PRIME Project

Privacy and Identity Management for Europe

Minsk, November 2006

Yves Deswarte
LAAS-CNRS, Toulouse, France
deswarte@laas.fr

Regulations

- **OECD (1980): *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data***
- **Council of Europe (1981), EST 108: *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data***
- **UN General Assembly (1990): *Guidelines Concerning Computerized Personal Data File***
- **European Union Charter of Fundamental Rights, Art.8: "*right to respect for private and family life*"**
- **European Directives**
  - **95/46/EC (personal data)**
  - **2002/58/EC (electronic communications, replacing 97/66/EC)**

Privacy: Basic Principles (1)

- **Self-determination:**
  - Personal data belong to the person (e.g., medical records)
  - Each person should keep the control on his/her personal data:
    - As much as possible, on a personal device (smart card, PDA, personal computer)
    - When personal data are disclosed, the person can impose his/her demands on how the data are to be handled (Data Handling Policy, DHP):
      - Access control
      - Obligations: e.g., erasure date, notification in case of disclosure, filtering, ...

Privacy: Basic Principles (2)

- **Personal Data Minimization: "need to know"**
  - The only personal data to be disclosed are those needed for the agreed purpose, and only for the accomplishment of the agreed task...
  - .... and then erased or deleted
  - on the Internet like in real life
  - With some limits: some personal data must be disclosed to judicial authorities to solve disputes or to fight crime.

Example: Electronic Commerce (1)

- **Involved parties: a customer, a merchant, a delivery company, a credit card company, the customer's bank, the merchant's bank, ISPs, ...**
  - **The merchant does not need the customer's identity, but must be confident in the payment order.**
  - **The delivery company does not need to know the customer's identity, what the goods are, how much has been paid, but needs to know the physical characteristics (weight, volume, ...), and the delivery address.**
  - **The customer's bank does not need to know the merchant or what has been purchased, but needs to know the account to credit**

Example: Electronic Commerce (2)

- **The merchant's bank does not need to know the customer's identity, what has been purchased, ..., but only the amount to be credited to the merchant's account.**
- **The ISP needs to know nothing about the transaction, except the quality of the transmissions.**
- **...**

PRIME - Privacy and Identity Management for Europe

User-Controlled Identity Management is Possible!

A Holistic Approach

- Legal, Social & Economic Framework
- Architecture
- Prototype implementation of architecture & user interface
- Application demonstrator (Collaborative eLearning, LBS)
- Tutorials (general public, end-user, experts)
- Research in all areas

Privacy Enhancing Technologies (PETs)

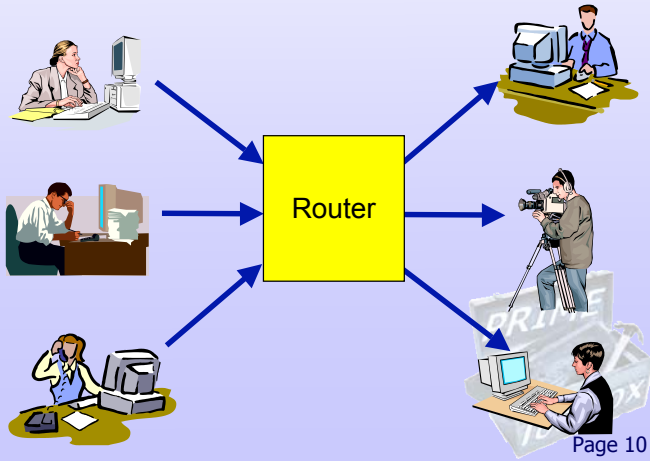
- **Identity management**
- **Anonymous communications**
- **Privacy-preserving authorization**
- **Personal data management**

Identity management

- **Linkability control: Reduce the links between a person and his/her actions, data or metadata**
- **Multiple identities (*pseudonyms*) for multiple actions:**
  - **Multiple identities rather than "Single-Sign-On"**
  - **Preferences: e.g., meteo**
  - **Roles: tax payer vs. elector**
  - **Authentication strength should be adapted to the identity theft risks / liability**
  - **Time validity adapted to the pseudonym use (linkability), from permanent to single use**

Anonymous Communciations

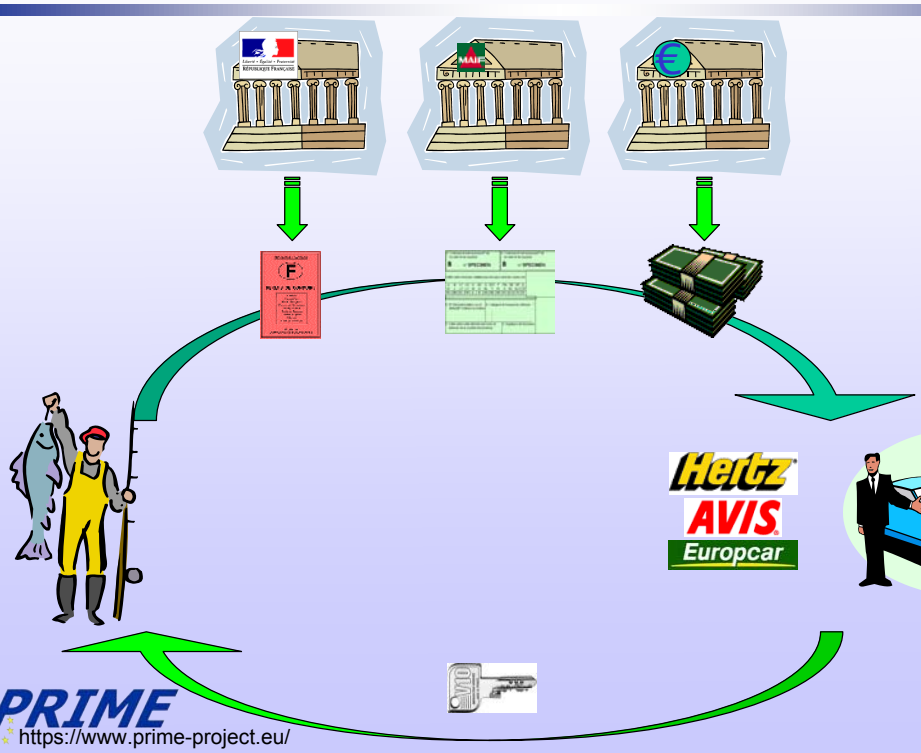
- **Traffic Analysis: an IP @ is a sensitive information**
  - **Identifying a user**
  - **Identifying the user's location**
  - **Server address = topics of interest**
- **MIX**
  = deciphering router



Privacy-Preserving Authorization

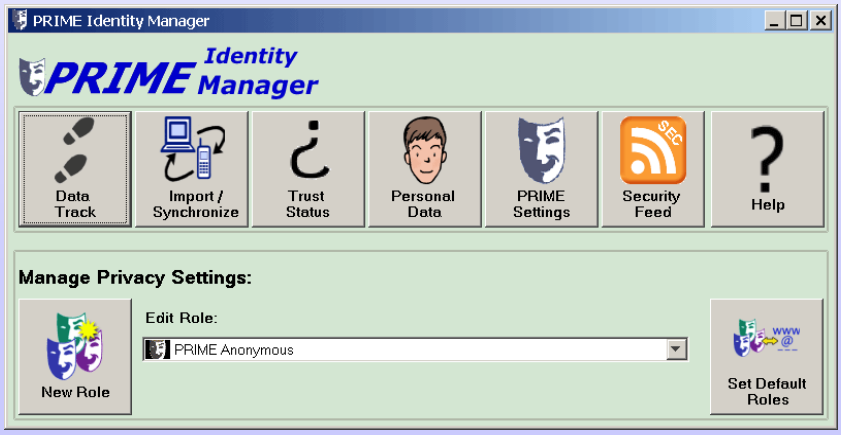
- **Some accesses are restricted to privileged users**
- **Classical solution: server discretionary control**
  - **The server grants/denies access according to the identity claimed by the client**
    - **Requires authentication, personal data storage**
    - **Personal data are collected to serve as evidence in case of dispute**
    - **These personal data can be abused: client profiling, direct marketing, customers file trading, blackmailing, etc.**

Anonymous Credentials

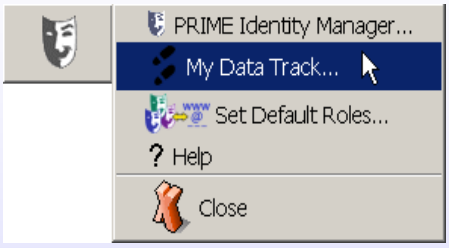


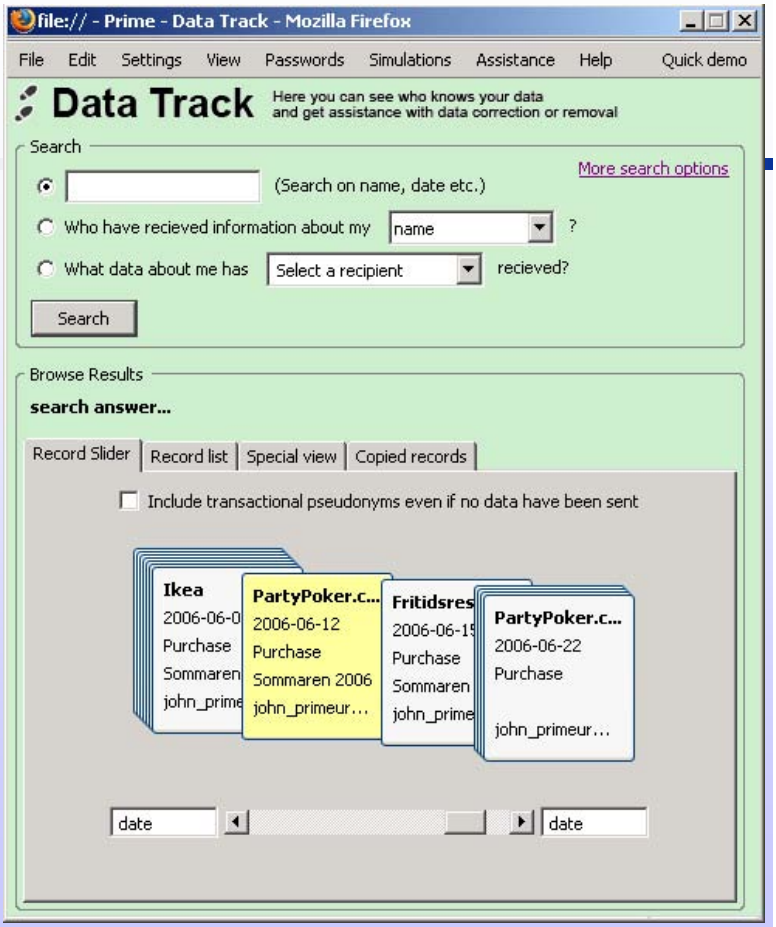
PRIME User-side implications

- Human factors
- Data track management
- Credential management
- Preference authoring and management
- Trust management
- Reputation management



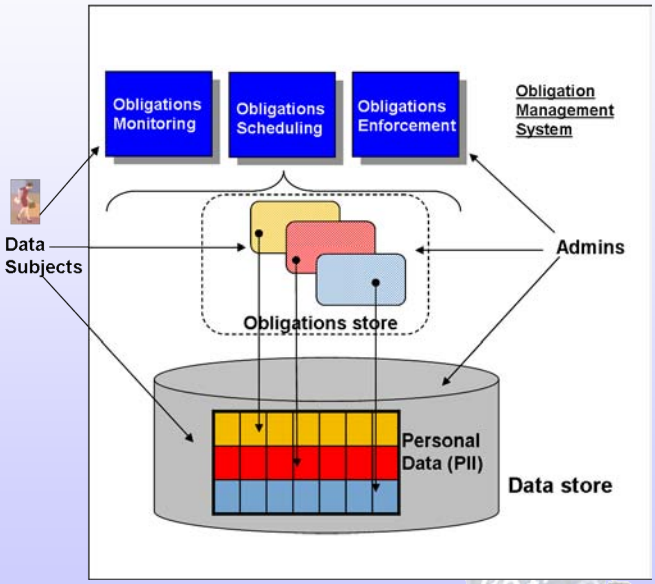
Data Track





PRIME Services-side implications

- **Fine-grained access control**
- **Obligation management**
- **Policy negotiation**
- **Policy compliance check and feedback**



Further information

- **www.prime-project.eu**
- **March 2004 to February 2008**
- *The PRIME project receives research funding from the European Union's Sixth Framework Programme and the Swiss Federal Office for Education and Science.*

Information Society Technologies