

Activity 6 - Infrastructures

Kai Rannenber, 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

3

PrimeLife Summit

June 7, 2011



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

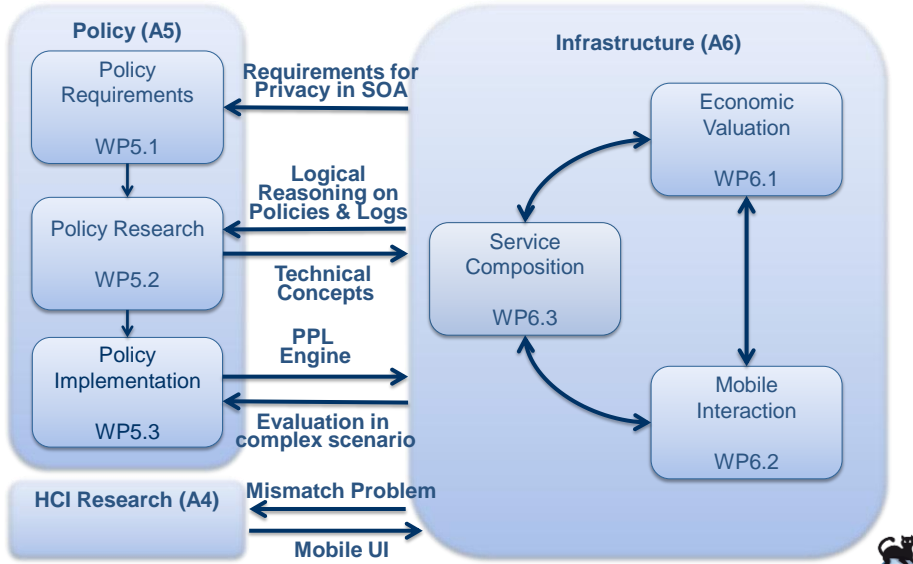
4

PrimeLife Summit

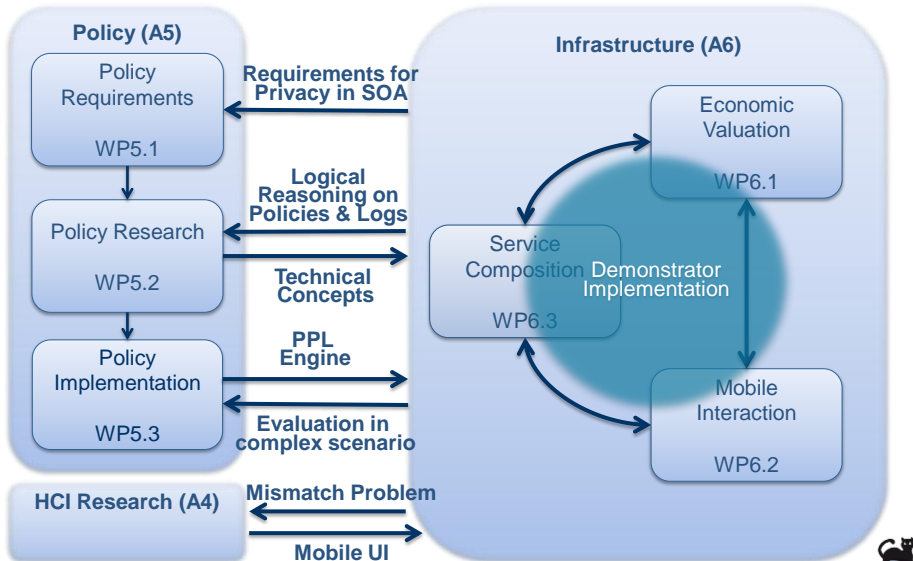
June 7, 2011



Collaboration

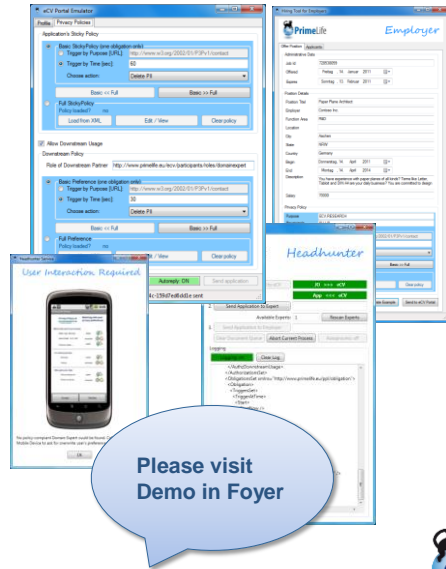


Collaboration



Demonstrator Implementation

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



7

PrimeLife Summit

June 7, 2011

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

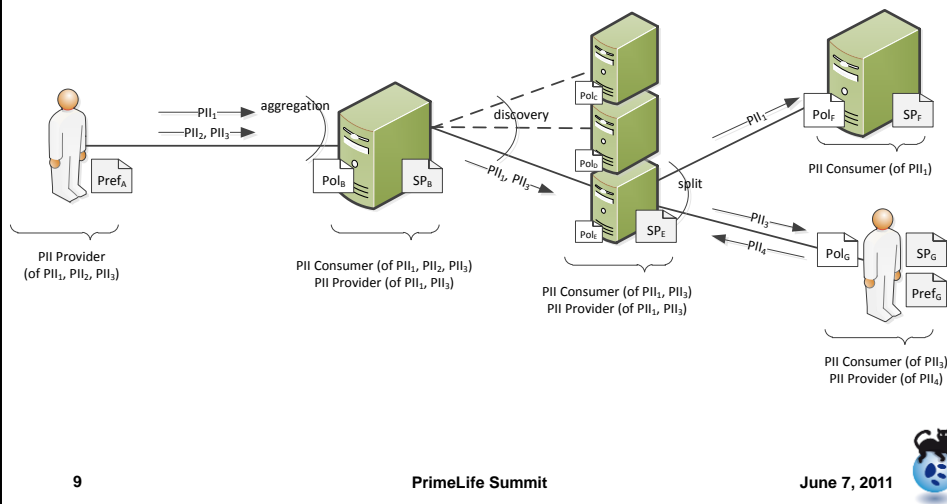
ABSTRACT PRIVACY POLICY FRAMEWORK

8

PrimeLife Summit

June 7, 2011

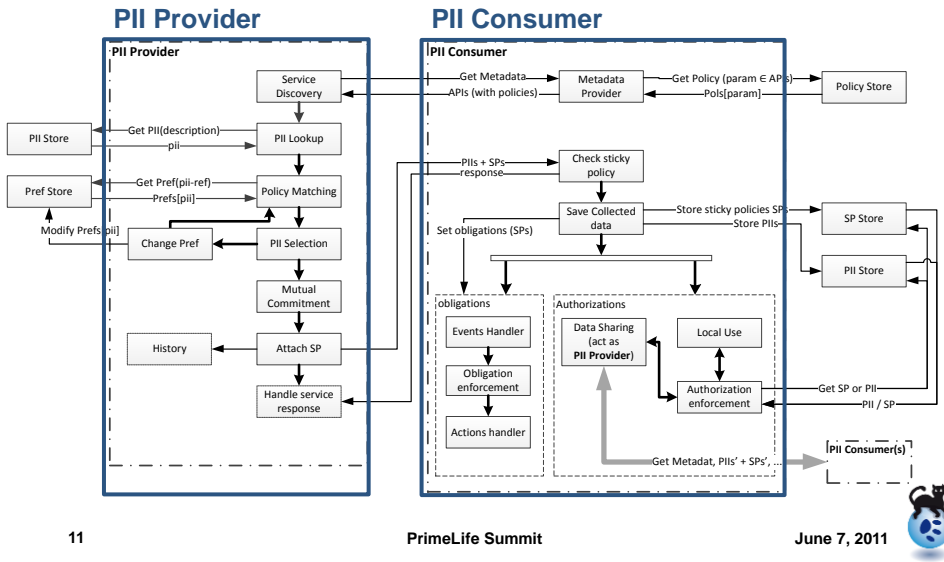
Privacy in SOA



Why an Abstract Privacy Policy Framework?

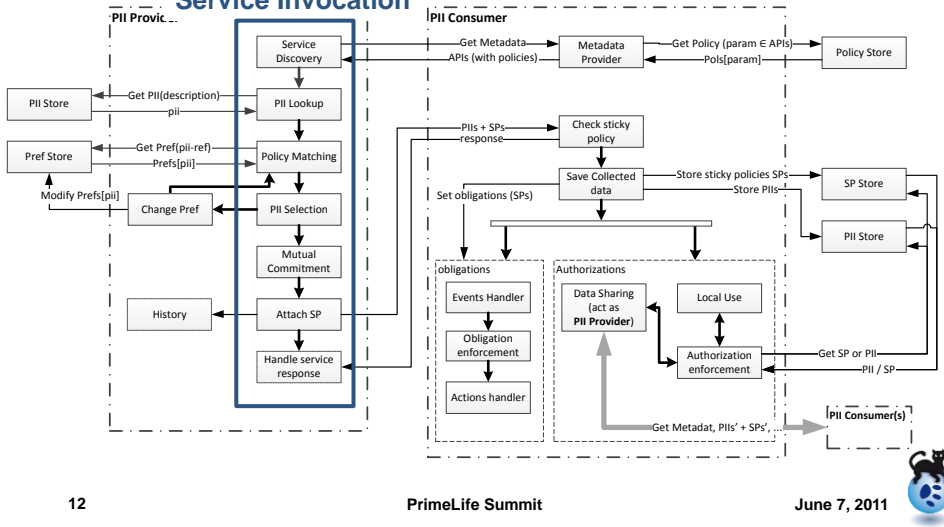
- Generalization
 - Distill reoccurring patterns
 - Language independent
 - Technology-agnostic
- Guidelines
 - How to create and deploy privacy policies in SOA?
 - What building blocks are needed?
- Identify missing features
 - Looking at shortcomings of existing languages
 - Define future work

Abstract Privacy Policy Framework

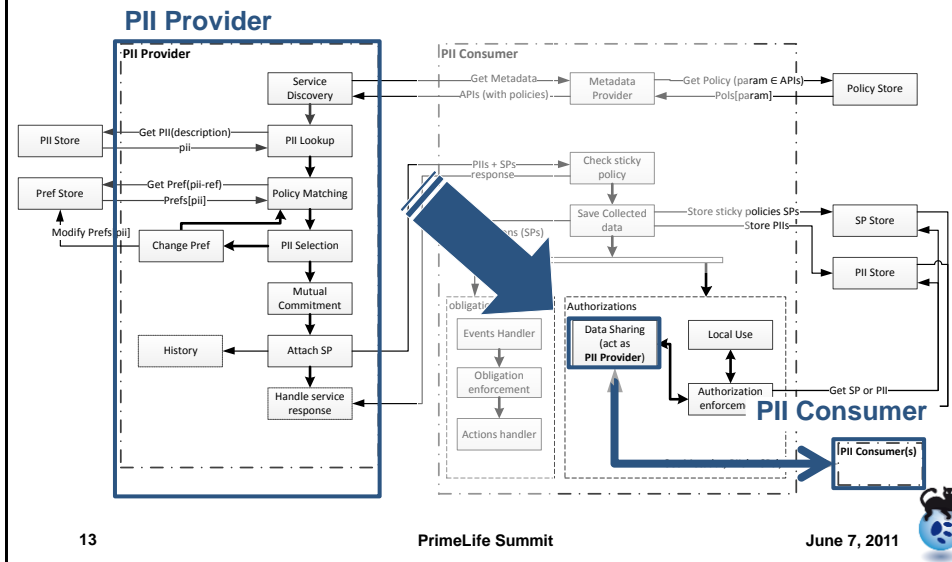


Abstract Privacy Policy Framework

Protocol for Service Invocation



Abstract Privacy Policy Framework



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

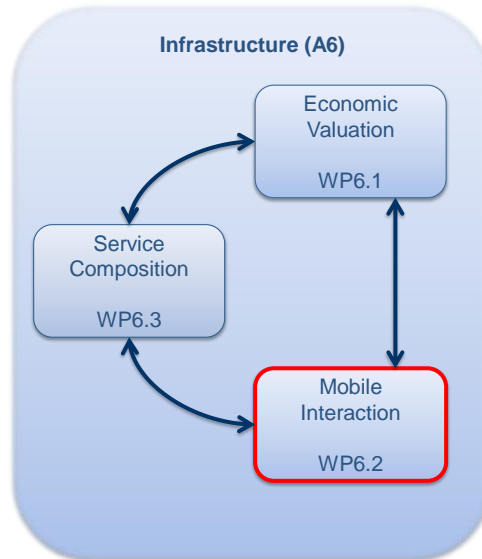


Focus on WP6.2 – Marc-Michael Bergfeld (G&D)

PRIVATE MOBILE SERVICES / MOBILE USAGE OF SERVICES



You are here!

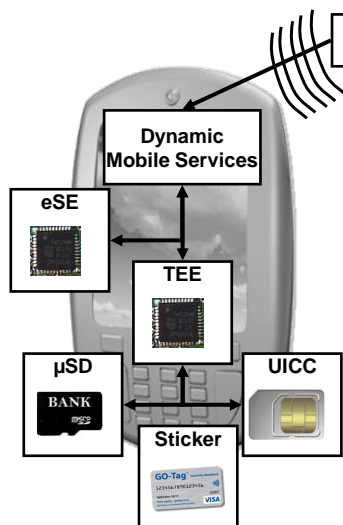


Present & Future Market & Technology Environment

■ What are we talking about....



Mobile Services and Secure Elements



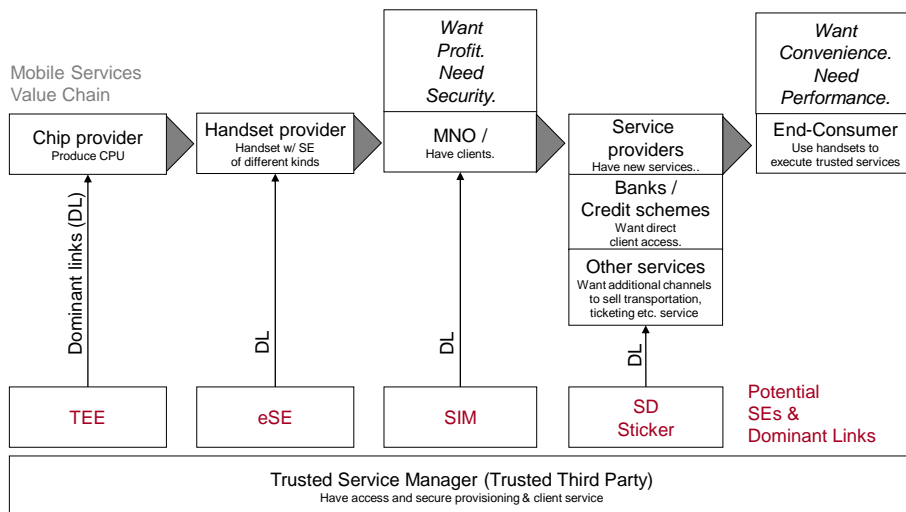
- Secure Elements in Mobile Devices are the identity modules of the future.
- Dominating (partial) identities and the data assigned to these is an important link between Mobile and Web-based services.



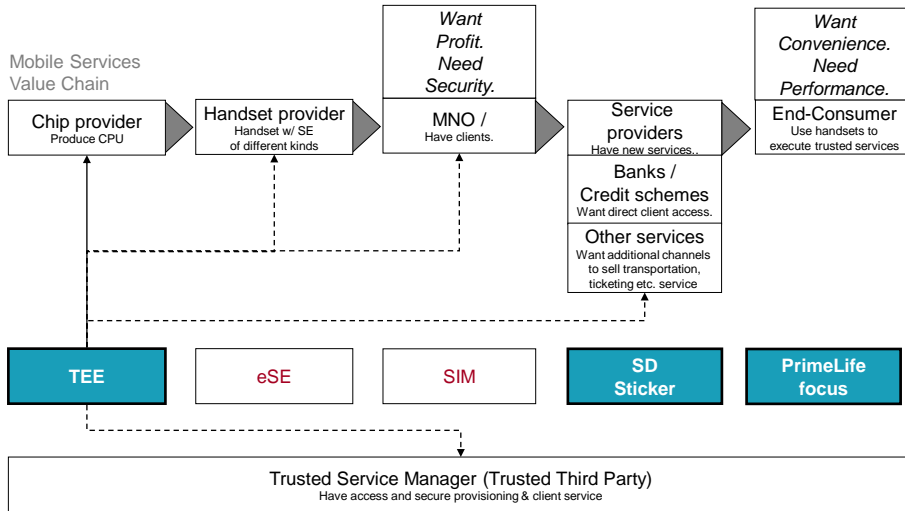
■ Why complex....



The Mobile Services Value Chain






The Mobile Services Value Chain



Technologies and Privacy in Mobile-Web-interactions




Privacy, Identity & the Secure Elements

	 TEE	 µSD	 Sticker
Highly dynamic	Yes	Partially	No
Trust: A Trusted Secure Element / Environment	Yes	Yes	Yes
Identity: A specific communication channel for the partial identity	Yes	Yes	No
Privacy: Secure communication, only for the individual	Yes	Yes	Partially
Anonymity: Unlinkability of the interaction to the individual	Possible	Possible	No

Remember: Mobile Services Value Chain!



Privacy, Identity & the Secure Elements

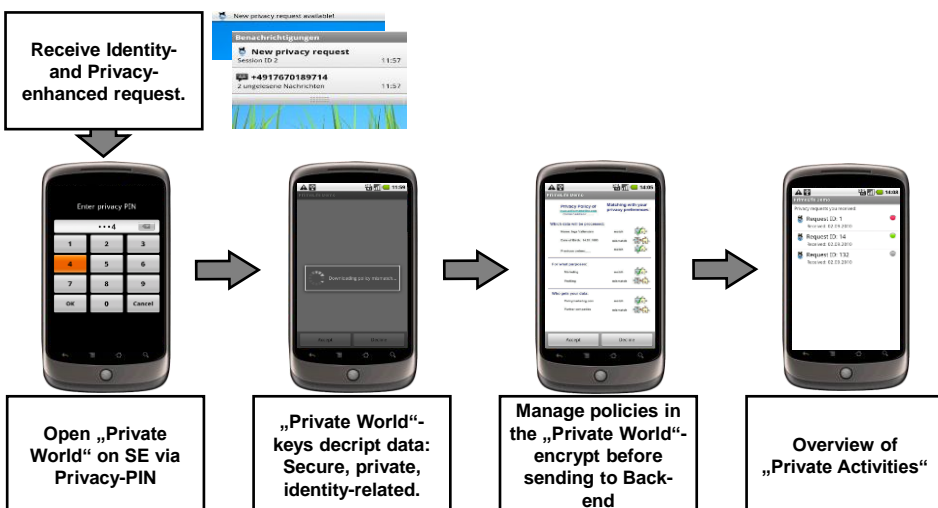
	 TEE	 µSD	 Sticker
Highly dynamic	PrimeLife Standard (Global Platform) Future research (e.g. SEPIA)	PrimeLife Demo (Secure SD Card) Lessons learned for TEE concepts	
Trust: A Trusted Secure Element / Environment			
Identity: A specific communication channel for the partial identity			
Privacy: Secure communication, only for the individual			
Anonymity: Unlinkability of the interaction to the individual			



PrimeLife Demo

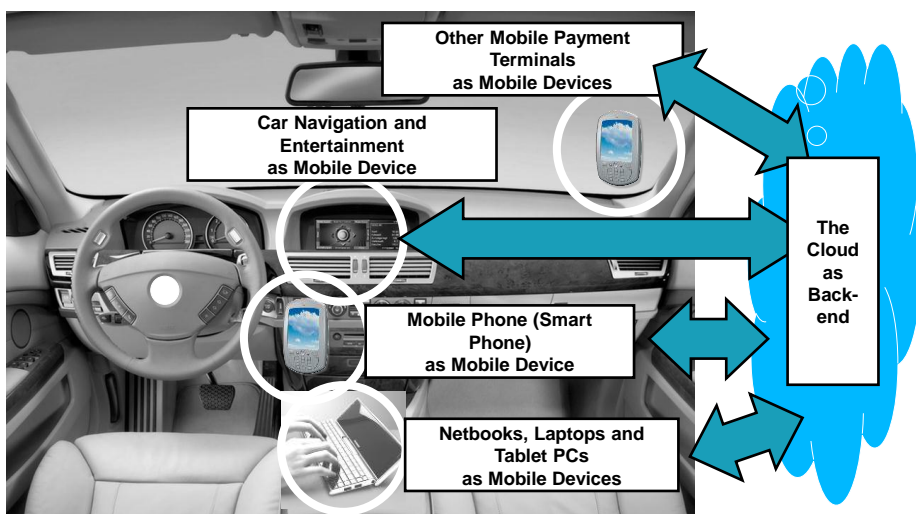
Mobile Privacy

The „Flow“ of „Mobile PrimeLife“



Outlook and Discussion

Privacy in a „Cloud-connected World“



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:
 - evaluate 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!**

33

PrimeLife Summit

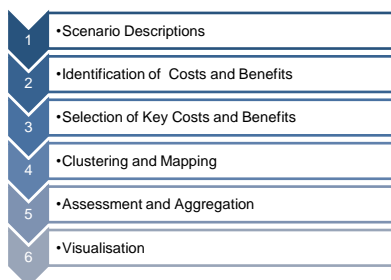
June 7, 2011



Economic Valuation Approach for Privacy-Enhancing Identity Management Services

Process Model:

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



Sequence Diagrams

Economic Value Diagrams

Decision Diagrams

Structure Model:

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



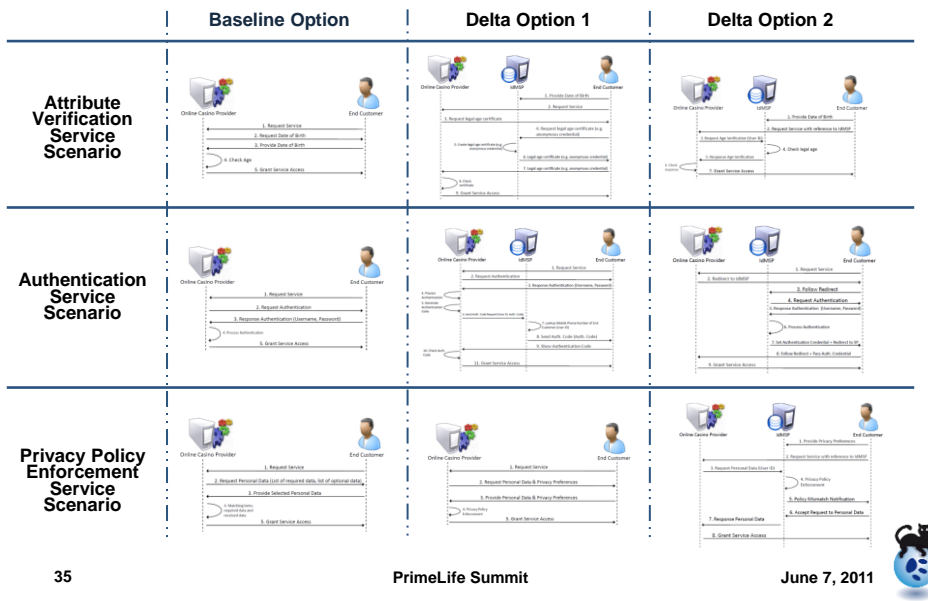
34

PrimeLife Summit

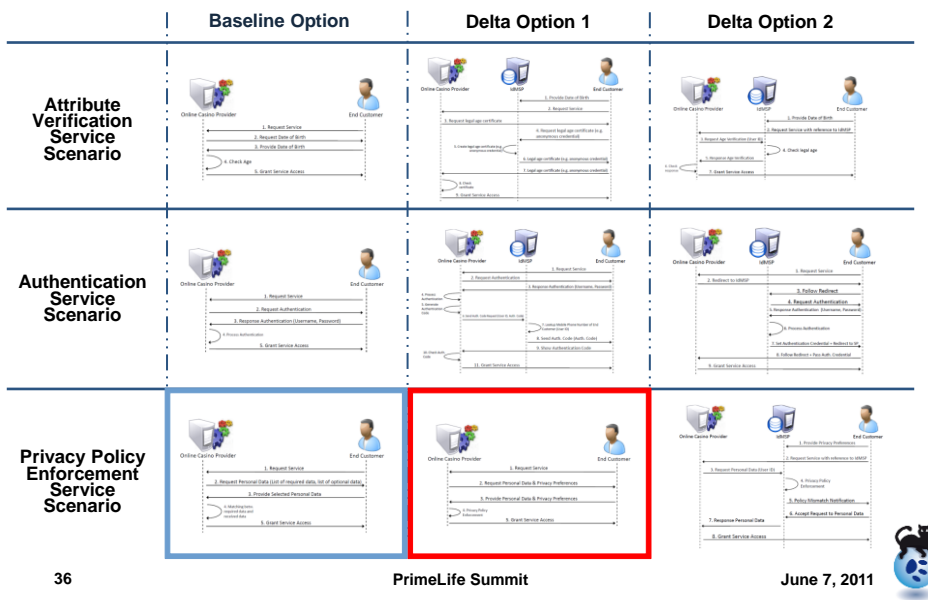
June 7, 2011



Real-life Identity Management Service Scenarios

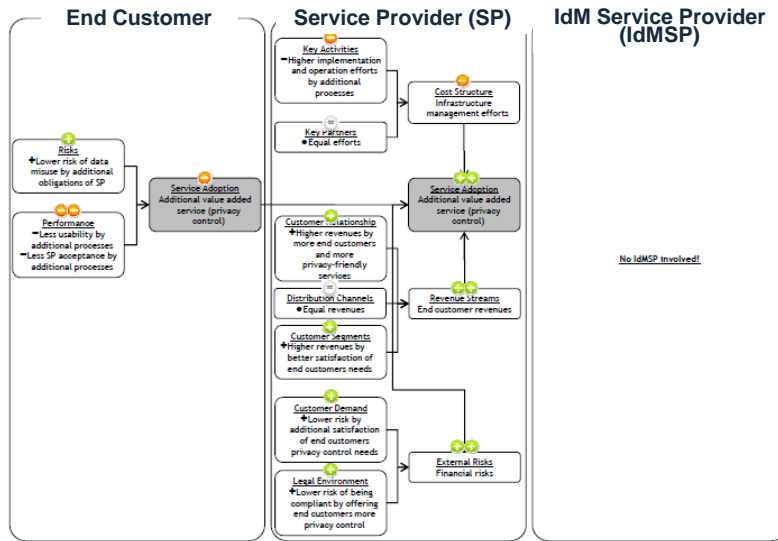


Brief Application Example – Privacy Policy Enforcement Baseline Option vs. Delta Option 1



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

Policy Enforcement Service Scenario - Delta Option 1 vs. Baseline Option - Assessment and Aggregation of Key Costs and Benefits



37

PrimeLife Summit

June 7, 2011



Brief Application Example – Privacy Policy Enforcement Baseline Option vs. Delta Option 2



38

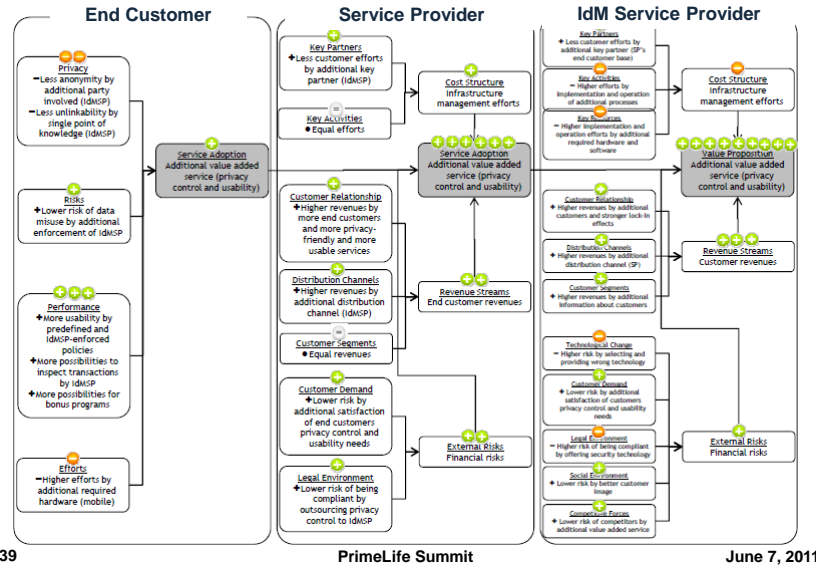
PrimeLife Summit

June 7, 2011

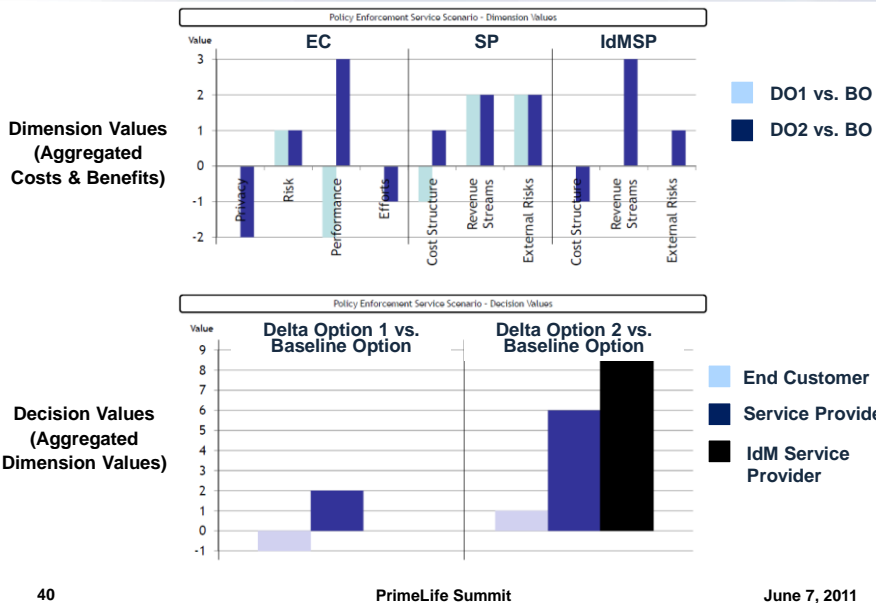


Brief Application Example – Privacy Policy Enforcement Baseline Option vs. Delta Option 2

Policy Enforcement Service Scenario - Delta Option 2 vs. Baseline Option - Assessment and Aggregation of Key Costs and Benefits



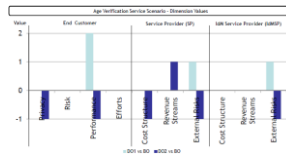
Brief Application Example – Privacy Policy Enforcement Delta Option 1 vs. Delta Option 2



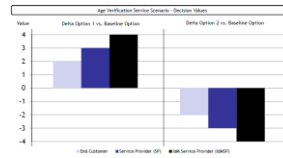
Results of Scenario Valuations – Summary

Attribute Verification Service Scenario

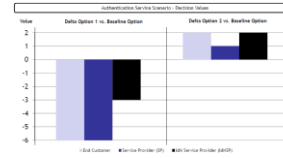
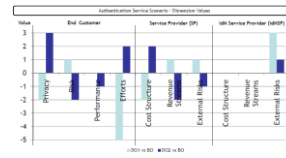
Dimension Values



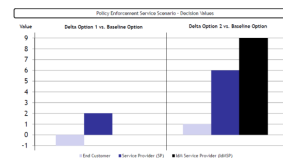
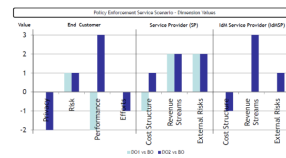
Decision Values



Authentication Service Scenario



Privacy Policy Enforcement Service Scenario



41

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
 - ...

42

PrimeLife Summit

June 7, 2011



KATHOLIEKE UNIVERSITEIT
LEUVEN

GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

cureGD

UNIVERSITY OF GENT

UNIVERSITY OF GENT

UNIVERSITY OF GENT

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

