European R&D for privacy and identity solutions for the Information Society

High Level Conference „eID and Public Registers”

Hradec Králové, 2009-04-06/07

Prof. Dr. Kai Rannenberg
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt, Germany
www.m-chair.net

Agenda

- Views on Identity Management
- Partial Identities
- Strong Sovereign Identifiers
  - Able to protect themselves
  - Standing with their holders
- Building trust with minimum disclosure
- Conclusions and Outlook

Who identifies whom ?

- Who has to be identified by whom for which purposes?
  - Citizen by (border) control ?
  - (Border) control by citizen‘s (or citizen‘s devices)
  - Entities in the Internet

- Who relies on whom in
  - Identification Processes
  - Identity Management

Identity Management (IdM)
2 sides of a medal

- **Organisations** aim to sort out
  - User Accounts in different IT systems
  - Authentication
  - Rights management
  - Access control
- **Unified identities** help to
  - ease administration
  - manage customer relations
- **Identity management systems**
  - ease single-sign-on by unify accounts
  - solve the problems of multiple passwords

- **People** live their life
  - in different roles (professional, private, volunteer)
  - using different identities (pseudonyms): email accounts, SIM cards, eBay trade names, chat names, 2ndLife names, …)
- **Differentiated identities** help to
  - protect
    - privacy, especially anonymity
    - personal security/safety
  - enable reputation building at the same time
- **Identity management systems**
  - support users using role based identities
  - help to present the “right” identity in the right context

Identity Management (IdM)
2 sides of a medal

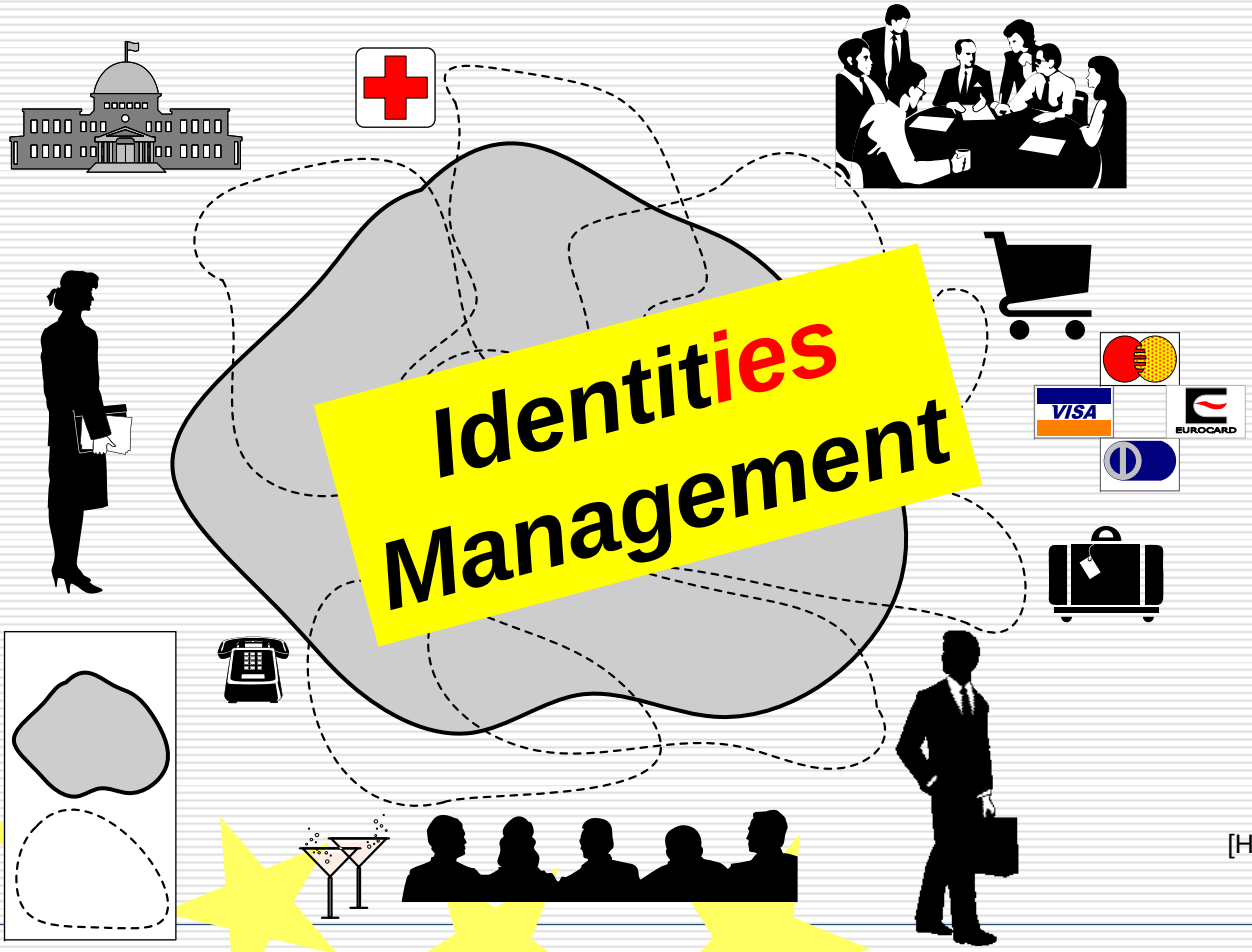
- **People** live their life
  - in different roles (professional, private, volunteer)
  - using different identities (pseudonyms): email accounts, SIM cards, eBay trade names, chat names, 2ndLife names, …)
- **Differentiated identities** help to
  - protect
    - privacy, especially anonymity
    - personal security/safety
  - enable reputation building at the same time
- **Identity management systems**
  - support users using role based identities
  - help to present the “right” identity in the right context

- **Organisations** aim to sort out
  - User Accounts in different IT systems
  - Authentication
  - Rights management
  - Access control
- **Unified identities** help to
  - ease administration
  - manage customer relations
- **Identity management systems**
  - ease single-sign-on by unify accounts
  - solve the problems of multiple passwords

Agenda

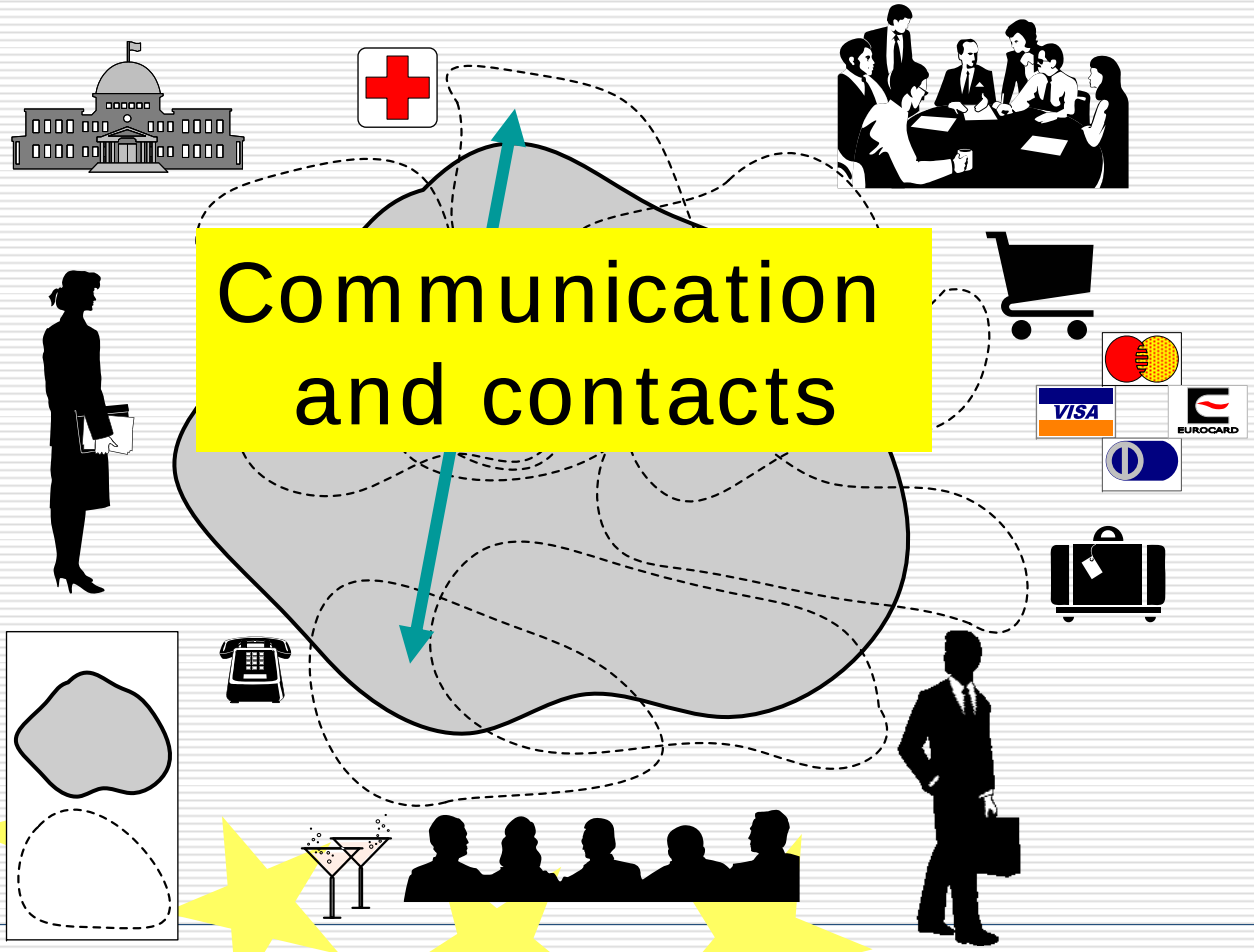
- Views on Identity Management
- Partial Identities
- Strong Sovereign Identifiers
  - Able to protect themselves
  - Standing with their holders
- Building trust with minimum disclosure
- Conclusions and Outlook

Partial Identities



[Hansen2005]

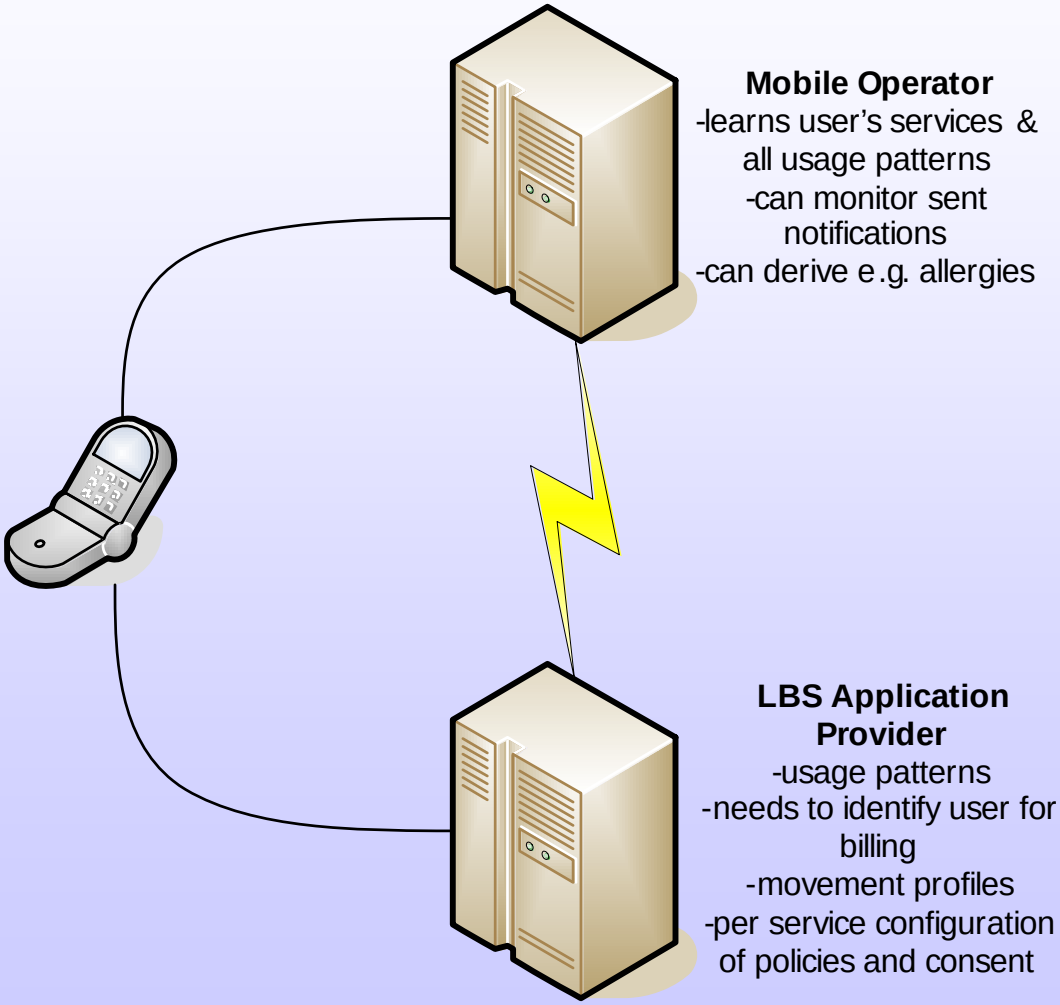
Changing borders of (partial) identities (cont.)



Enabling Partial Identities
PRIME LBS Application Prototype

- Enhance privacy for typical LBS
  - Pharmacy search (“pull”)
  - Pollen warning (“push”)
- Address wide user range by making only few requirements on the existing infrastructure
  - Version 1 simple WAP mobile phone
  - Version 2 Java phone
- Considering B2B scenarios in the value chain

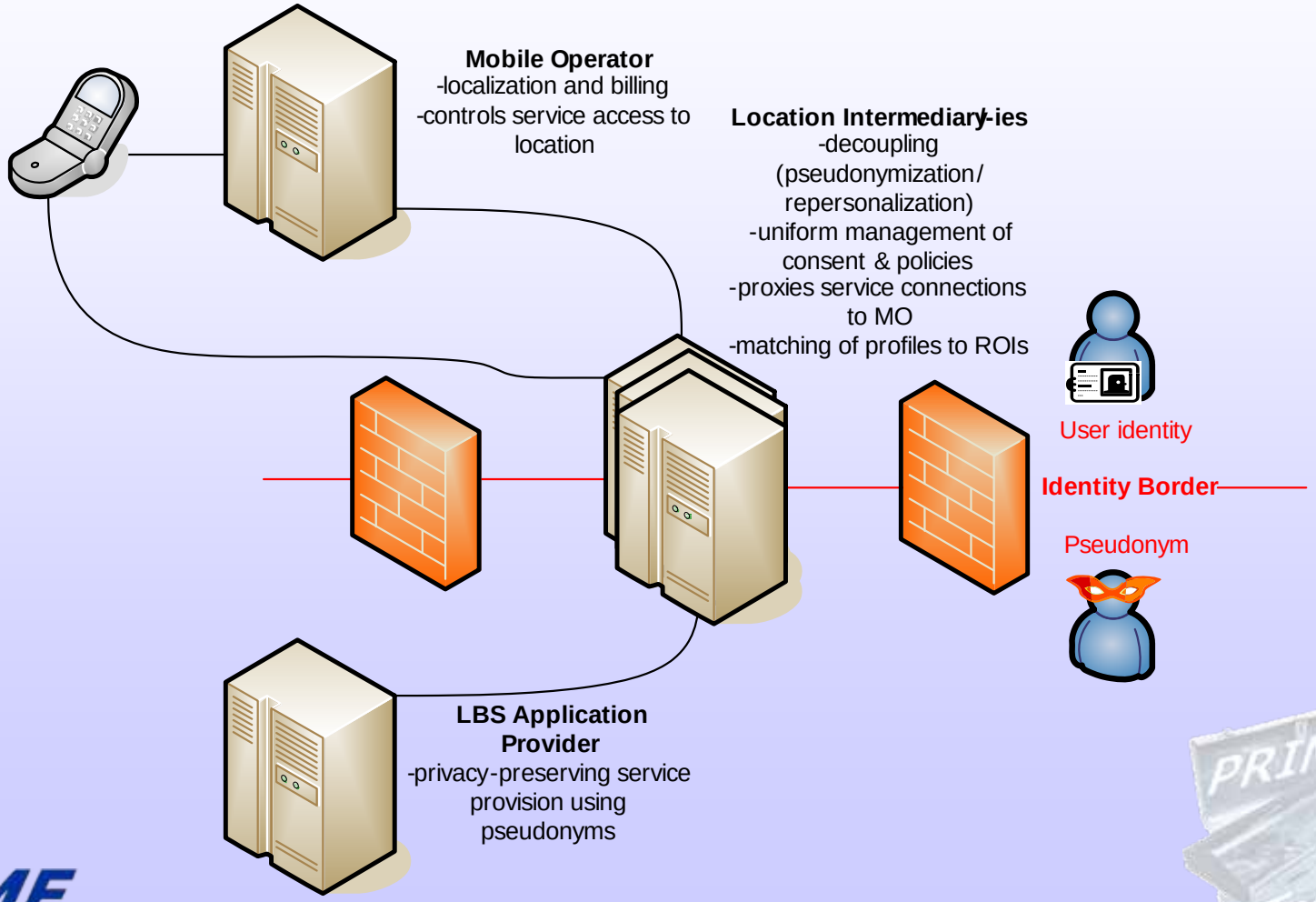
Conventional LBS Deployment



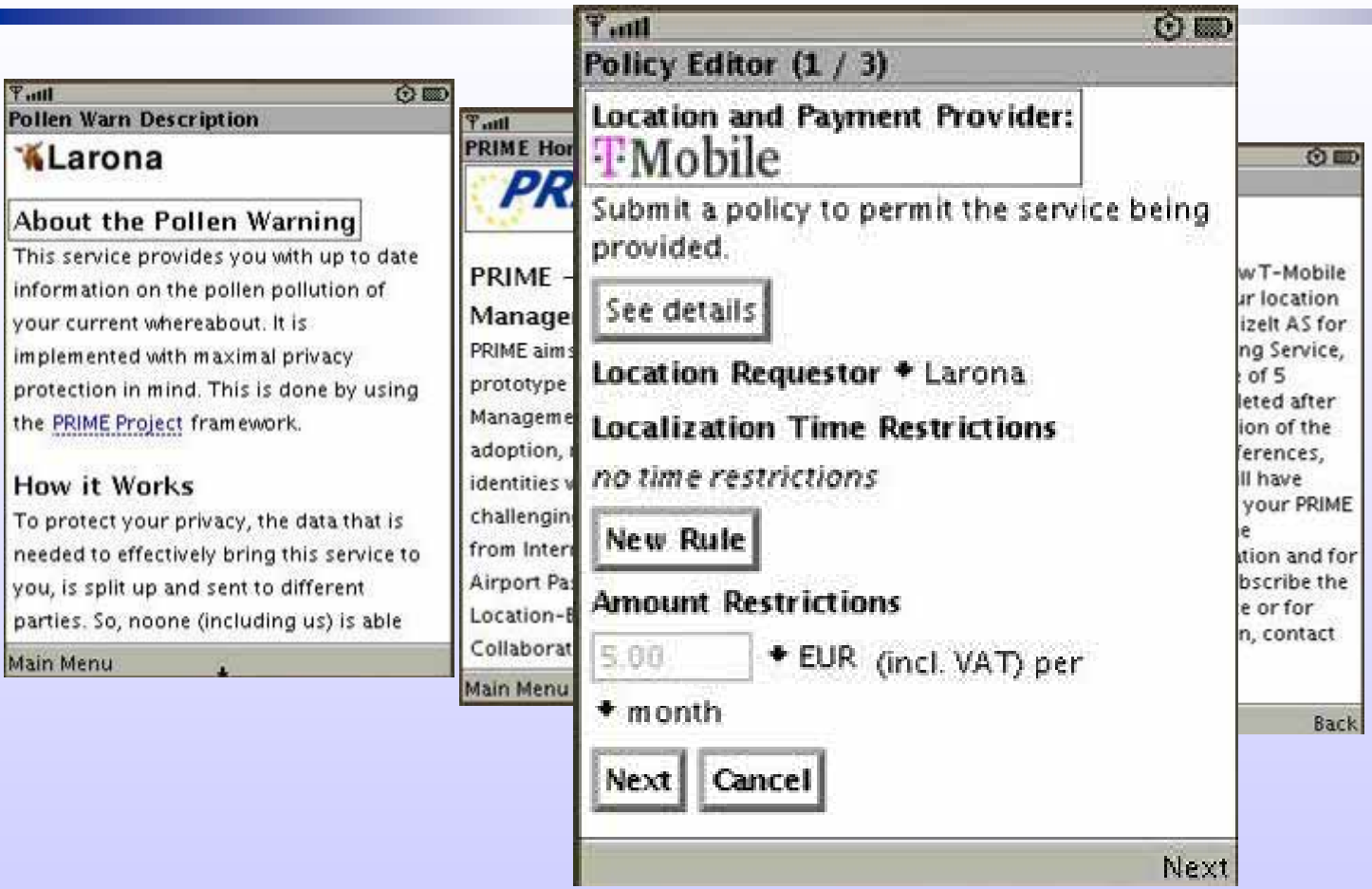
Mobile Operator
-learns user's services & all usage patterns
-can monitor sent notifications
-can derive e.g. allergies

LBS Application Provider
-usage patterns
-needs to identify user for billing
-movement profiles
-per service configuration of policies and consent

PRIME LBS Application Prototype
Intermediary Approach



PRIME LBS Application Prototype
Prototype Screens “Pollen Warning”

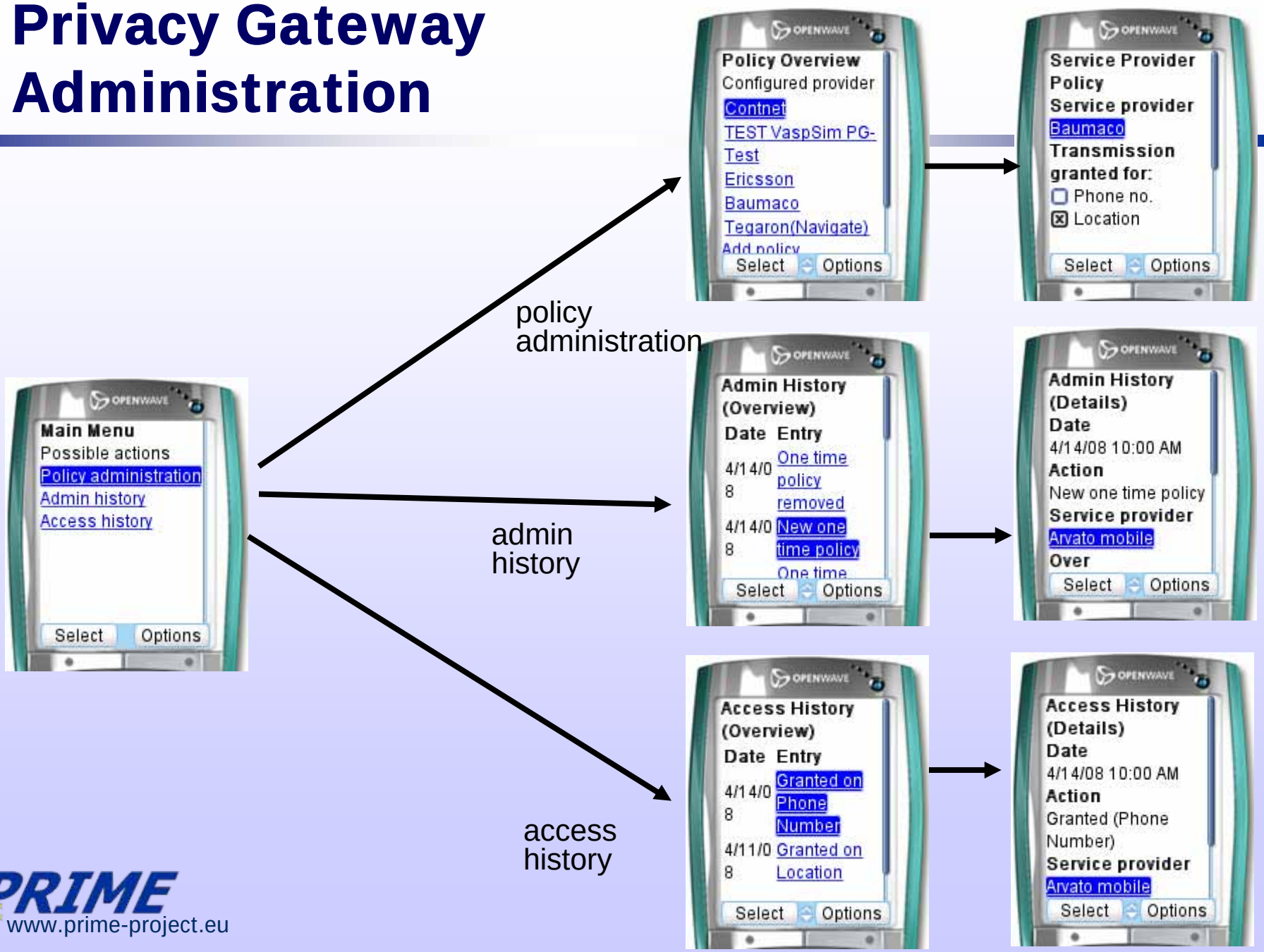


Product Transfer
Customer GUI

T-Zones / web'n'walk

Privacy Gateway Settings

Privacy Gateway Administration



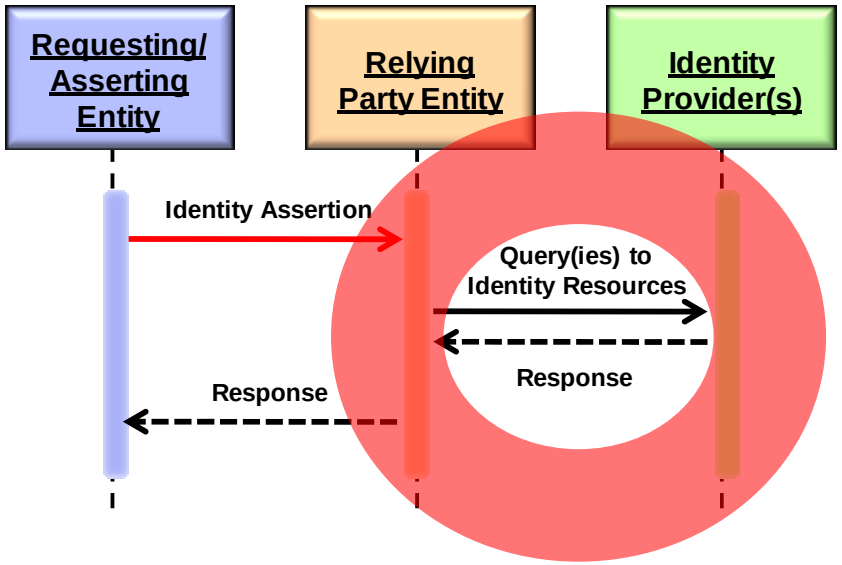
Agenda

- Views on Identity Management
- Partial Identities
- Strong Sovereign Identifiers
  - Able to protect themselves
  - Standing with their holders
- Building trust with minimum disclosure
- Conclusions and Outlook

Principles for the design of Secure Identifiers

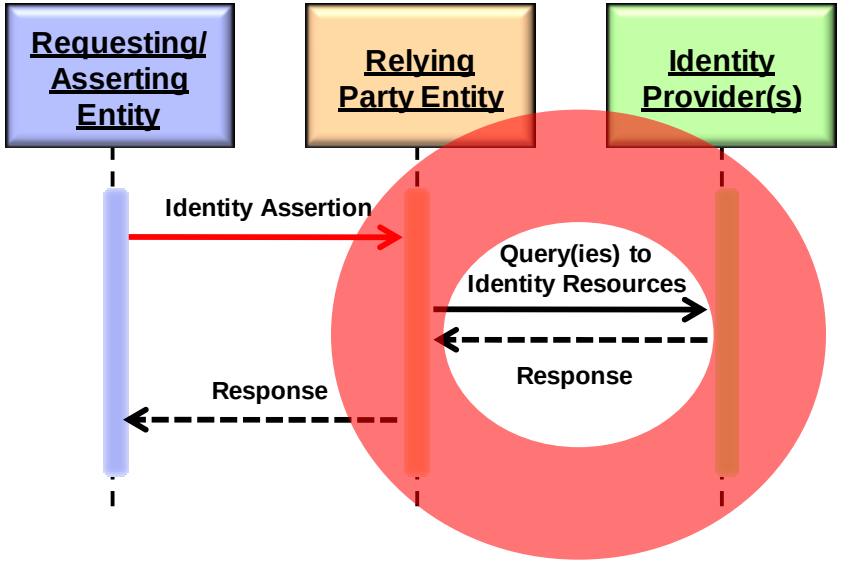
- Enabling the identity holder to influence
  - character and degree of identification and
  - amount of identification information
- Enabling the identifier to protect itself:
  - Ability to verify the controller by e.g. extra channel
  - A portfolio of communication mechanisms for redundancy
  - Sufficient access control towards relevant data (TPM?)
  - Enough processing power for complex operations
- Enabling communication
  - between identity holder and identifier

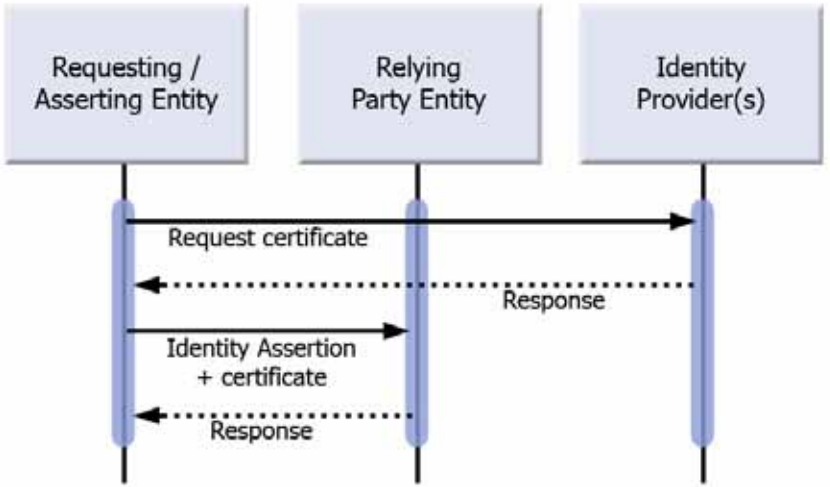
“To call or not to call (home)”



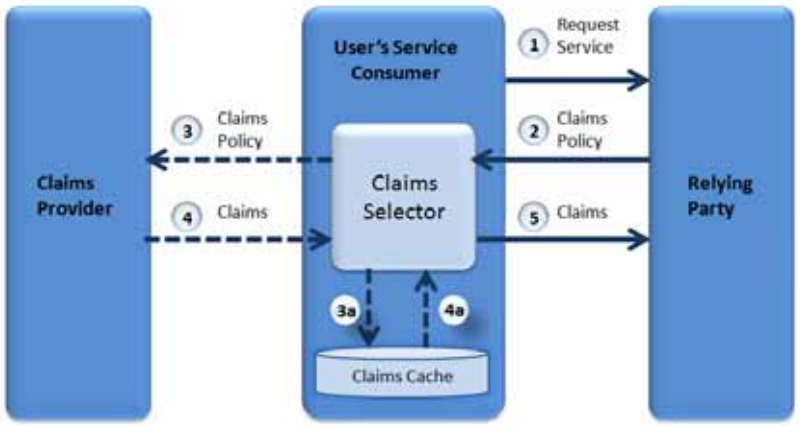
- Must an “Identity Provider” be involved in every interaction of user and relying party?

Overcoming the "Calling home"





- Is the "Identity Provider" involved in every interaction of user and relying party?



mobile business

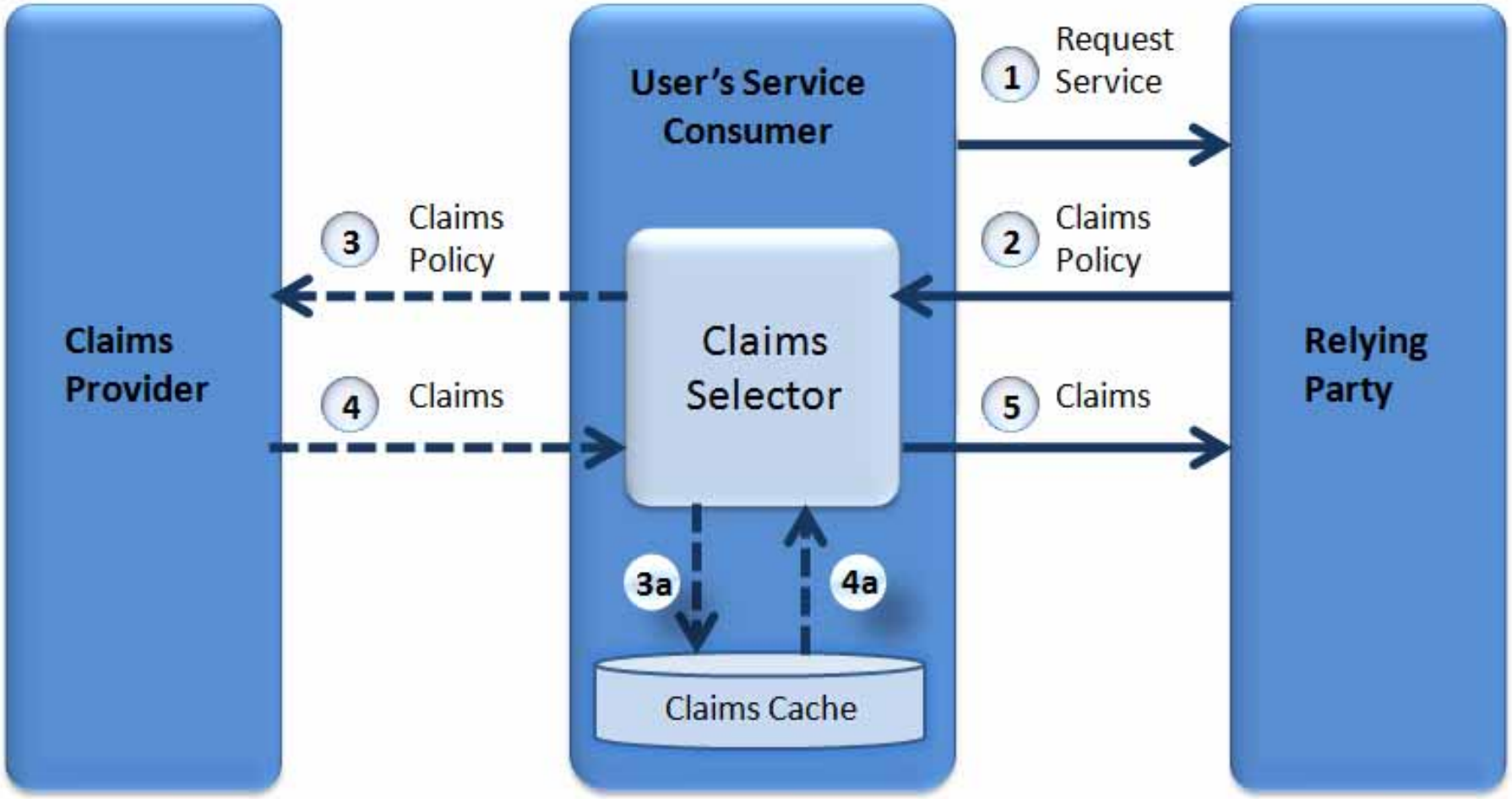
Agenda

- Views on Identity Management
- Partial Identities
- Strong Sovereign Identifiers
  - Able to protect themselves
  - Standing with their holders
- Building trust with minimum disclosure
- Conclusions and Outlook

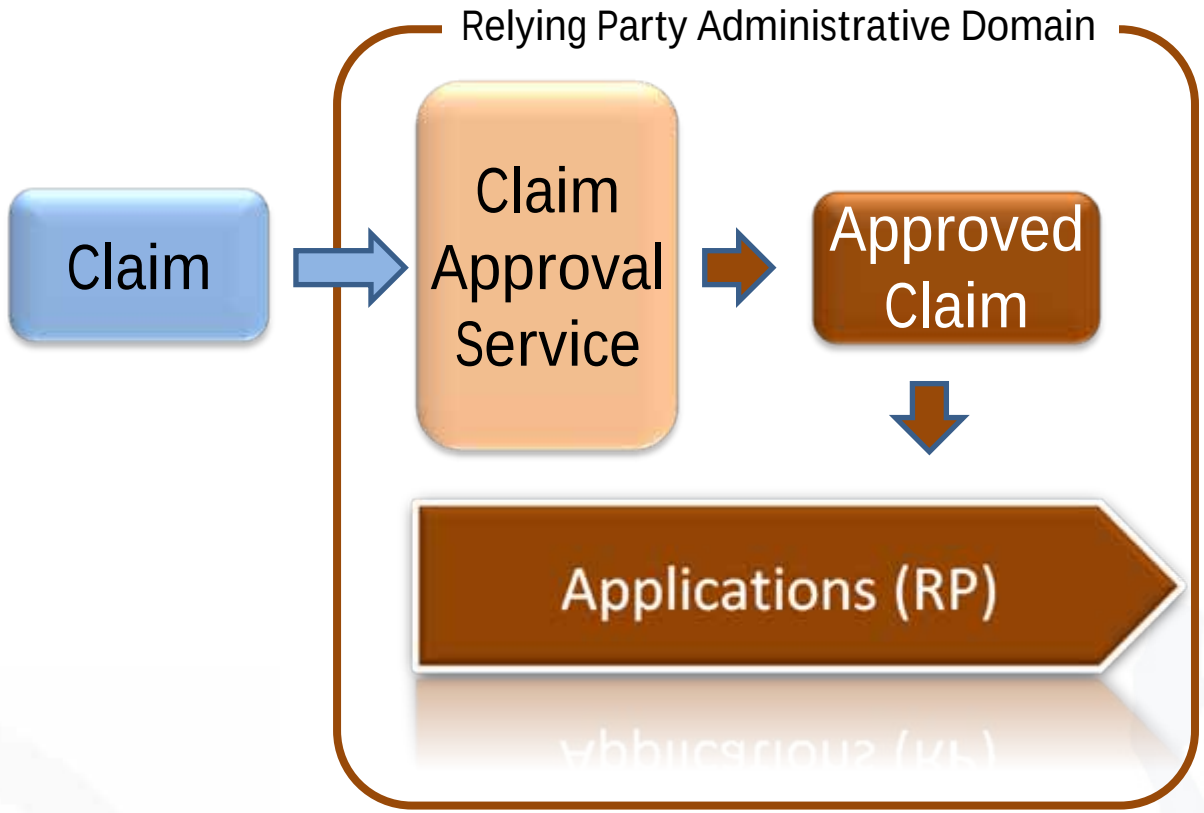
Building trust with minimum disclosure

- Users
  - State their properties and attributes (claims)
  - Organize corresponding credentials
  - Present what is needed according to policy (negotiation) but not more (minimum disclosure)
- Relying parties
  - Make policy decisions what assurance they need for which kind of service.
  - Reduce risk and liability, e.g.
    - Rely on assertions from trusted parties rather than unnecessarily maintaining sensitive information

Information flows between parties



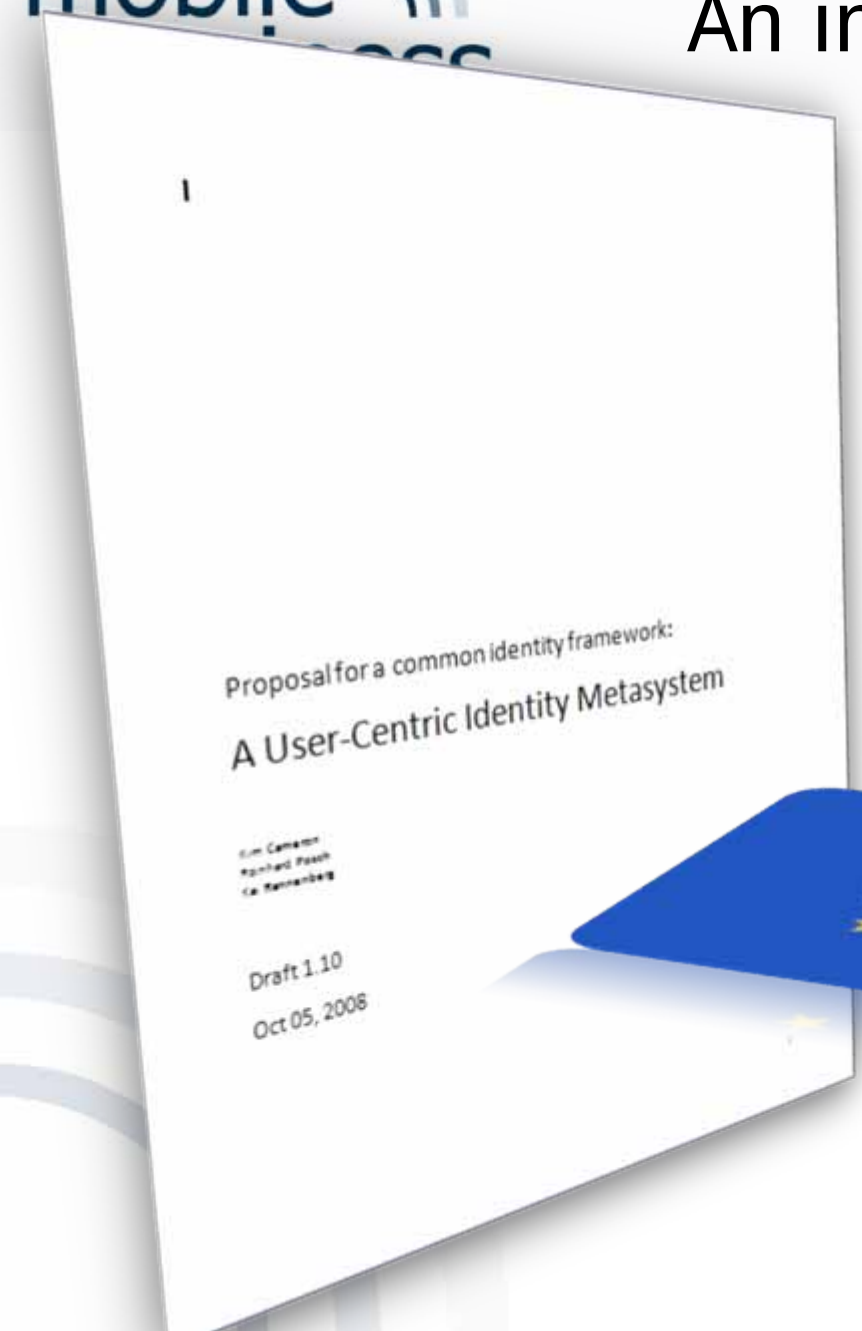
Relying parties

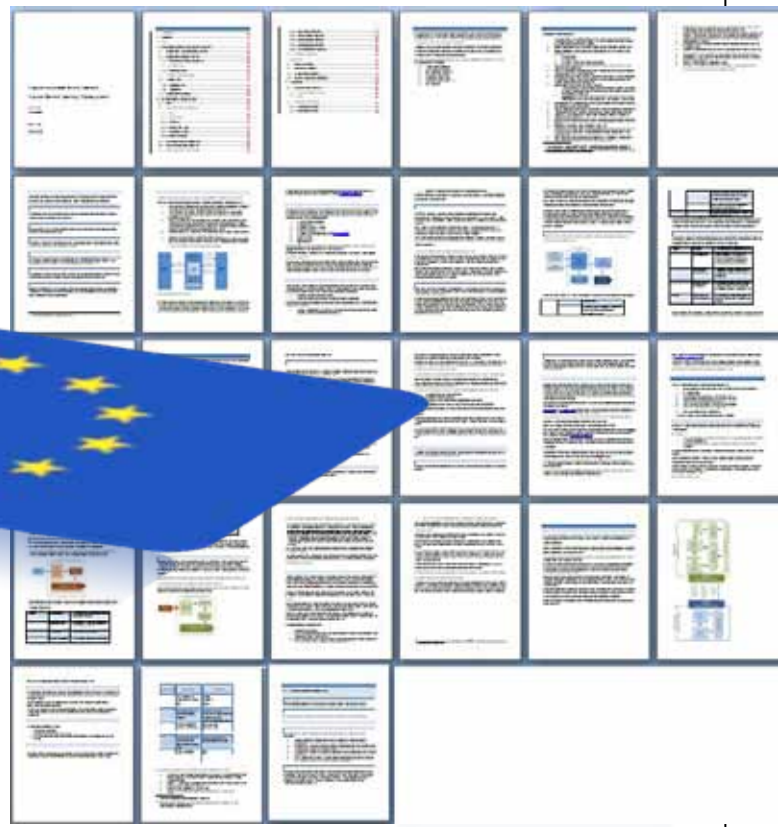


- ... consider and approve claims

An international conversation

- Kim **Cameron**
- Reinhard **Posch**
- Kai **Rannenberg**





Agenda

- Views on Identity Management
- Partial Identities
- Strong Sovereign Identifiers
  - Able to protect themselves
  - Standing with their holders
- Building trust with minimum disclosure
- Conclusions and Outlook

Challenges & Potential Identity Management

- Considering
  - the views of the respective stakeholders (Multilateral Security)
  - separations of domains that had been natural “before”
- Enabling users to manage their identities
- Frameworks and reference architectures
  - Along the value chain (with appropriate incentives)
  - For business processes and applications
  - For new communities and networks
- Globally standardized (e.g. in ISO/IEC JTC 1/SC 27/WG 5 “Identity Management and Privacy Technologies)

Conclusions & Outlook

- Identity management is happening (silently and via application (creep)).
- ICT and new services are coming ever closer to people.
- ➢ Trust is essential and requires:
  - ➢ Partial Identities
  - ➢ Strong Sovereign Identifiers
  - ➢ Minimum Disclosure

@ IFIP Sec 2009

- Kai.Rannenberg@m-chair.net
- www.m-chair.net
- www.fidis.net
- www.prime-project.eu
- www.picos-project.eu
- www.primelife.eu

References

- Kim Cameron, Reinhard Posch, Kai Rannenberg: Proposal for a common identity framework: A User-Centric Identity Metasystem
- FIDIS: Future of Identity in the Information Society; www.fidis.net
- FIDIS Deliverable 3.6: Study on ID Documents; 2006; www.fidis.net
- ISO/IEC JTC 1/SC 27/WG 5: Identity Management and Privacy Technologies; www.jtc1sc27.din.de
- PICOS: Privacy and Identity Management for Community Services; www.picos-project.eu
- PRIME: Privacy and Identity Management for Europe; www.prime-project.eu
- PrimeLife: Privacy and Identity Management for Life; www.primelife.eu
- Kai Rannenberg: Multilateral Security – A concept and examples for balanced security; Pp. 151-162 in: Proceedings of the 9th ACM New Security Paradigms Workshop 2000, September 19-21, 2000 Cork, Ireland; ACM Press; ISBN 1-58113-260-3
- Kai Rannenberg: CamWebSim and Friends: Steps towards Personal Security Assistants; Pp. 173 - 176 in Viktor Seige et al.: The Trends and Challenges of Modern Financial Services – Proceedings of the Information Security Summit; May 29-30, 2002, Prague; Tate International; ISBN 80-902858-5-6
- Kai Rannenberg: Identity management in mobile cellular networks and related applications; Information Security Technical Report; Vol. 9, No. 1; 2004; pp. 77 – 85; ISSN 1363-4127
- Kai Rannenberg ; Denis Royer; Andre Deuker: The Future of Identity in the Information Society - Opportunities and Challenges; Springer Verlag; to appear in May 2009
- T-Mobile Chair for Mobile Business & Multilateral Security; www.m-chair-net
- Jan Zibuschka, Lothar Fritsch, Mike Radmacher, Tobias Scherner, Kai Rannenberg: Enabling Privacy of Real-Life LBS: A Platform for Flexible Mobile Service Provisioning; in Proceedings of the 22nd IFIP TC-11 International Information Security Conference 2007; 14-16 May 2007, Sandton, South Africa; Springer IFIP Series
- Jan Zibuschka, Mike Radmacher, Tobias Scherner, Kai Rannenberg: Empowering LBS Users: Technical, Legal and Economic Aspects; in: Proceedings of the eChallenges conference 2007; The Hague, The Netherlands

BackUp

The FIDIS initial challenge: "Identity" is changing

- IT puts more HighTech on ID cards
  - Biometrics to bind them closer to a human being
  - Chips to add services (such as a PKI)
- Profiles may make the „traditional" ID concept obsolete
  - People are represented not by numbers or ID keys any more but by data sets.
  - Identities become "a fuzzy thing".
- New IDs and ID management systems are coming up
  - Mobile communication (GSM) has introduced a globally interoperable „ID token": the Subscriber Identity Module
  - Ebay lets people trade using Pseudonyms.
- Europe (the EU) consider joint ID and ID management systems
  - European countries have different traditions on identity card use
  - Compatibility of ID systems is not trivial
- ...

Future of Identity in the Information Society (FIDIS)

- ***Vision:*** Europe will develop a deeper understanding of how appropriate identification and ID management can progress the way to a fairer European information society.

- **Why an EU FP 6 Network of Excellence?**
  - Consequences of "new" IDs are unclear
  - "Change" Trends come from different fields and disciplines
  - Joint work will promote the European Information Society

⇒ FIDIS NoE : An international interdisciplinary **N**etwork **o**f **E**xcellence on the **F**uture of **ID**entity in the **I**nformation **S**ociety (2004-04-01 – 2009-06-30)

FIDIS Participants

- Goethe University Frankfurt, D
- AXSionics AG, CH
- BUTE-UNESCO Information Society Research Institute, H
- Europäisches Microsoft Innovations Center GmbH, D
- European Institute of Business Administration, F
- Institut de recherche criminelle de la gendarmerie nationale, F
- Institute for Prospective Technological Studies, E
- International Business Machines Corporation, CH
- Karlstad University, S
- Katholieke Universiteit Leuven, B
- London School of Economics & Political Science, GB
- Masarykova universita v Brne, CZ
- National TU of Athens, GR
- Netherlands Forensic Institute, NL
- SIRRIX Security Technologies, D
- TU Berlin, D
- TU Dresden, D
- Tilburg University, NL
- Unabhängiges Landes-zentrum für Datenschutz, D
- University of Freiburg, D
- University of Reading, GB
- VaF, Bratislava, SK
- Virtual Identity and Privacy Research Center, CH
- Vrije Universiteit Brussels, B

What can FIDIS offer (to Europe)?

What do we want to achieve within the next years?

- Being a respected expert player (pool of experts) in the identity discussions
- A collection of Information
  - ID Management systems
  - ID regulation (legislation and case law)
  - How they are used
  - …
- Coordinated expert publications (Deliverables available at www.fidis.net)
- Supporting the scene
  - Research Institutions
  - Scientific Communities
  - Standardisation Bodies (ISO/IEC JTC 1, ETSI,…)
  - Decision makers

Joint Research of FIDIS Topics/Activities

- „Identity of Identity“
- The HighTechID and emerging technologies
- Interoperability of IDs and ID management systems
- Profiling and AmI Environments
- Forensic Implications
- De-Identification
- Privacy
- Mobility and Identity

Selected FIDIS Deliverables

- D2.1: Inventory of Topics and Clusters
- D2.2: Set of use cases and scenarios
- D2.3: Models
- D3.1: Overview on IMS
- D3.3: Study on Mobile Identity Management
- D3.6: Study on ID Documents
- D3.8: Study on protocols with respect to identity and identification – an insight on network protocols and privacy-aware communication
- D3.9: Study on the Impact of Trusted Computing on Identity and Identity Management
- D4.1: Structured account of approaches on interoperability
- D5.1: A survey on legislation on ID theft in the EU and a number of other countries
- D6.1: Forensic Implications of Identity Management Systems
- D7.2: Descriptive analysis and inventory of profiling practices

ISO/IEC JTC 1/SC 27 „IT Security Techniques“ in ISO/IEC JTC 1

ISO International Organization for Standardization

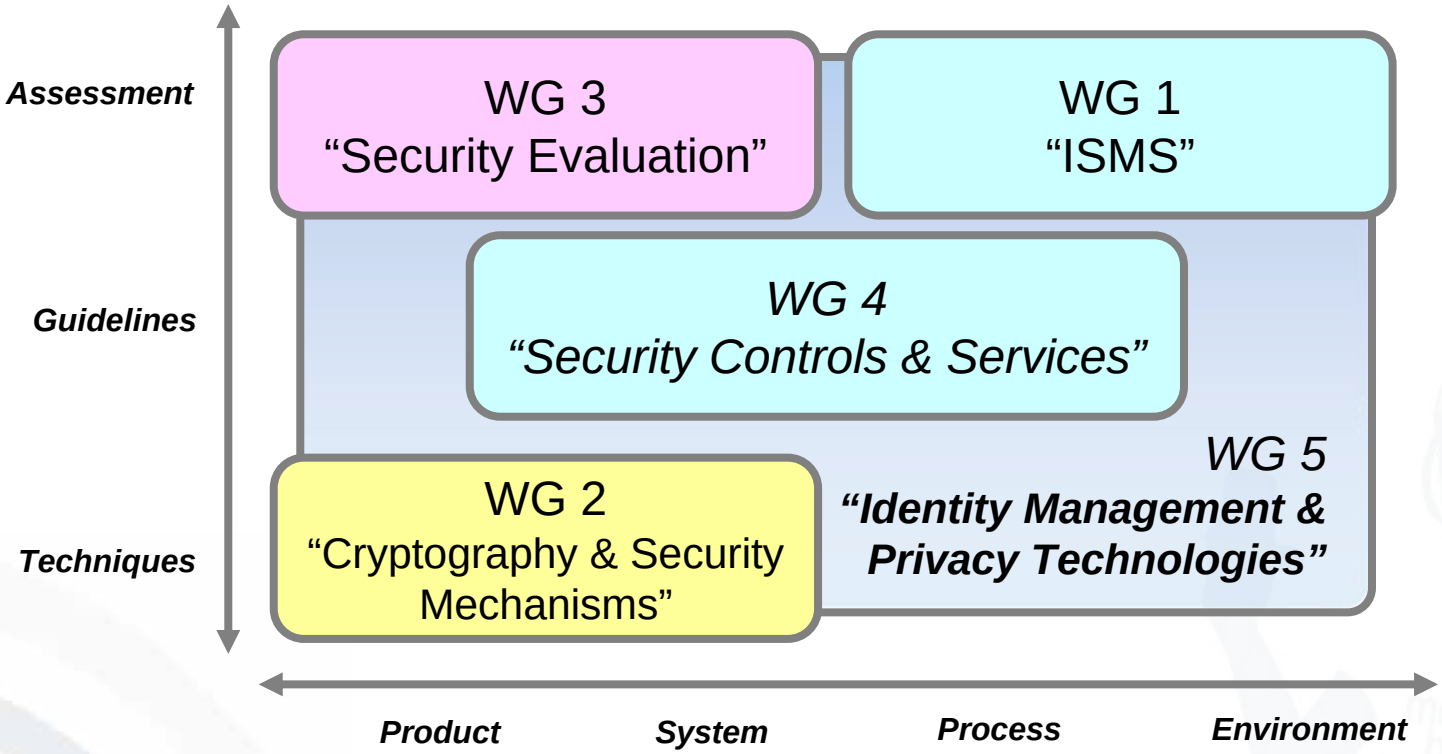
IEC International Electrotechnical Commission

ISO JTC 1 IEC
Information Technology Standards

Joint Technical Committee 1

Subcommittee 27 „IT Security Techniques“
www.ni.din.de/sc27

ISO/IEC JTC 1/SC 27 "IT Security Techniques" Structure



*WGs in **italics** are new*

How can a secure identifier protect itself?

- Processing power to do complex operations, e.g. crypto
- Storage space to have some „memory“
- Alternative/redundant means of communication for e.g. checking of reader certificates

Challenges & Potential for Europe

- User-Centricity
- Identity Management
- Minimisation and decentralisation of data
- (Standardized) reference architectures to integrate fragmented details
- Raising trustworthiness of embedded systems

Challenges & Potential User-Centricity

- Empowering users to …
  - better control of (identity) data flows
    - User-controlled hardware (Trustable computing) for
      - Identity data
      - (Anonymous) Communications
    - Transparent policies
  - select trusted partners from a choice of offers
    - Identity intermediary networks
    - Service provider networks
  - deal with the trade-offs
    - Testbeds to
      - Experience tradeoffs
      - … and quickly “feel” the results of the respective decisions.

- Minimising and decentralising data
  - Respecting proportionality
  - Reducing temptation
  - Avoiding misuse
  - Raising transparency on data flows
  - ...

- (Standardized) reference architectures to integrate fragmented approaches
  - Privacy enhancing technologies (PETs)
  - Identity management
  - Credentials
  - Information flow control
  - ...

- Raising trustworthiness of embedded systems
  - Addressing e.g. computerized/networked cars and household appliances
  - Combining experiences from Safety and IT Security
  - Improving transparency
  - …