PrimeLife

Reference Group Meeting

23-24 March 2009

Activity 6: Privacy in Infrastructures

A research project funded by the European Commission's 7th Framework Programme

Prof. Dr. Kai Rannenberg, Goethe University Frankfurt

ACTIVITY 6 AT A GLANCE

Research Background: Reality Check

- Design of identity related infrastructures (e.g. PKIs) very often neglects specific challenges of infrastructures.
- Examples
  - People rather tend to accept identity management, when it comes
    - with an application or
    - another incentive beyond the identity management solution.
  - An identity management token may have to piggyback on an existing solution, e.g. a widespread piece of hardware, such as
    - SIM cards or
    - smart cards deployed for eGovernment applications.
  - Identity management infrastructures must be interoperable
    - among themselves or
    - with existing legacy solutions.
  - Many applications (also outside of the www, e.g. ring tones for mobile phones or location based services) are being provided by consortia that need some kind of identity management for e.g. charging.

Research Approach

- Rather focus on a solution or solutions, that can be rolled out successfully (including economically successfully) in a large scale even if
  - timescales go beyond the duration of PrimeLife,
  - the infrastructures have less to do with the WWW/Internet
- Examining
  - touching points with existing systems (such as the GSM/UMTS-SIM system, citizen ID/signature cards, and maybe large portal accounts) and
  - the resulting interoperability potentials and challenges
- Designing and implementing infrastructures as a basis for
  - privacy-enhancing IdM and
  - their subsequent establishment.
- Investigating technical and non-technical (e.g. legal, economic) requirements for successfully implementing solutions on top of existing and newly developed infrastructural elements.

Research Objectives

- Enhancing the infrastructures with privacy-enhancing features
- Ensuring privacy-enhancing features can work in the investigated infrastructures
- Aligning identity management solutions and privacy concepts, leveraging e.g. trusted base infrastructures to support privacy concepts
- In an economically relevant and successful manner

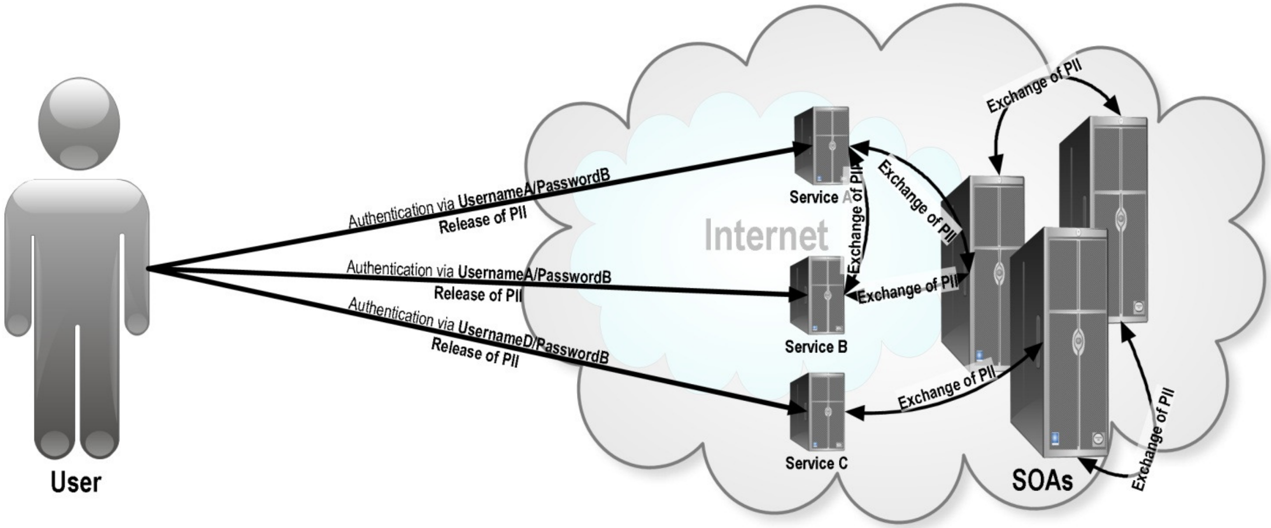
WPs & Participants

- WP6.1 Privacy-preserving identity management for service architectures
  - **GUF**, EMIC, GD, SAP, ULD
- WP6.2 Trusted Infrastructure elements
  - **GD**, GUF, ULD
- WP6.3 Service composition
  - **EMIC**, GD, GUF, SAP, ULD

Dr. Marc-Michael Bergfeld, Giesecke & Devrient

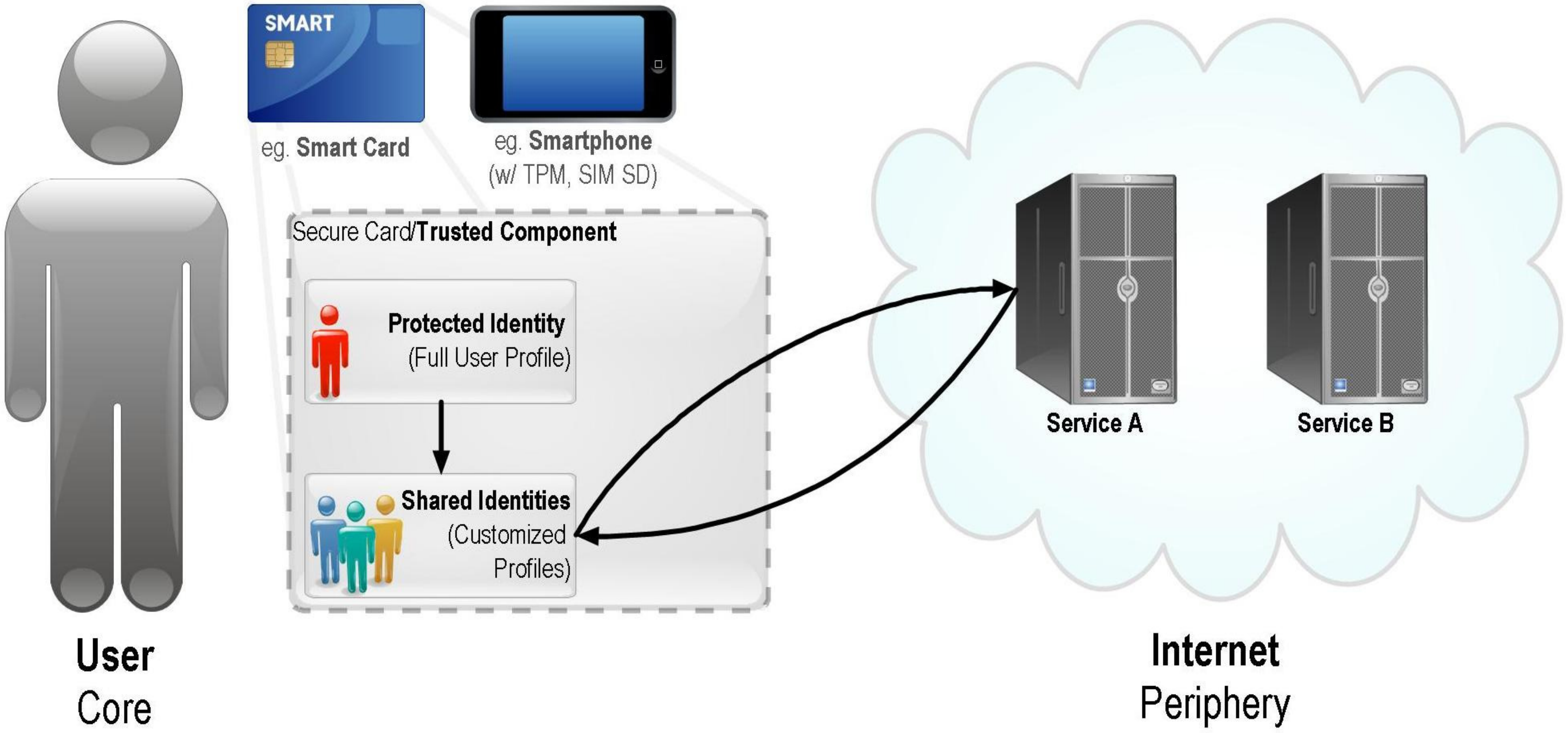
TRUSTED INFRASTRUCTURE

The current scenario



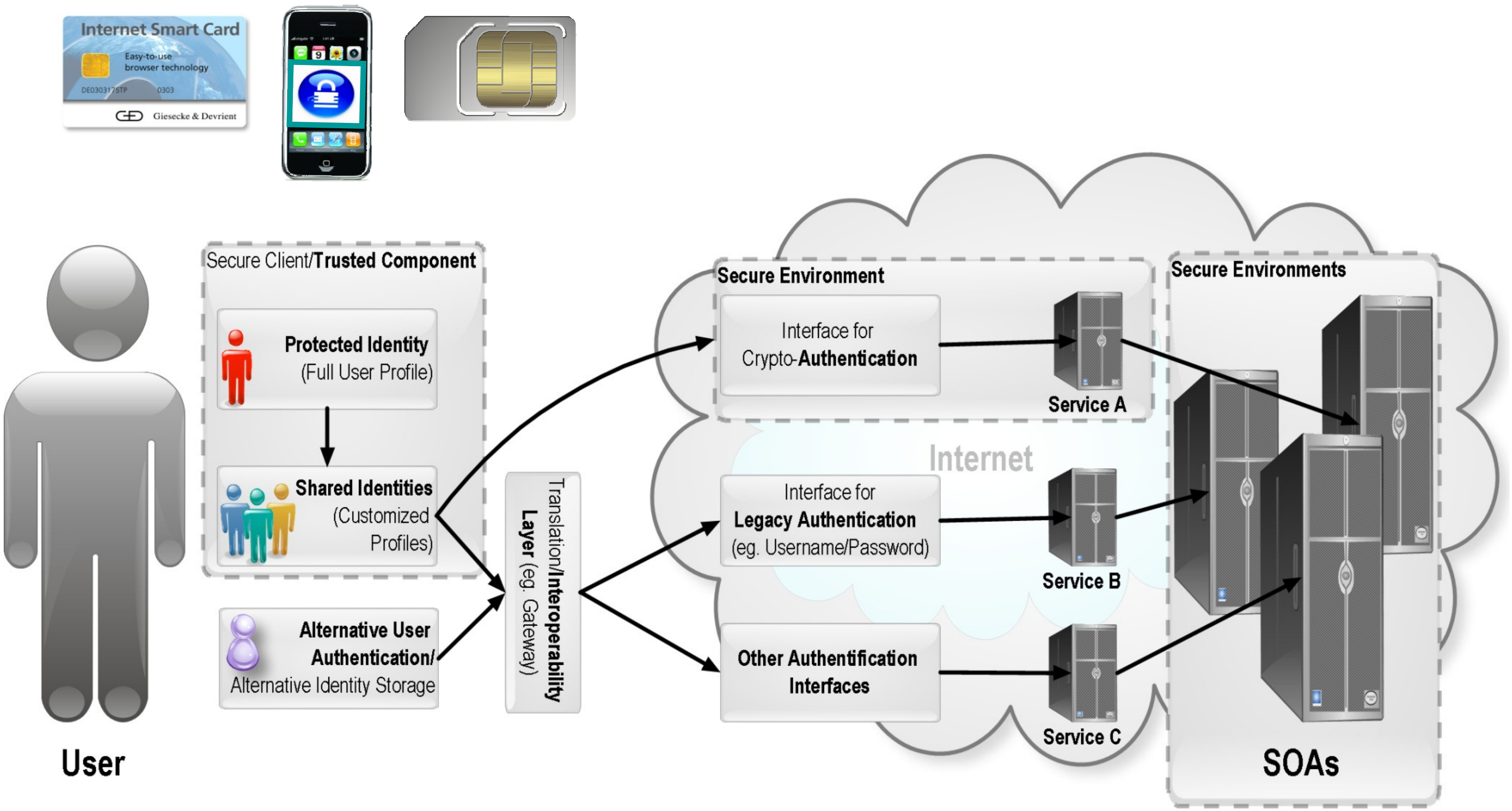
Source: Deliverable 6.2.1

Managing different identities from one protected core data set



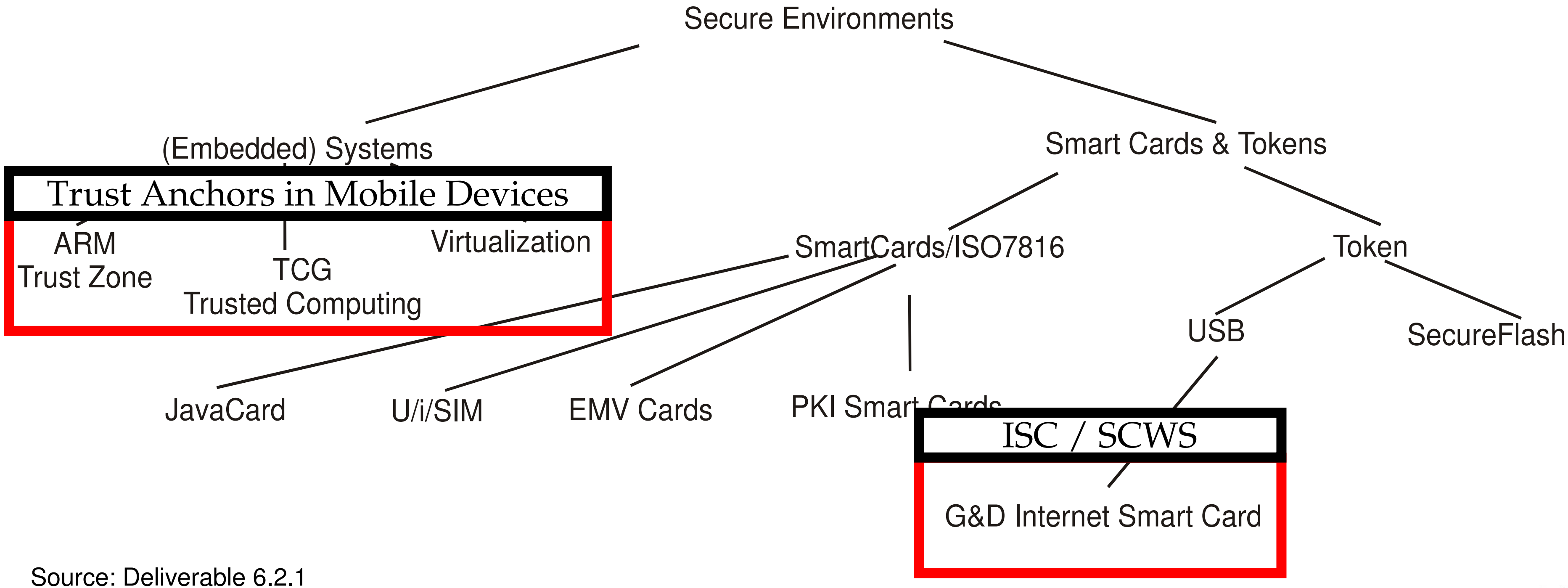
Source: Deliverable 6.2.1

Security of Service enhanced by Trusted Devices



Source: Deliverable 6.2.1

Infrastructure technologies to protect privacy and manage identity



Secure Environments

(Embedded) Systems

Trust Anchors in Mobile Devices

ARM Trust Zone

TCG Trusted Computing

Virtualization

Smart Cards & Tokens

SmartCards/ISO7816

Token

USB

SecureFlash

JavaCard

U/i/SIM

EMV Cards

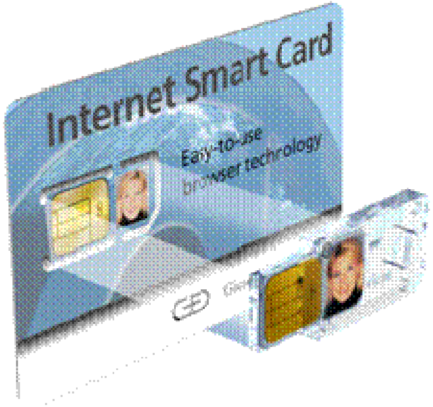
PKI Smart Cards

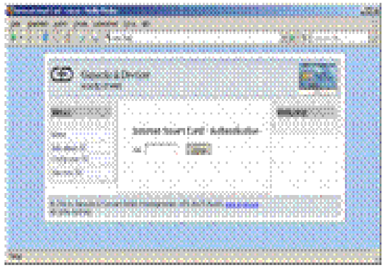
ISC / SCWS

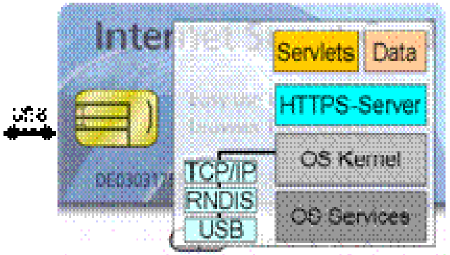
G&D Internet Smart Card

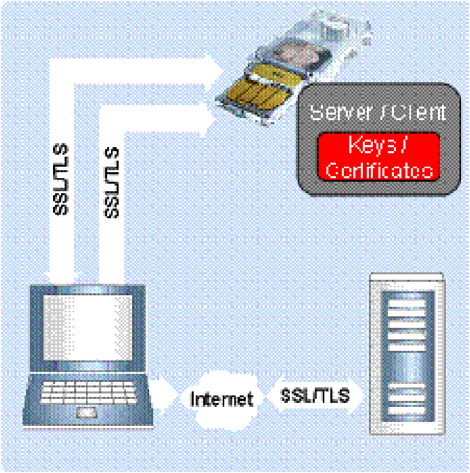
Source: Deliverable 6.2.1

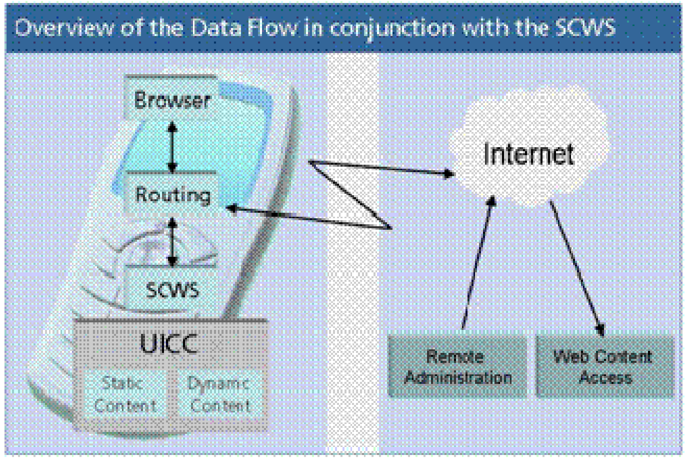
The G&D Internet Smart Card & Smart Card Web Server





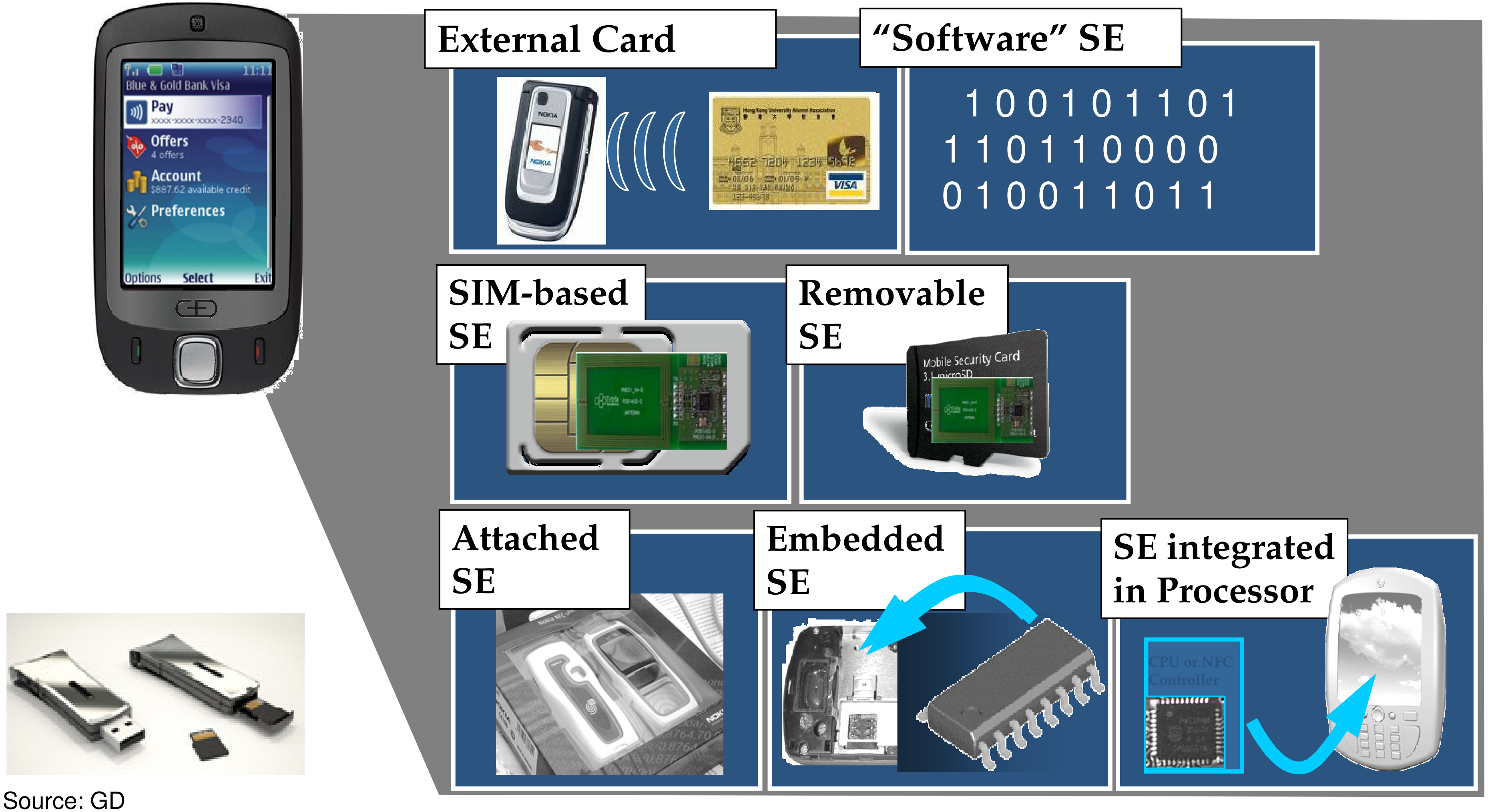






Source: Heartbeat 6.2.1

Potential Trust Anchors for Mobile Devices



Source: GD

This Meeting is YOUR Meeting

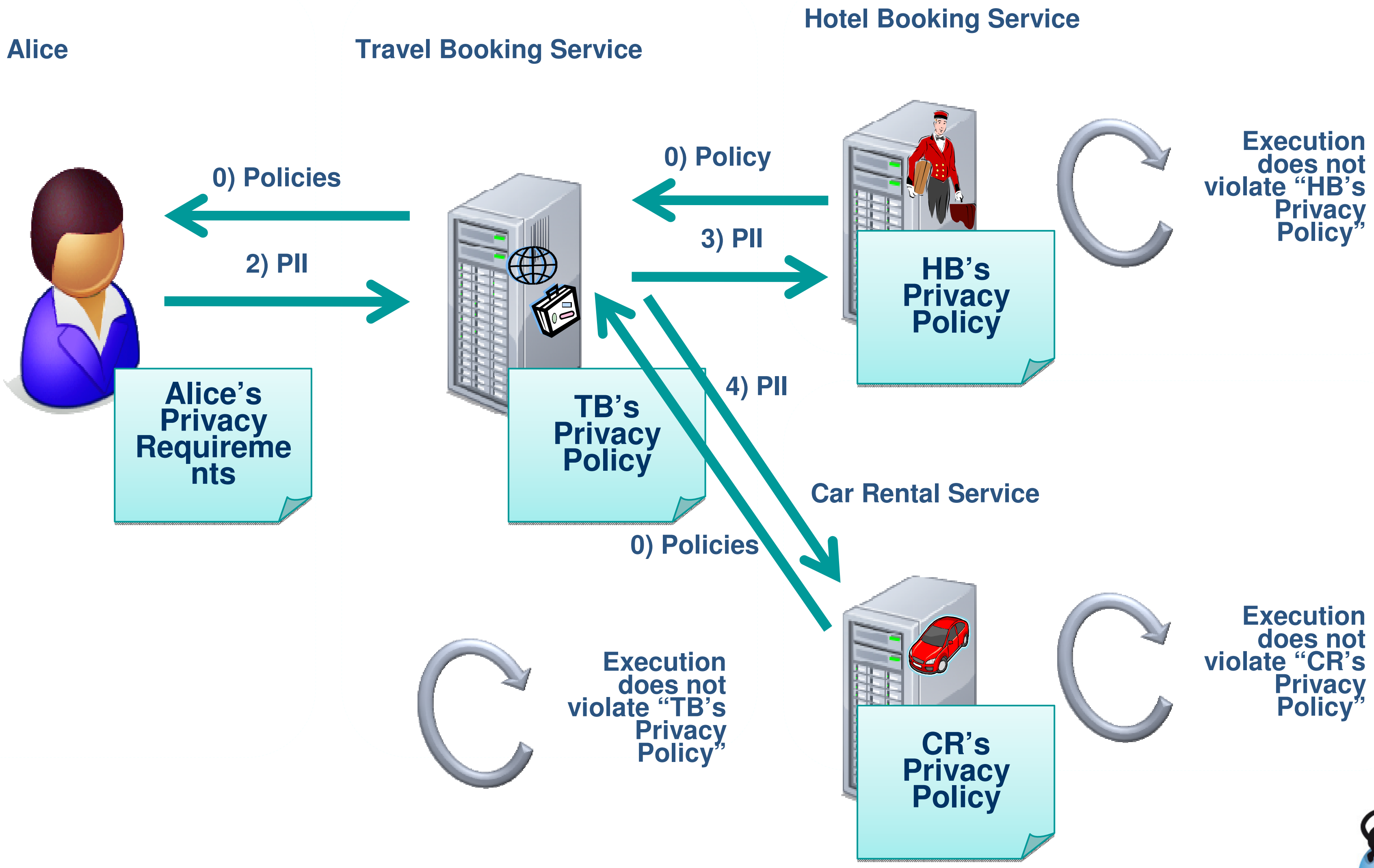
Our questions:

- How do you see the distribution of data between mobile devices and backend / web-based services?
- On which module should privacy & identity management be assured?

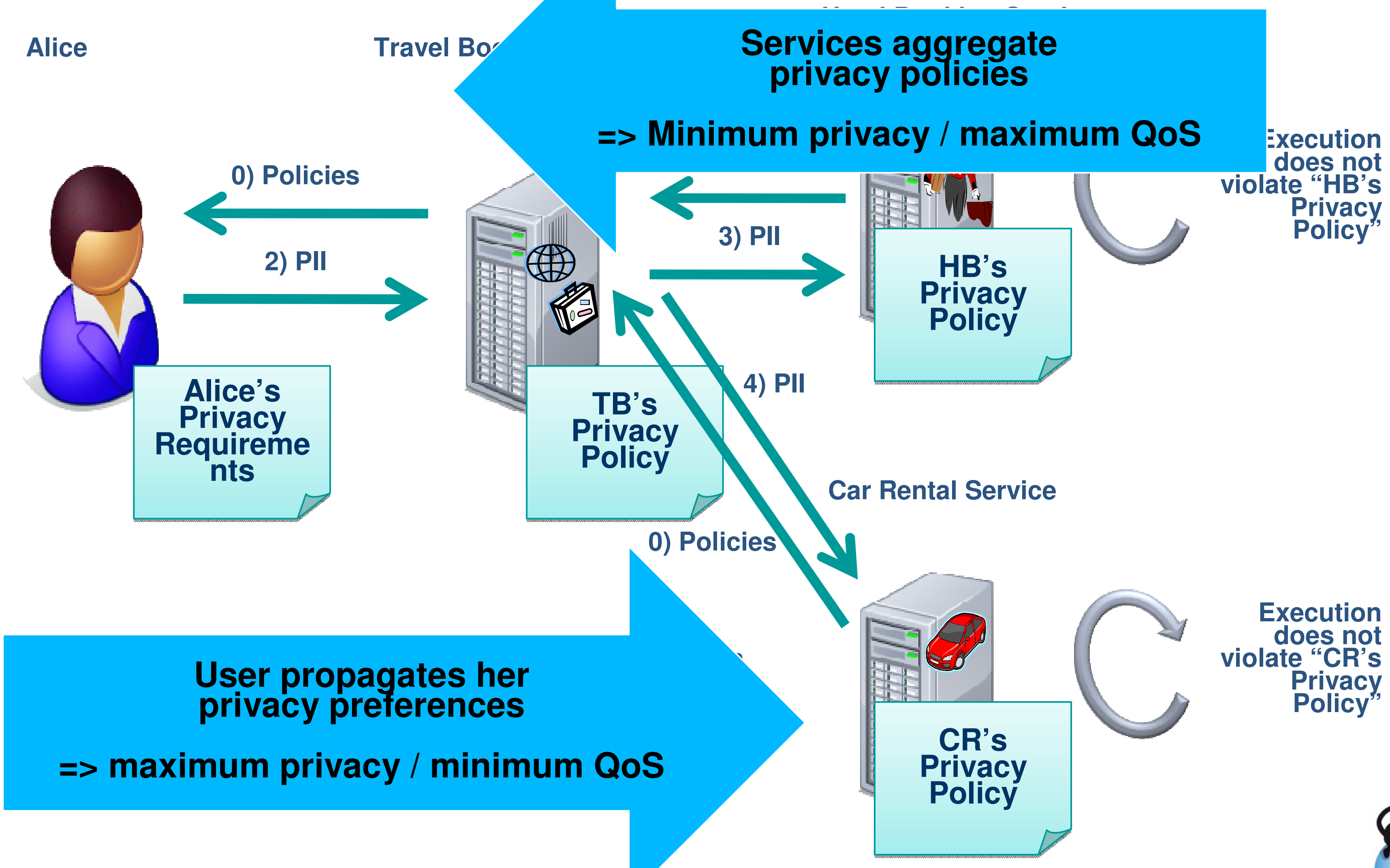
Dr. Ulrich Pinsdorf, European Microsoft Innovation Center

PRIVACY IN SERVICE COMPOSITIONS

Motivation


Alice
Travel Booking Service
Hotel Booking Service
0) Policies
2) PII
0) Policy
3) PII
4) PII
0) Policies
Car Rental Service
Alice's Privacy Requirements
TB's Privacy Policy
HB's Privacy Policy
CR's Privacy Policy
Execution does not violate "HB's Privacy Policy"
Execution does not violate "CR's Privacy Policy"
Execution does not violate "TB's Privacy Policy"

Motivation



Services aggregate privacy policies

=> Minimum privacy / maximum QoS

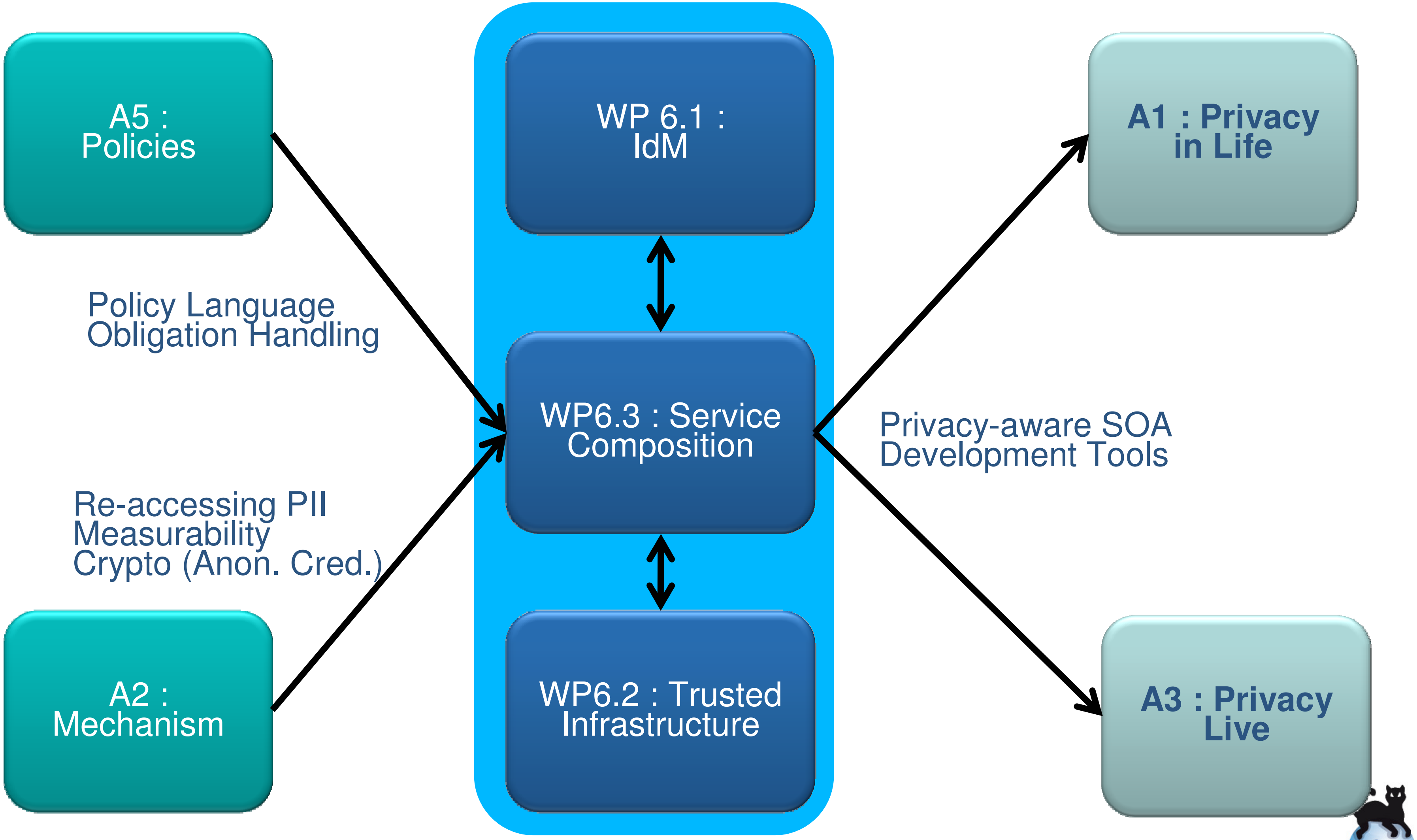
User propagates her privacy preferences

=> maximum privacy / minimum QoS

WP “Service Composition”

- Mission
  - Privacy implications that are specific to service oriented architectures
  - Enforce control on users’ PII even in dynamic services compositions
  - Leverage IdM and trusted devices in such scenarios
- Expected results
  - Mechanisms for policy composition
  - Mechanisms to enforce privacy policies at runtime
  - Toolset for designing privacy-respecting distributed systems
  - Validation in example scenario

Cooperation in PrimeLife



Privacy & Security Requirements

- 39 Requirements on Security & Trust in SOA
- Grouped in categories
  - Core Requirements
  - Privacy Logging Requirements
  - Requirements on Access of Primary Information
  - Cross-Domain-specific Requirements
  - Requirements for Additional Mechanisms
- Reflecting both legal and technical aspects

PrimeLife

Privacy and Identity Management in Europe for Life

Requirements for privacy-enhancing Service-oriented architectures

Editors:	Sebastian Meissner (ULD) Jan Schallaböck (ULD)
Reviewers:	Carine Bournez, (W3C) Claudio Ardagna, (UniMi)
Identifier:	H6.3.1
Type:	Heartbeat
Class:	Public
Date:	February 27, 2009

Abstract

Service-oriented architectures expose new chances and challenges for privacy and data protection. The potentially increased distribution of personal information across multiple domains make subject access requests difficult to handle. Which service did process what data? Whom to address for liability issues? At the same time, the service orientation offers a new approach for the granularity of data processing, allowing clearer responsibilities and better auditing.

This deliverable develops a comprehensive set of requirements for Service-oriented architectures. If applied in the construction of Service-oriented architectures, legal compliance with privacy legislation should be facilitated. Even more, they offer additional support for privacy enhancing Service-oriented architectures.

Copyright © 2008 by the PrimeLife Consortium

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 216483.

SEVENTH FRAMEWORK PROGRAMME

Selected Requirements

- It must be possible to maintain communicated policies even if the Service Oriented Architecture is dynamically adapted. – Req. 25

- A service provider whose service is a downstream part (those that process data later) of the overall workflow must adhere to policies given by service providers whose services are upstream parts (those that process data first) of the workflow. – Req. 27

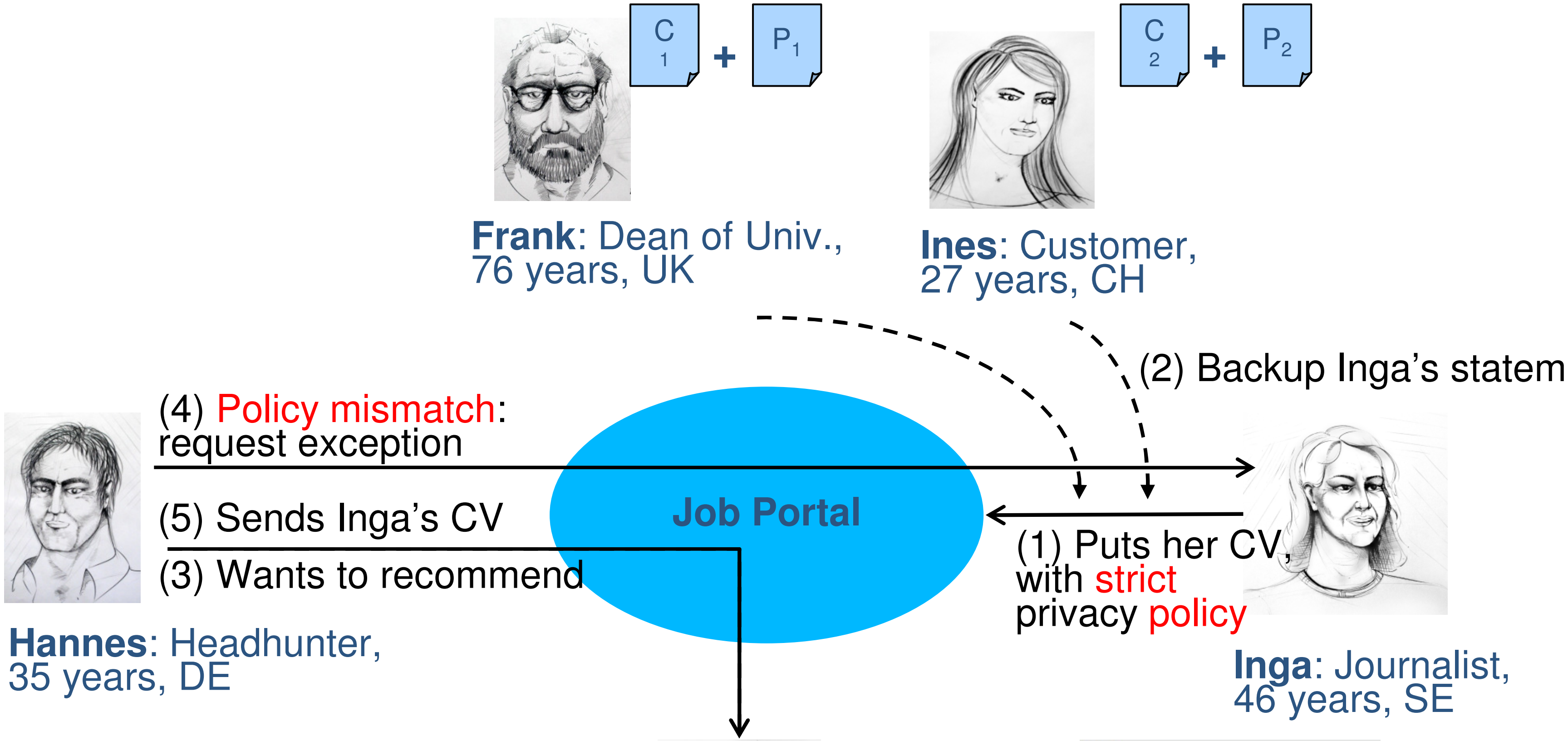
- The ability of the data subject to have access to information must be ensured for the future. – Req. 29

Scenario Selection

- Featuring the prioritized requirements
- Composition of policies on data source side
- Composition of services on data sink side
- Featuring trusted devices and IdM
- Matching of privacy policies and preferences
- Enable user to stay in control over her PII
- Good alignment with work in other Activities
- Scenario-wise complementary to Activity 1

=> Job recommendation scenario (“eCV scenario”)

Scenario



Frank: Dean of Univ., 76 years, UK

Ines: Customer, 27 years, CH

(2) Backup Inga’s statements

(4) Policy mismatch: request exception

(5) Sends Inga’s CV

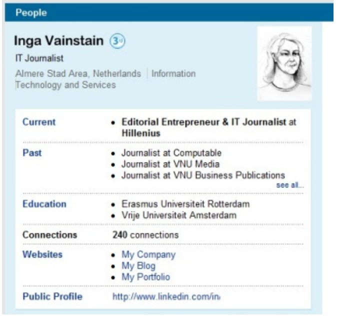
(3) Wants to recommend

(1) Puts her CV, with strict privacy policy

Hannes: Headhunter, 35 years, DE

Inga: Journalist, 46 years, SE

Florence: Manager, 42 years, FR



People

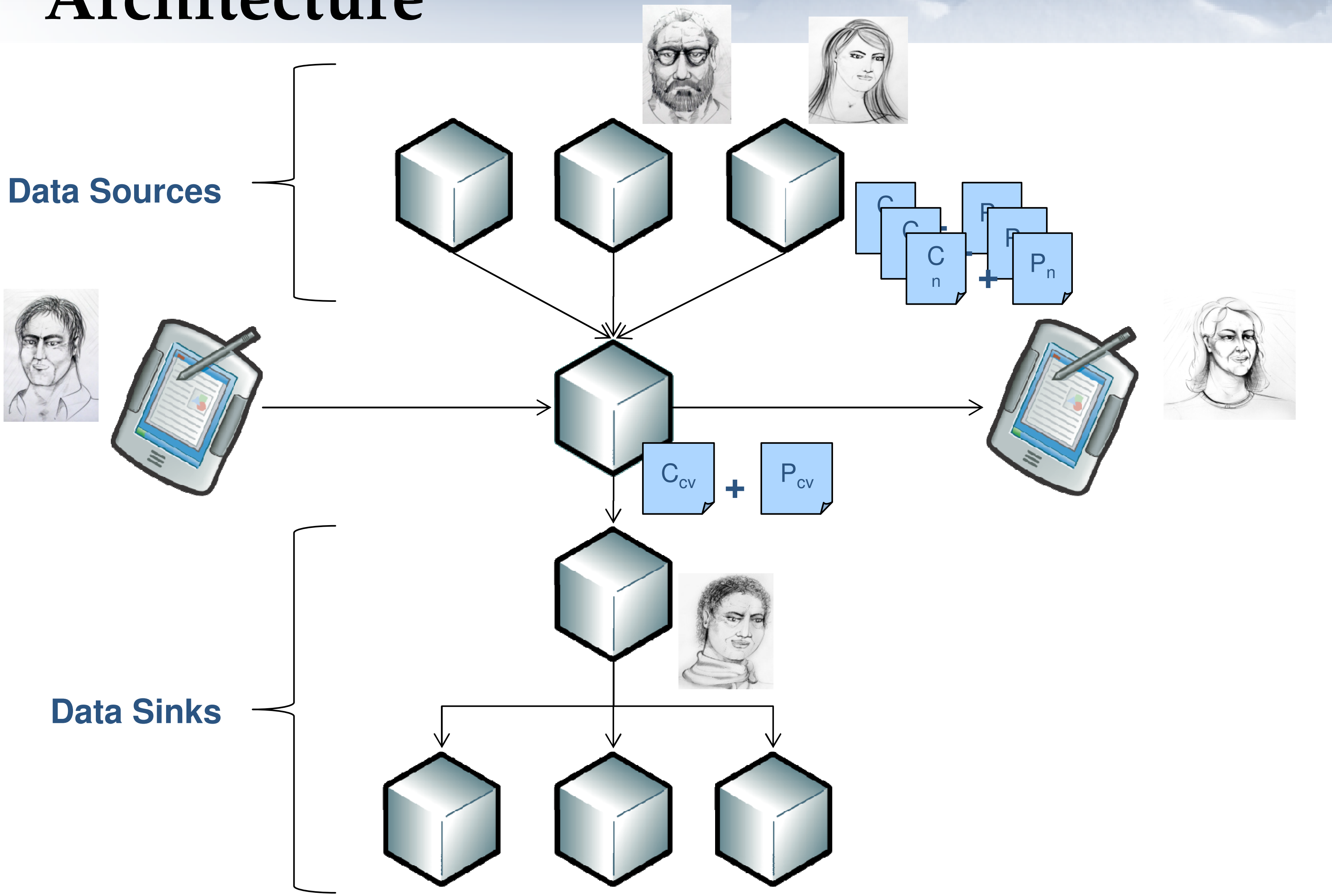
Inga Vainstain 3rd

IT Journalist

Almere Stad Area, Netherlands | Information Technology and Services

Current	**Editorial Entrepreneur & IT Journalist at Hillenius**
Past	Journalist at Computable Journalist at VNU Media Journalist at VNU Business Publications see all...
Education	Erasmus Universiteit Rotterdam Vrije Universiteit Amsterdam
Connections	240 connections
Websites	My Company My Blog My Portfolio
Public Profile	http://www.linkedin.com/in/

Architecture



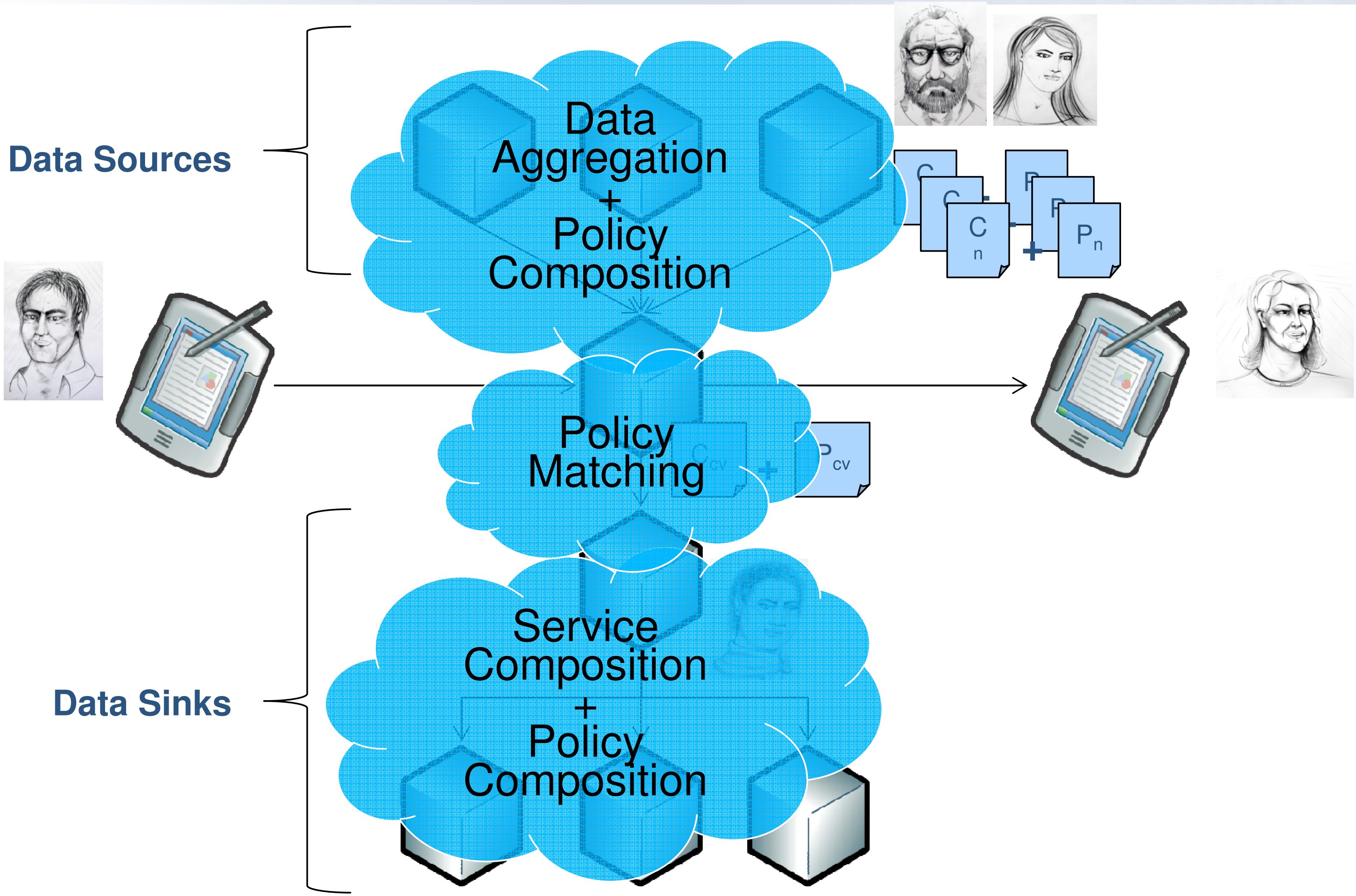
Data Sources

Data Sinks

C_n + P_n

C_{cv} + P_{cv}

Architecture



Data Sources

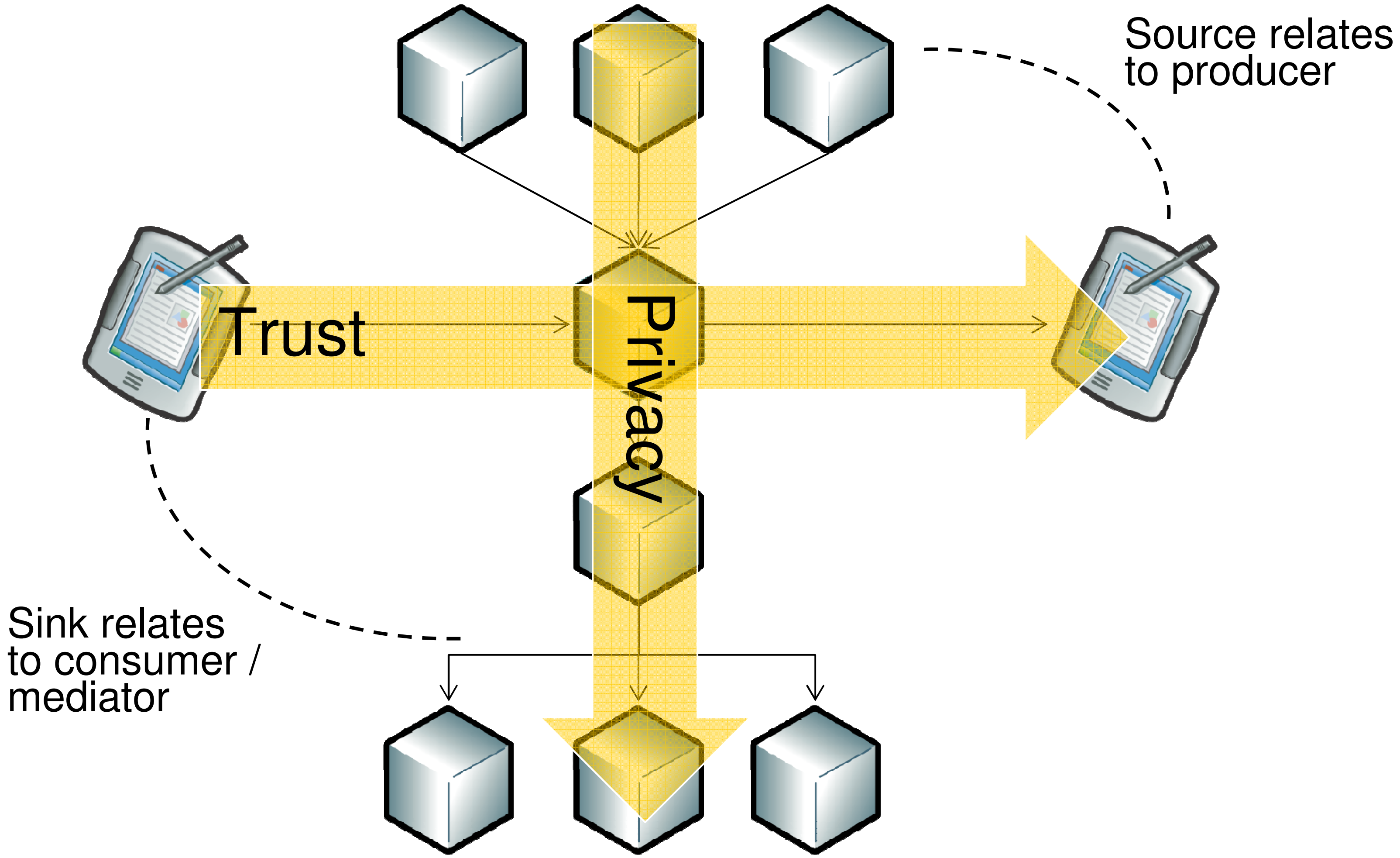
Data Sinks

Data Aggregation + Policy Composition

Policy Matching

Service Composition + Policy Composition

Generalization


Source relates to producer
Trust
Privacy
Sink relates to consumer / mediator

Questions to the Reference Group

- Do you see other interactions between privacy and SOA that we should look at?
- What specific technologies might be suitable for solving the privacy challenge in composed services?
- Do you see privacy issues that are not covered by our cross-domain workflow scenario, e.g. in user defined mashups?