Privacy and Identity Management for Europe

- The PRIME project receives research funding from the Community’s Sixth Framework Programme and the Swiss Federal Office for Education and Science.

- Integrated Project in the Information Society Technologies Priority

- Duration: 4 years (March 2004 – February 2008)

- Budget: M€ 18 (M€ 10 granted EC contribution, M€ 1 Swiss contr.)

- Number of Partners: 20

- Reference Group
PRIME Partners: Industry & Academia

IBM Belgium, B
IBM Zürich Research Lab, CH
Unabhängiges Landeszentrum für Datenschutz, D
Technische Universität Dresden, D
Katholieke Universiteit Leuven, B
Universiteit van Tilburg, NL
Hewlett-Packard, UK
Karlstads Universitet, S
JRC / IPSC Ispra, I
Università di Milano, I
Centre National de la Recherche Scientifique / LAAS, F
Johann Wolfgang Goethe-Universität Frankfurt am Main, D
Chaum LLC, USA
RWTH Aachen, D
Institut EURECOM, F
Erasmus Universiteit Rotterdam, NL
Fondazione Centro San Raffaele del Monte Tabor, I
Deutsche Lufthansa, D
Swisscom, CH
T-Mobile, D
PRIME Goals
Identity, Privacy, and Trust Management

**Vision:** In the Information Society, users can act and interact in a safe and secure way while retaining control of their private sphere.

**Goal:** Empower the user to manage and protect her private data effectively.
PRIME's Objectives

- Advance the state-of-the-art in privacy-enhancing identity management
- Demonstrate how to embed (European) privacy laws and regulations into technology
- Empower individuals to effectively realise their right to privacy and informational self-determination

→ Development of real-world tools and solutions for identity management
   - Legal, Social, Economic Framework
   - Architecture and middleware prototype incl. Identity Mixer

→ Demonstrator for 3 real-world applications
   - eLearning (Anonymous Learning, Roles, Certificates)
   - Location based Services (Policies)
   - Airport Security Controls (Data Minimization)
PRIME Approach
Privacy Enhancing IDM Design Principles I

- Privacy needs an Integrated Approach
  - Legal, social, economic requirements
  - Roles and responsibility of different stakeholders
    - Individuals (users, data subjects)
    - User & Consumer associations
    - Policy Makers, Parlamentarians
    - Privacy Commissioners
    - Research Communities
    - Data processors
    - Service providers, Operators
    - Standardisation Organisations
    - System developers and designers
    - Business and industry organisations, Trade Unions
    - Law enforcement organisations
    - Media
Privacy Enhancing IDM Design Principles II

- Design must start from maximum privacy
  - Anonymous & secure communication
  - No transaction linking by default
  - Privacy friendly business processes
  - Sometimes special crypto application (voting, etc)
- Explicit privacy rules govern system usage
  - Explicitly set the rules
  - Explicitly set the per role settings
- Privacy rules must be enforced, not just stated
- Privacy enforcement must be trustworthy
- Privacy must be usable
  - Users need tool support for IDM
  - Tools must be *easy to use* (good HCI)
PRIME Solution: Identity Mixer
Identity Mixer: Superior Privacy Protection...

Idemix-enabled ID Card
Identity file:
Date of birth = 1980/12/01
Unique ID = 123456...
Address file

Gov Citizen CA
Issuer

Citizen

Vendor
Policy: Must be older than 21.

Proof:
“My ID Card states: I’m older than 21.”

- Citizen holds ID Card with idemix private certificates.
- Vendor may have simple policies “age > 21”...
- ID Card generates new token from the original private certificate.
- Proves “age > 21 according to ID Card”...

Important: new token valid under public key of the Gov Citizen CA!
**Identity Mixer**: Strong Privacy Protection...

- Citizen holds ID Card with *idemix* private certificates.
- Vendor may have simple policies “age > 21” or complex formulas (opinion poll)
- ID Card generates *new* token from the original private certificate.
- Proves complete logical formula over arbitrary attributes.

**Important**: Unlinkability implies strong privacy protection for honest citizens!

**Policy**: Must be older than 21.

**Opinion Poll**
- Must be older than 18 AND
- Live in Brussels AND
- not used poll yet.

**Proof**: “My ID Card states:
I’m older than 18 AND live in Brussels AND I have not attended this poll yet.”
**Identity Mixer: ... AND Strong Security**

- Citizen may be offline after transaction.
- In case of disputes or fraud, anonymity of perpetrators can be easily revoked by authorities.
- Proof token contains unique ID (e.g., SSN number, strongly encrypted): only readable by authorities.

**Important:** honest citizens stay anonymous whereas fraudulent individuals are easily caught.

**Opinion Poll Policy:** Must be older than 18 AND live in Brussels AND not used poll yet.
Partial Identities with Identity Mixer

- Single Secret Key
Partial Identities with Identity Mixer

- Single Secret Key
- Different IDs/Pseudonyms
Partial Identities with Identity Mixer

- Single Secret Key
- Different IDs/Pseudonyms
- Credentials on different nyms (e.g., identity on ID Card)
Partial Identities with Identity Mixer

- Single Secret Key
- Different IDs/Pseudonyms
- Credentials on different nyms (e.g., identity on ID Card)
- Controlled Release of Attributes (e.g., age>21)
- Enable Accountability & Anonymity
Conclusions

- Identity management with strong privacy protection is emerging significantly.
- Open standards are vital for enabling collaboration between all stakeholders and organizations.
- Do promote pseudonyms, partial identities, and controlled attribute release.
- When in doubt, empower the user!
Contact Information

Public Web Site
- www.prime-project.eu

Speaker at OECD IdM Workshop
- Thomas Gross (ZRL)
  tgr@zurich.ibm.com

Project Management & Coordination
- Eric Goderniaux (Brussels)
  eric_goderniaux@be.ibm.com