyond 3G"

- ▸ Volume ~ 50 M€ over 5 years and 2 phases
  - ● November 2003 – December 2008

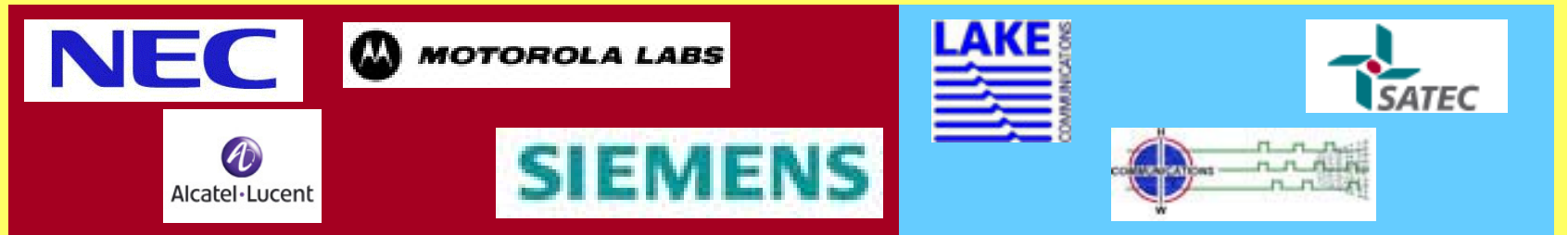- ▸ Currently 36 Partners

- ▸ Lead: Deutsche Telekom AG

Daidalos Consortium

Telco Operators

Industry & SMEs

Research Institutes & Academia

Daidalos Objectives

▸ **Integration of heterogeneous network technologies**
- Establish seamless mobility
- All-IP approach
- Decoupling services from access network and device
- Integrating broadcast as additional access network
- Including ad-hoc, moving and sensor networks.

▸ **Operator driven, with special focus on**
- Interfaces between operators and 3rd party providers
- Federation, accountability
- Measurement framework
- Policy based network management (simplified network administration)

Daidalos Architecture
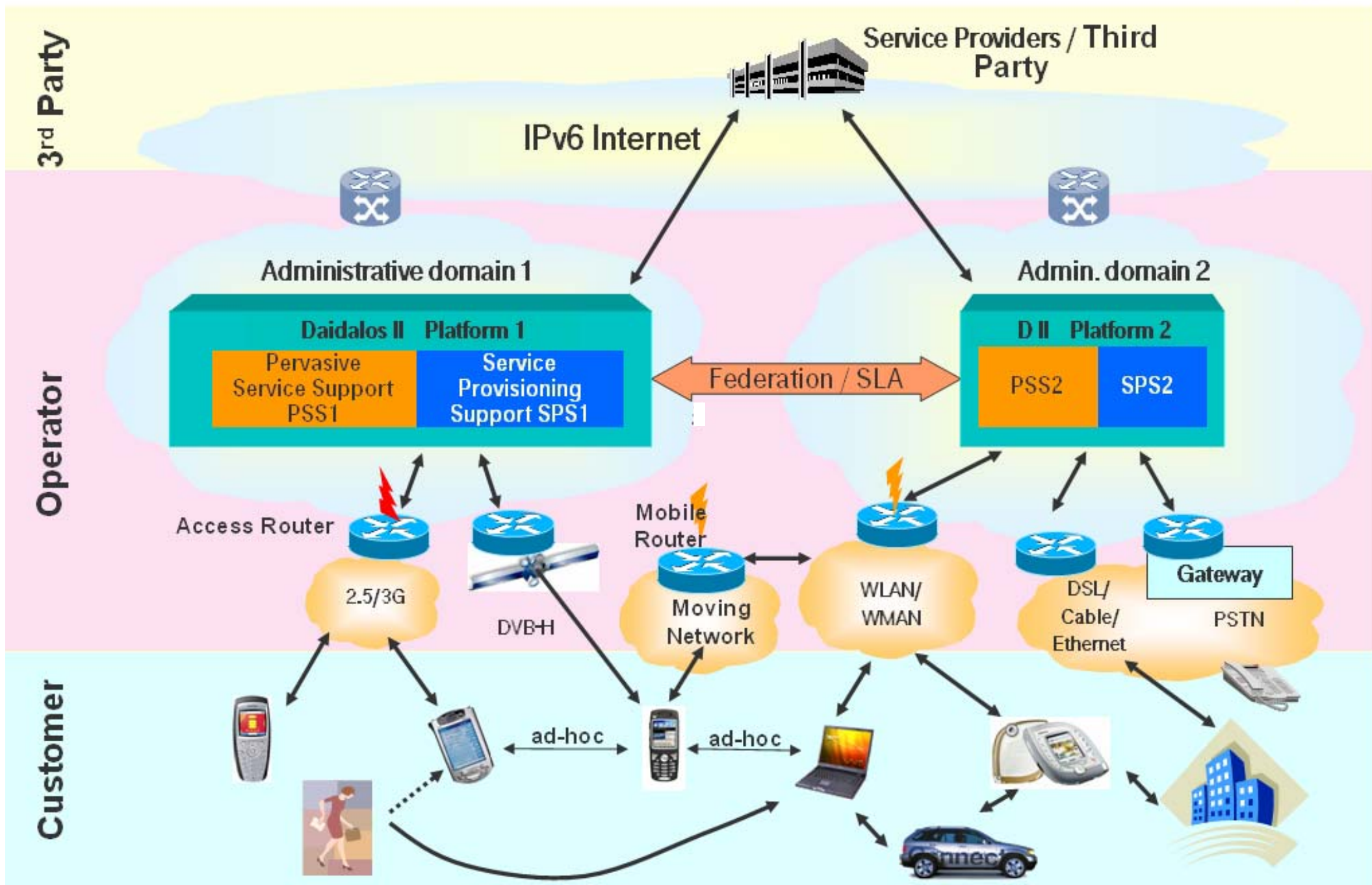
Daidalos – Building Blocks

▸ **Service Provisioning Support (SPS)**

- Mobility Support
- AAA, Auditing and Charging (A4C)
- QoS
- Multimedia Service Support

▸ **Pervasive Service Support (PSS)**

- Context Management
- Personalization and Learning
- Privacy Support
- Service Discovery and Composition
- Runtime Environment

Daidalos Key Concepts

‣ **MARQS** (Mobility Management, AAA, Resource Management, QoS and Security)
- functional integration for end-to-end services across heterogeneous technologies

‣ **VID** (Virtual Identities – personalisation at all levels)
- separates the user from a device, enables flexibility as well as privacy

‣ **USP** (Ubiquitous and Seamless Pervasiveness)
- enabling pervasiveness across personal and embedded devices, and allowing adaptation to changing contexts, movement and user requests

‣ **SIB** (Seamless Integration of Broadcast)
- at both the technology level, such as DVB-S/T-H, and
- at the services level, such TV, carousels and datacast

‣ **Federation** ("*comperation*": competitors in cooperation")
- allowing network operators and service providers to offer and receive services
- allowing players to enter and leave the field in a dynamic business environment
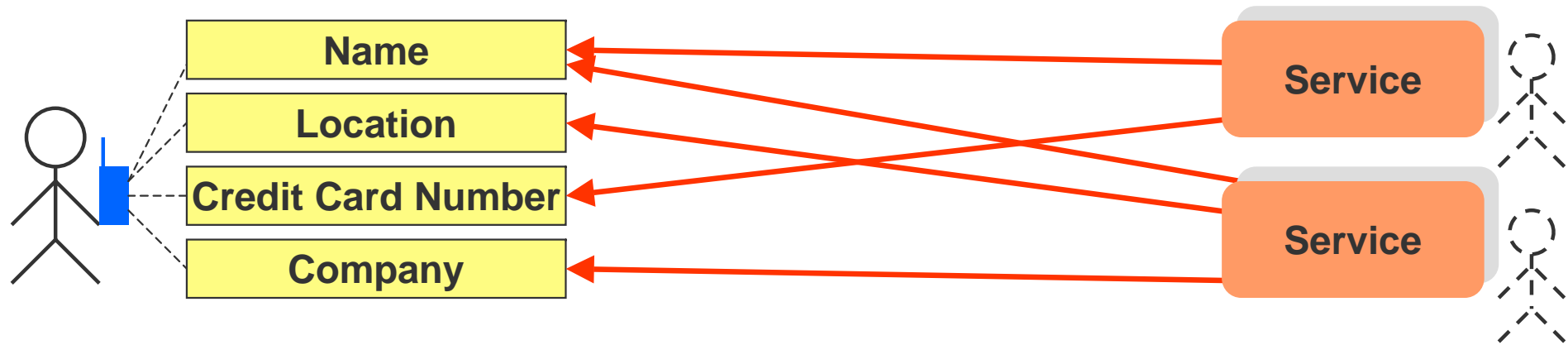
Daidalos VID Concept

VID – Problem Statement

Problem Statement
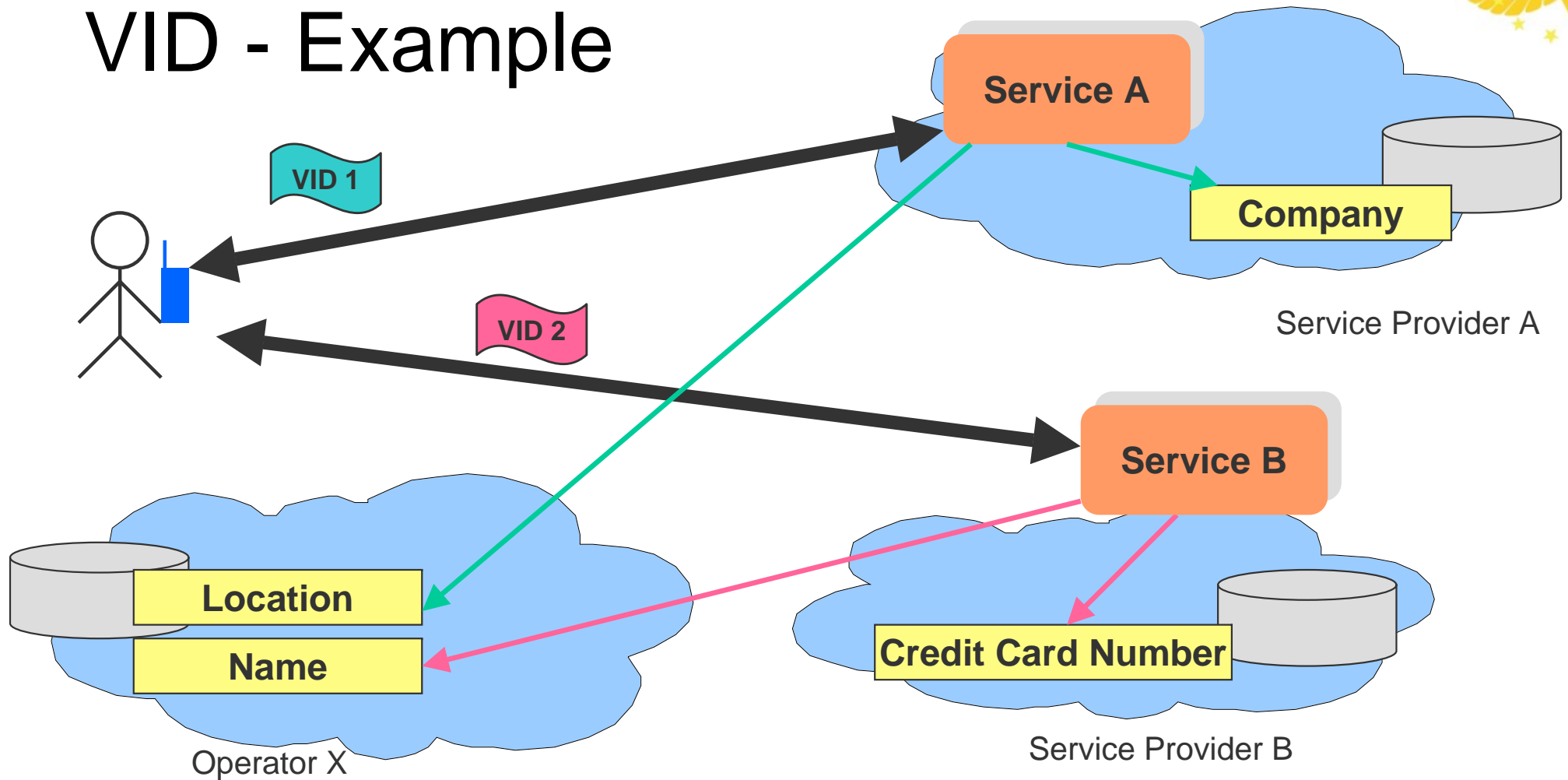
▸ Services operate more and more on privacy-sensitive data

▸ Dynamic business scenarios
- Services offered by unknown (potentially untrusted) 3rd Party Providers

▸ Simple access to services required for users
(platform with mobility support, Single-SignOn, Single-Bill)

→ **User must keep control over data disclosed**
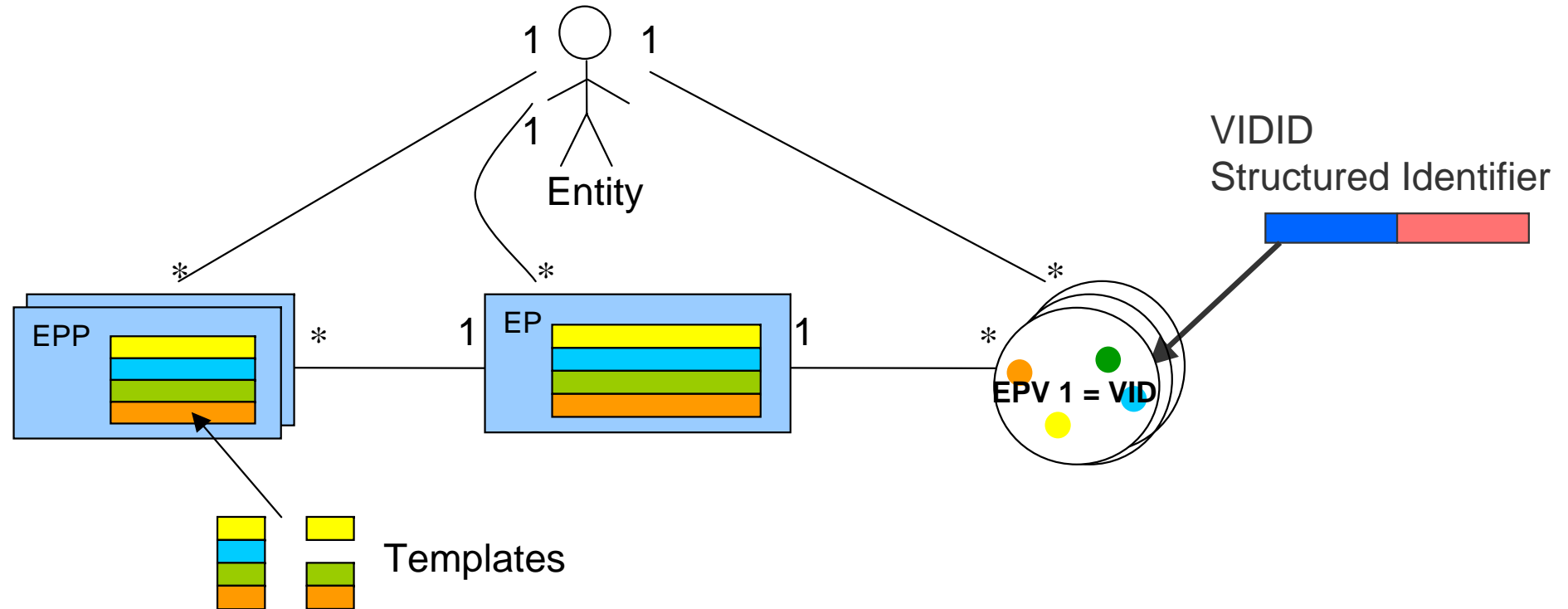
VID - Example

- ▸ Service usage based on Virtual Identities (VIDs)
- ▸ VID selected according to privacy policies (automatically)

Identity Model

E....Entity: User and/or Group

EP: Entity Profile
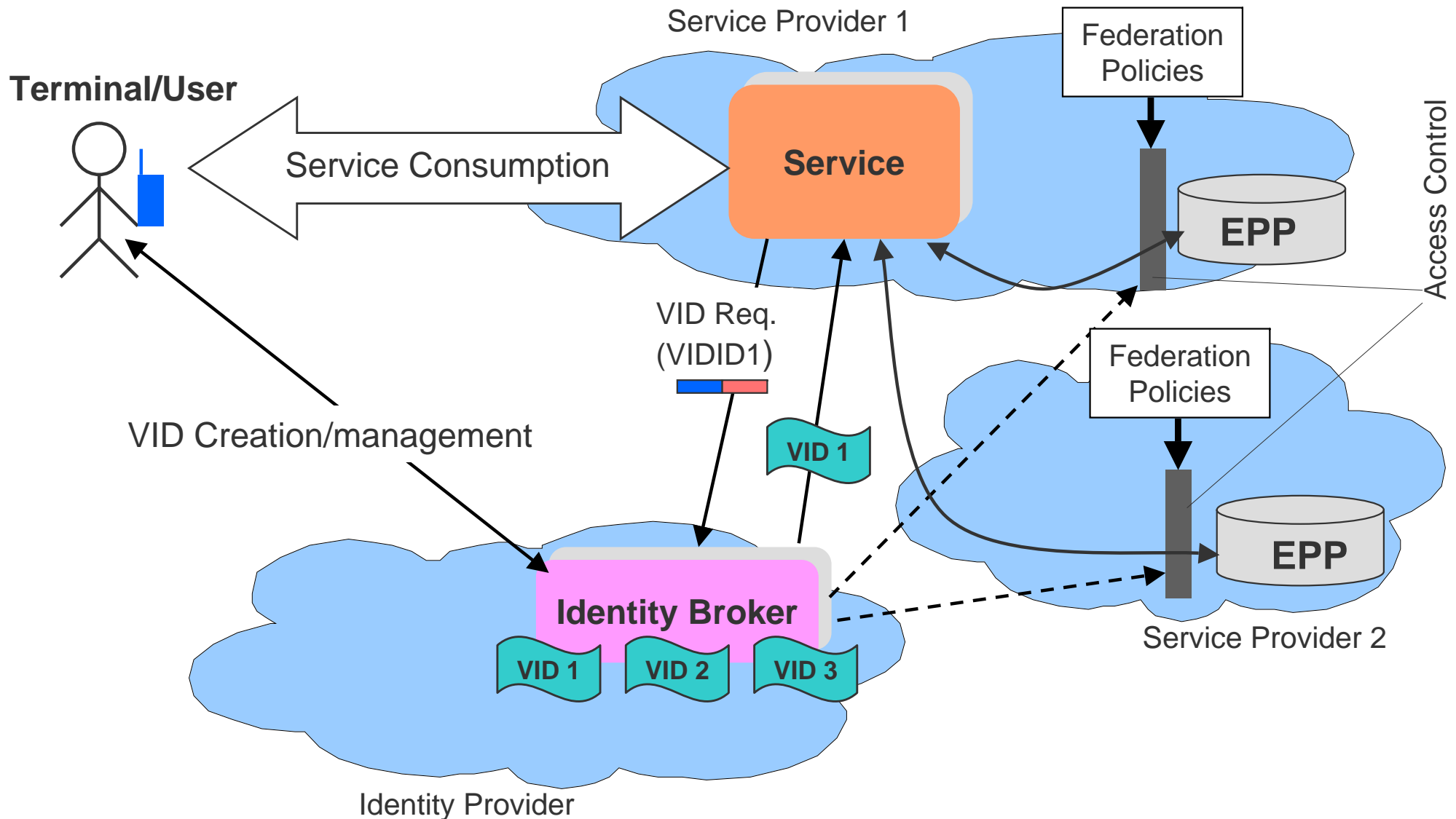
EPP: Entity Profile Part

EPV: Entity Profile View (Virtual Identity)

VIDID: Pointer to EPV

Daidalos VID Concept

VID – Architecture Building Blocks

Service Provider 1

Federation Policies

Terminal/User

Service Consumption

Service

Access Control

EPP

VID Req. (VIDID1)

VID Creation/management

VID 1

Federation Policies

Identity Broker

VID 1   VID 2   VID 3

EPP

Service Provider 2

Identity Provider

VID as a
Vertical Concept

IP Addresses and Privacy

Today

Converged Networks

**Daidalos
VID-enabled Networks**

Dynamic IP (+NAT)
Mobile access: GRX tunnels

One static IP address
- per device/user/contract
- mobility solved on network
  layer **(FMC)**

One IP address per VID

Dial-in
IP

Company
IP

Foreign
IP

GPRS **IP**

Static IP

t_1 t_2

IP 2 VID 2

IP 1 VID 1

VID 3
IP 3

IP 4 VID 4

**Service
Provider**

**Service
Provider**

**Service
Provider**

**Service
Provider**

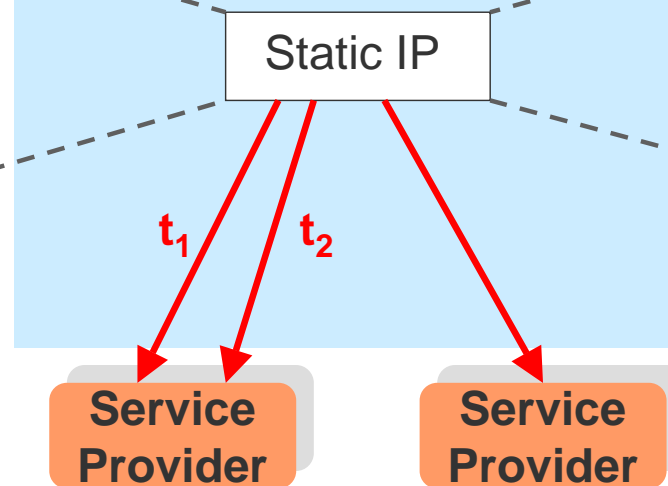**Service
Provider**
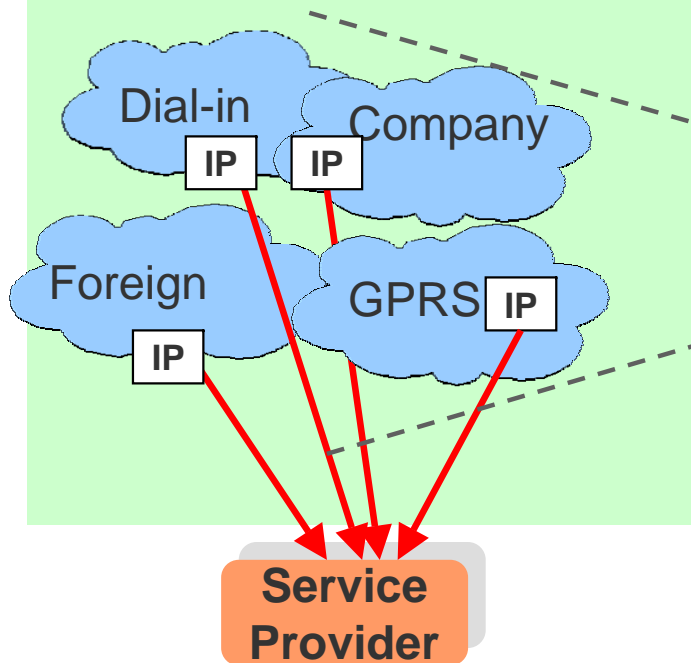
Privacy implications

IP reveals: Rough location,
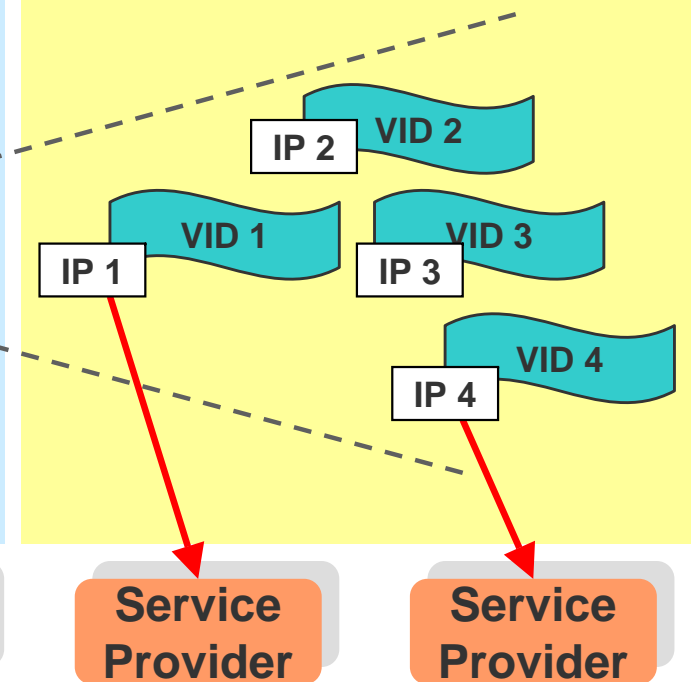company, mobile phone usage
e.g. webshop: customer profile

Perfect linkability based on IP

Hard to link VIDs

IP Address as part of VID

Location

Company

IP Address

VID 1

Service A

Name

Credit Card Number
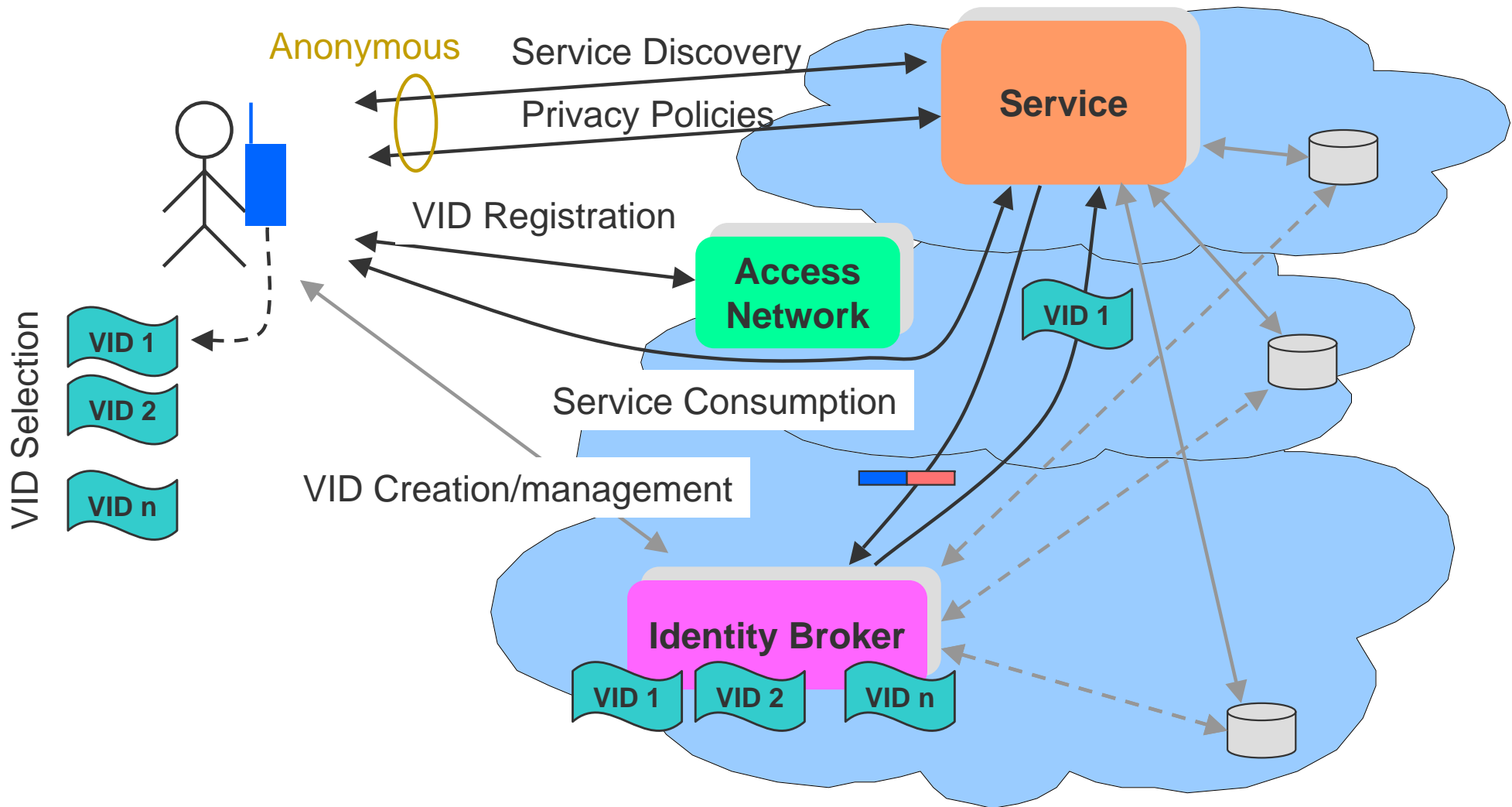
IP Address

VID 2
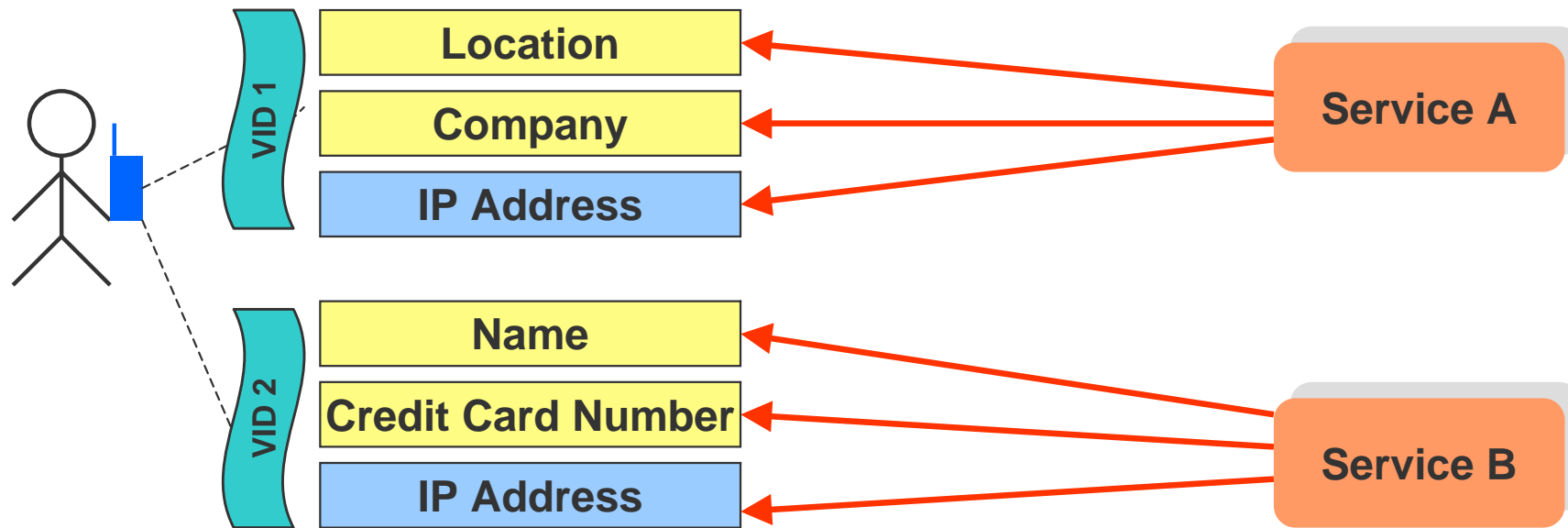
Service B

▸ IP Address (HoA) is EPP
  → is part of VID (contained in service view on user)

▸ Initial contact?
  → Anonymous negotiation of privacy policies necessary

VID – Example Scenario

Anonymous

Service Discovery

Privacy Policies

Service

VID Registration

Access Network

VID Selection

VID 1

VID 2

VID n

Service Consumption

VID 1

VID Creation/management

Identity Broker

VID 1   VID 2   VID n

Summary

Daidalos

▸ Works on a complete beyond 3G platform

▸ Dynamic business scenarios demand for Identity Management as a main building block

VID concept

▸ Vertical concept: privacy for a converged mobile world on the network and service layer

▸ Enhanced user experience:
support for automatic privacy-aware VID selection

▸ No anonymity, but trust in VIDs (accountability)

▸ Will be integrated in all Daidalos subsystems

▸ Combines privacy and personalization

Daidalos VID Concept