Activity 6: Privacy in Infrastructures
Prof. Dr. Kai Rannenberg, Goethe University Frankfurt

ACTIVITY 6 AT A GLANCE
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
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

Smart Cards
- JavaCard
- U/i/SIM
- EMV Cards
- PKI Smart Cards

ISC / SCWS
- G&D Internet Smart Card

Source: Deliverable 6.2.1

<March 24, 2009>
The G&D Internet Smart Card & Smart Card Web Server

Source: Heartbeat 6.2.1
Potential Trust Anchors for Mobile Devices

![Diagram showing different types of security elements (SE) for mobile devices.](source: GD)

- **External Card**
- **“Software” SE**
- **SIM-based SE**
- **Removable SE**
- **Attached SE**
- **Embedded SE**
- **SE integrated in Processor**

Source: GD

March 24, 2009
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

Car Rental Service

Alice's Privacy Requirements

TB's Privacy Policy

CR's Privacy Policy

HB’s Privacy Policy

Execution does not violate “TB’s Privacy Policy”

Execution does not violate “CR’s Privacy Policy”

Execution does not violate “HB’s Privacy Policy”

0) Policies

2) PII

3) PII

4) PII

0) Policy

0) Policies

March 24, 2009
Motivation

User propagates her privacy preferences
=> maximum privacy / minimum QoS

Services aggregate privacy policies
=> Minimum privacy / maximum QoS

Execution does not violate “HB’s Privacy Policy”

Execution does not violate “CR’s Privacy Policy”
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

A5 : Policies
Policy Language Obligation Handling

WP 6.1 : IdM

WP6.3 : Service Composition
Privacy-aware SOA Development Tools

A1 : Privacy in Life

A2 : Mechanism
Re-accessing PII Measurability Crypto (Anon. Cred.)

WP6.2 : Trusted Infrastructure

A3 : Privacy Live

March 24, 2009
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
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
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

C₁ + P₁

C₂ + P₂

Job Portal

(4) Policy mismatch: request exception

(2) Backup Inga’s statements

(1) Puts her CV, with strict privacy policy

(5) Sends Inga’s CV

(3) Wants to recommend

Hannes: Headhunter, 35 years, DE

Inga: Journalist, 46 years, SE

Florence: Manager, 42 years, FR

March 24, 2009
Architecture

Data Sources

Data Sinks

Cv + Pcv
Architecture

Data Sources

Data Aggregation + Policy Composition

Policy Matching

Service Composition + Policy Composition

Data Sinks
Generalization

Source relates to producer

Sink relates to consumer / mediator

Trust

Privacy
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?