PrimeLife Summit
June 7, 2011

Activity 6 - Infrastructures

Kai Rannenberg, GUF
Ulrich Pinsdorf, EMIC
Marc-Michael Bergfeld, GD
Sascha Koschinat, GUF
Stuart Short, SAP

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

Outline

- PrimeLife “Infrastructure“ Activity at a Glance
- Service Composition (WP6.3)
- Secure Mobile Interaction (WP6.2)
- Economic Valuation (WP6.1)
ACTIVITY 6 AT A GLANCE

Activity 6 “Infrastructures”

- Mission
  - Improve infrastructures, devices and services with privacy-enhancing features
  - Focus on cross-domain service composition

- Research Focus
  - WP6.1 – Economic Aspects for Privacy in SOA
  - WP6.2 – Secure Mobile Usage of Services
  - WP6.3 – Service Composition

- Partners
  - GUF, SAP, EMIC, GD, ULD
Demonstrator Implementation

- Policy Composition
- PPL Engine
- Downstream Data Usage
- Mobile User Interaction
- Obligation Enforcement
- Privacy–aware service binding

Please visit Demo in Foyer

Focus on WP6.3 – Ulrich Pinsdorf (Microsoft EMIC)

ABSTRACT PRIVACY POLICY FRAMEWORK
Privacy in SOA

Why an Abstract Privacy Policy Framework?

- Generalization
  - Distill reoccurring patterns
  - Language independent
  - Technology-agnostic

- Guidelines
  - How to create and deploy privacy policies in SOA?
  - What building blocks are needed?

- Identify missing features
  - Looking at shortcomings of existing languages
  - Define future work
Instantiations

- **Validation**
  - APPEL + P3P (+EPAL)
  - PrimeLife Policy Language (PPL)
  - SecPAL for Privacy
  - Remote management of XACML
  - PRIME Data Handling Policy + Framework

- **Key Findings**
  - Access control on PII is not sufficient without obligations
  - Preference and sticky policies needed for complex downstream cases
  - Language should allow for logic reasoning
More Details

- 12 pages summary at iNetSec 2011, see you there

- Dedicated Talk
  IFIP WG 11.4 iNetSec
  Thursday, 15:55
  Forum 2.14

- Full details in public
  Deliverable D6.3.2

Focus on WP6.2 – Marc-Michael Bergfeld (G&D)

PRIVATE MOBILE SERVICES / MOBILE USAGE OF SERVICES
You are here!

Infrastructure (A6)

- Economic Valuation
  WP6.1
- Service Composition
  WP6.3
- Mobile Interaction
  WP6.2

Present & Future Market & Technology Environment
What are we talking about....

- Secure Elements in Mobile Devices are the identity modules of the future.
- Dominating (partial) identities and the data assigned to these is an important link between Mobile and Web-based services.
Why complex….

The Mobile Services Value Chain

Mobile Services Value Chain

- **Chip provider**
  - Produce CPU

- **Handset provider**
  - Handset w/ SE of different kinds

- **MNO / Have clients.**

- **Service providers**
  - Have new services.
  - Banks / Credit schemes
  - Want direct client access
  - Other services
  - Want additional channels to sell transportation, ticketing etc. service

- **End-Consumer**
  - Use handsets to execute trusted services

- **Potential SEs & Dominant Links**
  - eSE
  - SIM
  - SD Sticker

- **Trusted Service Manager (Trusted Third Party)**
  - Have access and secure provisioning & client service

- **Dominant links (DL)**
The Mobile Services Value Chain

Mobile Services Value Chain

Chip provider
Produce CPU

Handset provider
Handset w/ SE of different kinds

Want
Profit.
Need
Security.

MNO / Have clients.

Service
providers have core services.
Banks / Credit schemes Want direct client access.
Other services Want additional channels to sell transportation, ticketing etc. services

End-Consumer
Use handsets to execute trusted services.

Want
Convenience.
Need
Performance.

TEE
eSE
SIM
SD Sticker
PrimeLife focus

Trusted Service Manager (Trusted Third Party)
Have access and secure provisioning & client service

PrimeLife focus

The Mobile Services Value Chain

Technologies and Privacy in Mobile-Web-interactions
Privacy, Identity & the Secure Elements

<table>
<thead>
<tr>
<th>Trust: A Trusted Secure Element / Environment</th>
<th>TEE</th>
<th>µSD</th>
<th>Sticker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identity: A specific communication channel for the partial identity</th>
<th>TEE</th>
<th>µSD</th>
<th>Sticker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Partially</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Privacy: Secure communication, only for the individual</th>
<th>TEE</th>
<th>µSD</th>
<th>Sticker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Partially</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Anonymity: Unlinkability of the interaction to the individual</th>
<th>TEE</th>
<th>µSD</th>
<th>Sticker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible</td>
<td>Possible</td>
<td>Partially</td>
<td>No</td>
</tr>
</tbody>
</table>
PrimeLife Demo
Mobile Privacy

The „Flow“ of „Mobile PrimeLife“

Receive Identity- and Privacy-enhanced request.

Open „Private World“ on SE via Privacy-PIN

„Private World“-keys decrypt data: Secure, private, identity-related.

Manage policies in the „Private World“-encrypt before sending to Back-end

Overview of „Private Activities“
Outlook and Discussion

Privacy in a "Cloud-connected World"

- Other Mobile Payment Terminals as Mobile Devices
- Car Navigation and Entertainment as Mobile Device
- Mobile Phone (Smart Phone) as Mobile Device
- Netbooks, Laptops and Tablet PCs as Mobile Devices

The Cloud as Backend
Key results

- Direct user interaction between mobile and back-end in “Private World”.
  - Shown in real-life demonstrator (see D 6.3.2)

- Lessons learned in Demonstrator -> Global Platform standardization
  - APIs published (D. 6.3.1)

- Future research: Certification & Isolation of “Private World” (see SEPIA).

Focus on WP6.1 – Sascha Koschinat (Goethe University Frankfurt)

**ECONOMIC VALUATION OF PRIVACY-ENHANCING IDENTITY MANAGEMENT SERVICES**
Challenge to be addressed

- Developers and providers of innovative privacy-enhancing identity management services need appropriate methods in order to:
  - valuate the potentials and risks of alternative service designs
  - select the most promising service designs for investments and market introductions
- Due to different shortcomings current valuation approaches are not appropriate for valuations in this domain, e.g.:
  - Six Forces Model: considers only external factors to the decision maker - competition, new entrants, end users, suppliers, substitutes, government
  - SWOT analysis: considers only highly abstract factors to the decision maker - strength, weaknesses, opportunities, threats
- ...  

➤ Develop an economic valuation approach appropriate for privacy-enhancing identity management services!

Economic Valuation Approach for Privacy-Enhancing Identity Management Services

Process Model:
6 process steps (instructions) that guide the decision maker through the decision process

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Scenario Descriptions</td>
</tr>
<tr>
<td>2</td>
<td>Identification of Costs and Benefits</td>
</tr>
<tr>
<td>3</td>
<td>Selection of Key Costs and Benefits</td>
</tr>
<tr>
<td>4</td>
<td>Clustering and Mapping</td>
</tr>
<tr>
<td>5</td>
<td>Assessment and Aggregation</td>
</tr>
<tr>
<td>6</td>
<td>Visualisation</td>
</tr>
</tbody>
</table>

Structure Model:
Building blocks (elements) that support the decision maker to represent the decision situation

- Sequence Diagrams
- Economic Value Diagrams
- Decision Diagrams
### Real-life Identity Management Service Scenarios

<table>
<thead>
<tr>
<th>Baseline Option</th>
<th>Delta Option 1</th>
<th>Delta Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attribute Verification Service Scenario</strong></td>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
</tr>
<tr>
<td><strong>Authentication Service Scenario</strong></td>
<td><img src="image4.png" alt="Image" /></td>
<td><img src="image5.png" alt="Image" /></td>
</tr>
<tr>
<td><strong>Privacy Policy Enforcement Service Scenario</strong></td>
<td><img src="image7.png" alt="Image" /></td>
<td><img src="image8.png" alt="Image" /></td>
</tr>
</tbody>
</table>

---

### Brief Application Example – Privacy Policy Enforcement
Baseline Option vs. Delta Option 1

<table>
<thead>
<tr>
<th>Baseline Option</th>
<th>Delta Option 1</th>
<th>Delta Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attribute Verification Service Scenario</strong></td>
<td><img src="image10.png" alt="Image" /></td>
<td><img src="image11.png" alt="Image" /></td>
</tr>
<tr>
<td><strong>Authentication Service Scenario</strong></td>
<td><img src="image13.png" alt="Image" /></td>
<td><img src="image14.png" alt="Image" /></td>
</tr>
<tr>
<td><strong>Privacy Policy Enforcement Service Scenario</strong></td>
<td><img src="image16.png" alt="Image" /></td>
<td><img src="image17.png" alt="Image" /></td>
</tr>
</tbody>
</table>

---

PrimeLife Summit  
June 7, 2011
Conclusion & Outlook

- **Conclusion:**
  - Presents decision-relevant information in a simple, structured, and transparent way without over-challenging the decision maker
  - Enables a stronger focus on (and integration of) privacy-effects on consumers as an essential factor for economic success
  - Considers individual value perceptions of stakeholders and interdependencies to enable application field-specific valuations of IdM services
  - Structures complex decision processes and simplifies a separation into transparent sub-aspects
  - ...

- **Outlook:**
  - More intensive testing of the method on real world use-cases
  - Enhancement and improvement of each step by more sophisticated methods and concepts
  - More intensive focus on privacy-related effects
  - Reducing possible errors caused by subjectivity of the decision maker
  - ...
Thank you for your attention

Activity 6: Key Results

- WP6.1 – Economic Aspects for Privacy in SOA
  - Privacy as an essential factor for economic success
  - Simple, structured, and transparent valuation method for privacy-enhancing IdM services

- WP6.2 – Mobile Device in SOA
  - Trustworthy mobile interaction enables end user’s control in infrastructure
  - Isolation designed into future TEEs (standardized)

- WP6.3 – Privacy-Enhanced Infrastructures
  - Requirements for Privacy in SOA
  - Abstract Privacy Framework
  - Test implementation and evaluation of PPL Engine