Concepts of Privacy-Enhancing Identity Management for Privacy-Enhancing Security Technologies

PRISE
privacy • security

PRISE Conference

“Towards privacy enhancing security technologies – the next steps”

April 28-29, 2008 in Vienna

Marit Hansen

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Overview

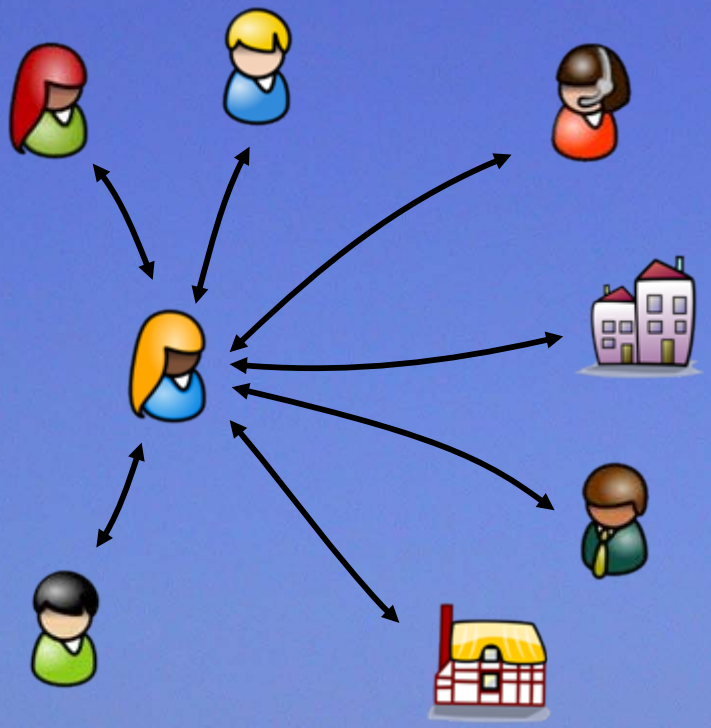
- Enhancing user-centric identity management: PRIME – Privacy and Identity Management for Europe
  - Objective
  - Building blocks
    - “Various Pseudonyms and Private Credentials”
    - “Anonymous Communication”
    - “Transparency Functionality”

- How to use components of privacy-enhancing identity management in security technologies?

ULD-i
Datenschutz innovativ

Vision of PRIME

– Privacy and Identity Management for Europe



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

Slide: PRIME Project / Jan Camenisch

Example: Anonymous Wine Shop

Wine Shop

Proof (age > 20),
enc_K(name, address)

User

enc_K(name, address)

Shipping Company

K (public key)

“Anonymous user”
Proof of age > 20 AND
Encryption of name & addr with K

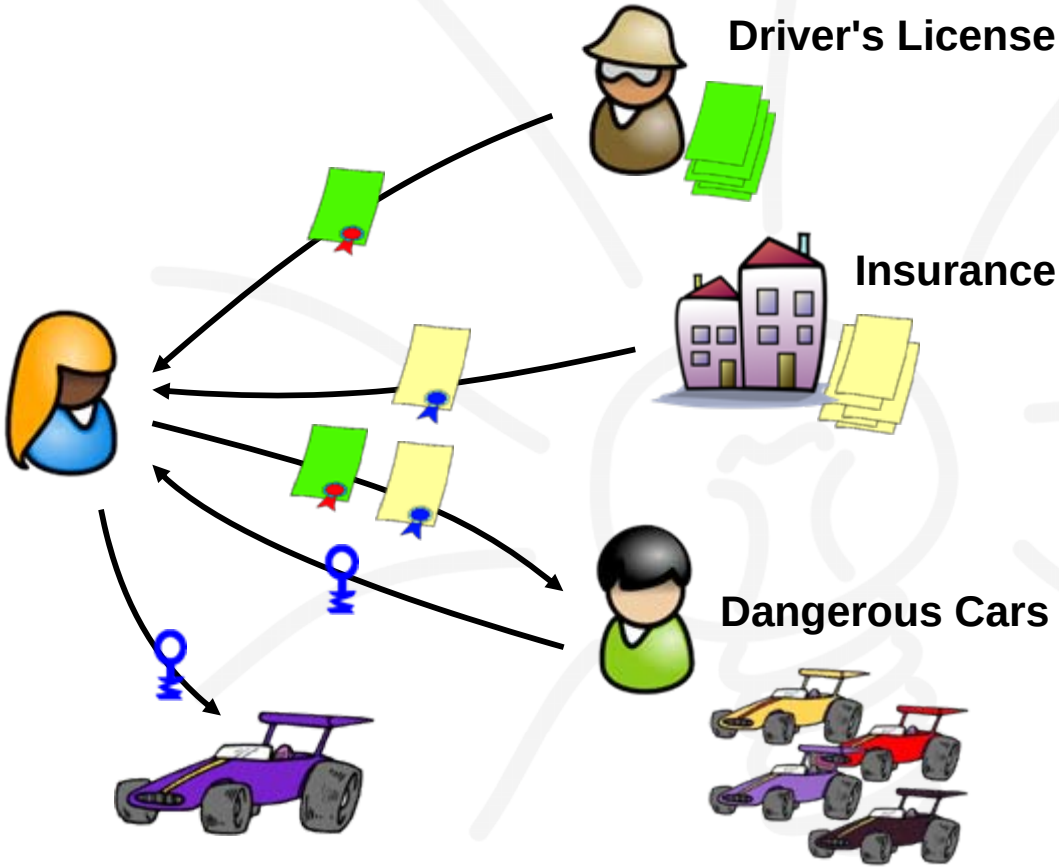
“Registered user”
Cryptographic pseudonym

Building Block “Various Pseudonyms and Private Credentials”

Anonymity & strong authentication at the same time

ULD-i
Datenschutz innovativ

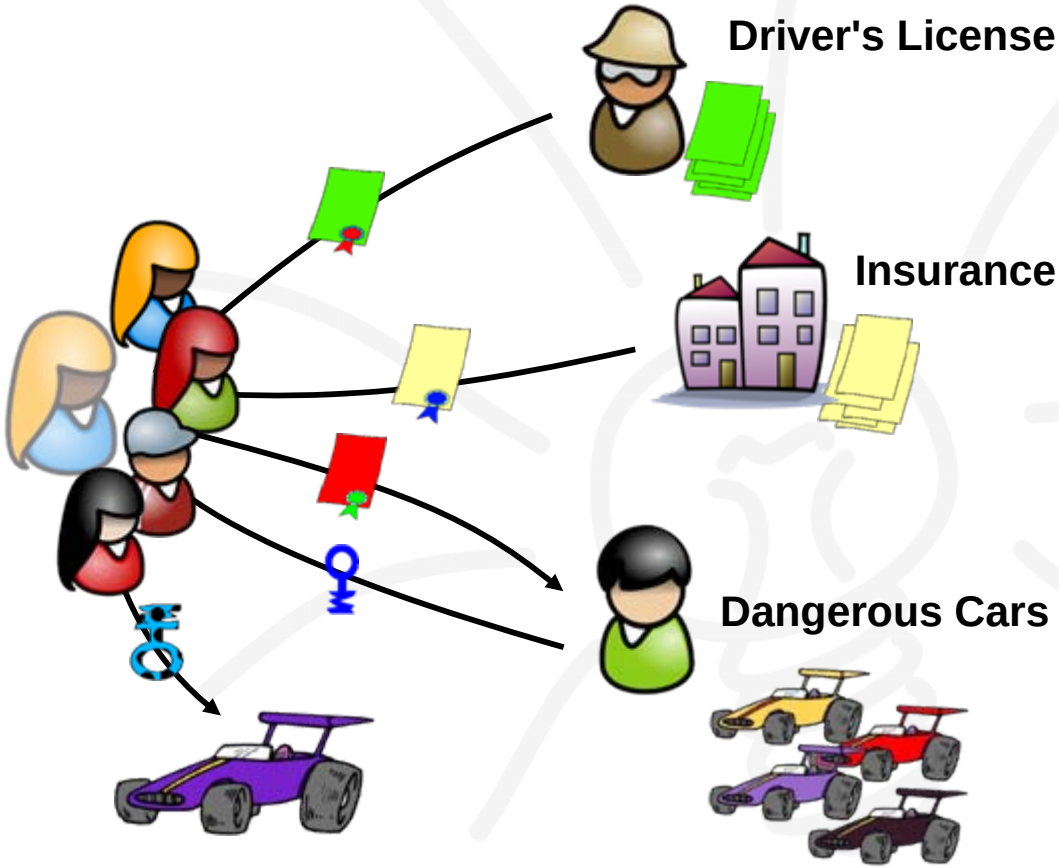
What's the Problem?



Slide: PRIME Project / Jan Camenisch

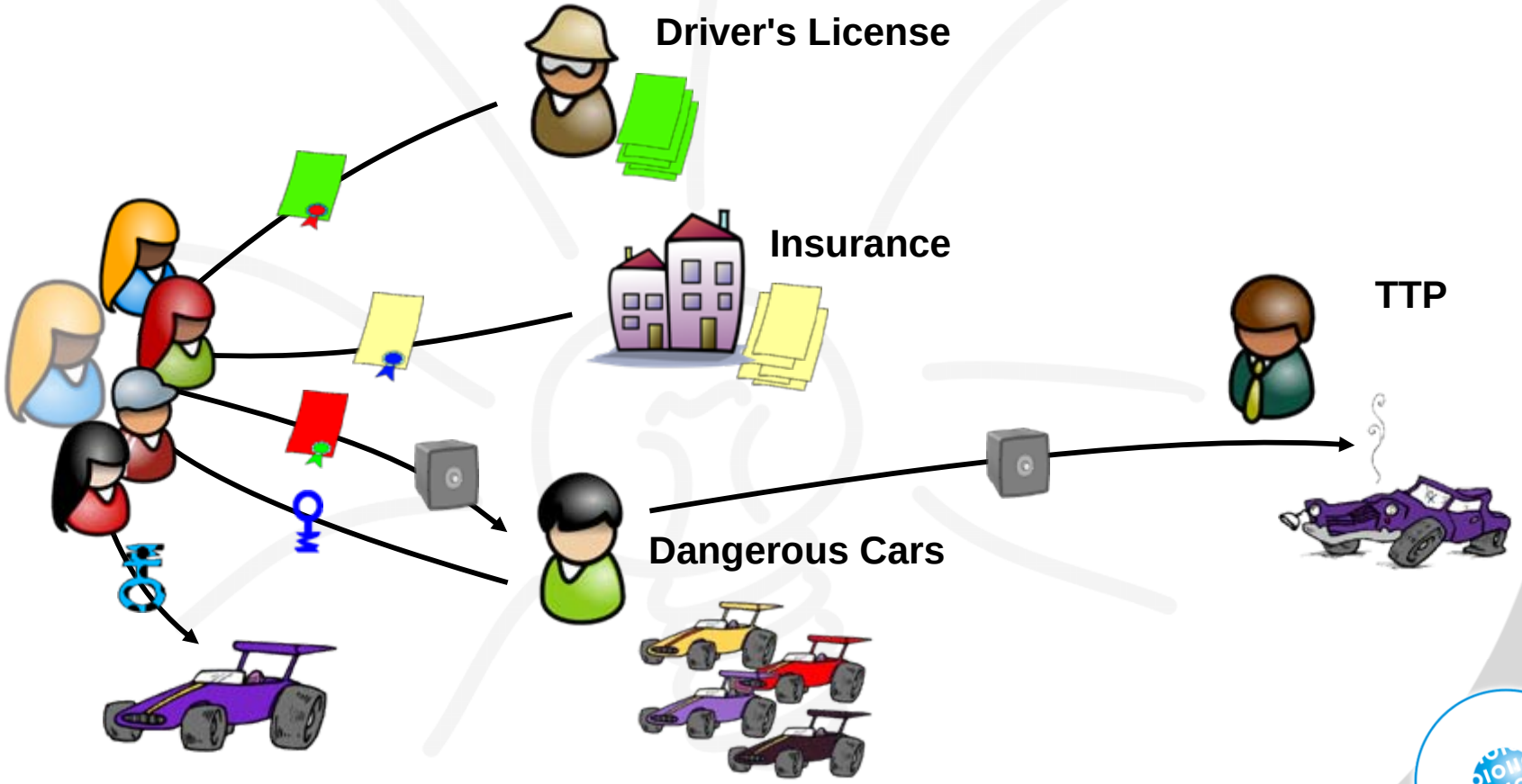
ULD-i
Datenschutz innovativ

The Solution: Private Credentials



Slide: PRIME Project / Jan Camenisch

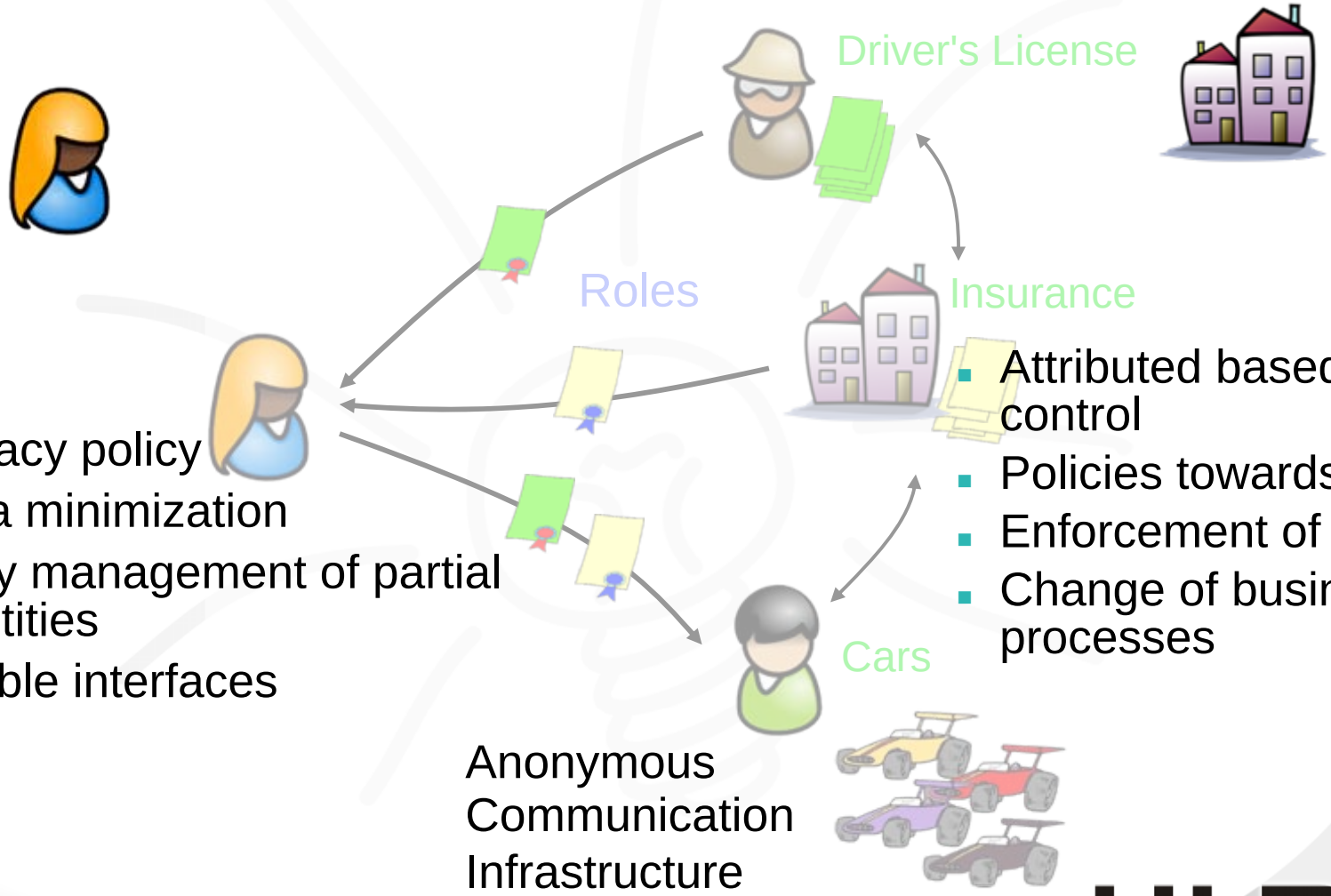
The Solution: Private Credentials



Slide: PRIME Project / Jan Camenisch

ULD-i
Datenschutz innovativ

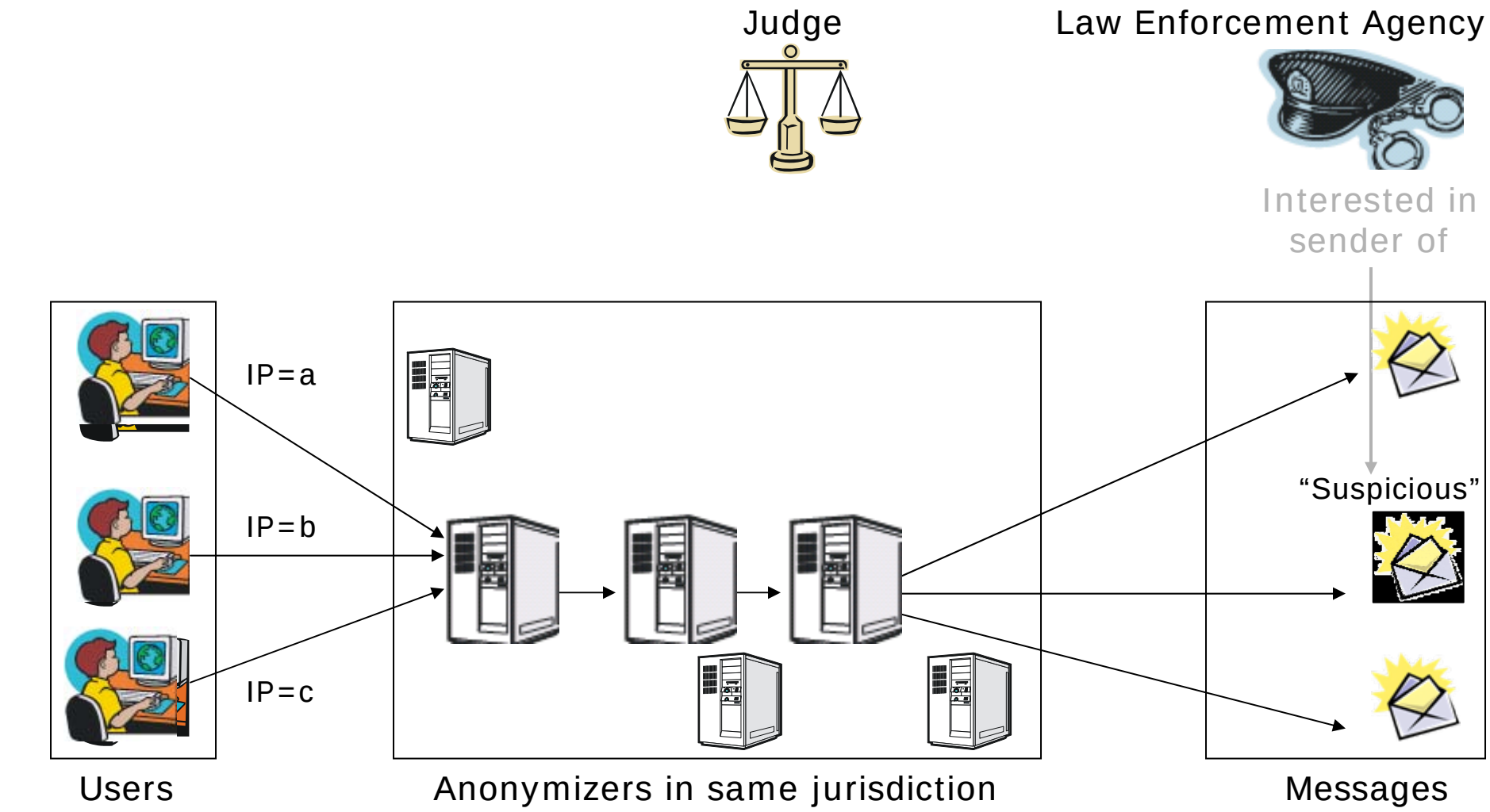
The Full Picture: What is needed?



- Privacy policy
- Data minimization
- Easy management of partial identities
- Usable interfaces

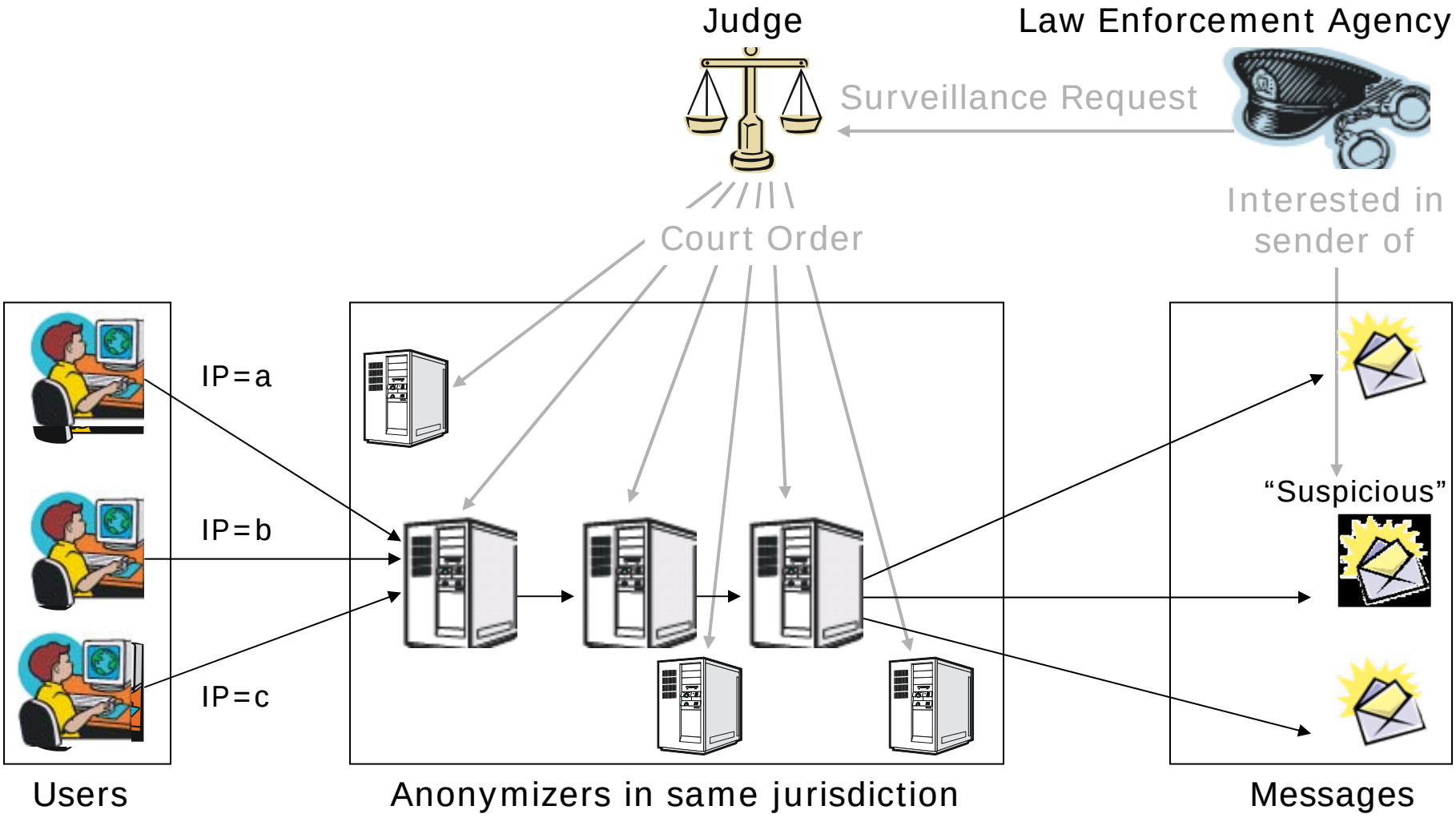
- Attributed based access control
- Policies towards users
- Enforcement of policies
- Change of business processes

Anonymous Communication Infrastructure (1/3)



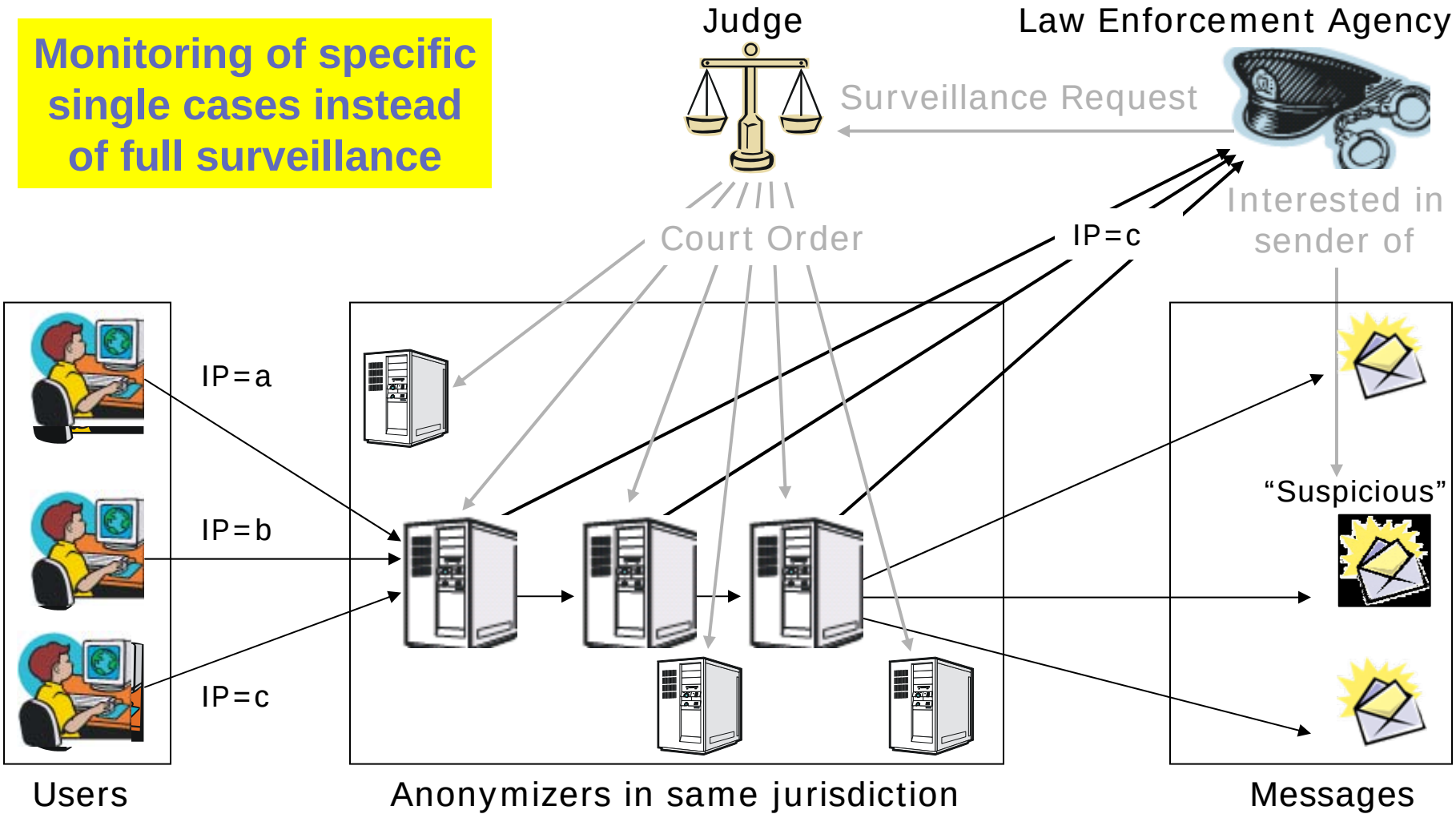
Slide: AN.ON Project / Stefan Köpsell – www.anon-online.de

Anonymous Communication Infrastructure (2/3)



Anonymous Communication Infrastructure (3/3)

Monitoring of specific single cases instead of full surveillance



Building Block “Transparency Functionality”

Giving information in an **understandable** way

&

empowering users to act accordingly

ULD-i

Datenschutz innovativ

Overview: Transparency Functionality

- **Objective:** empower users to understand and act

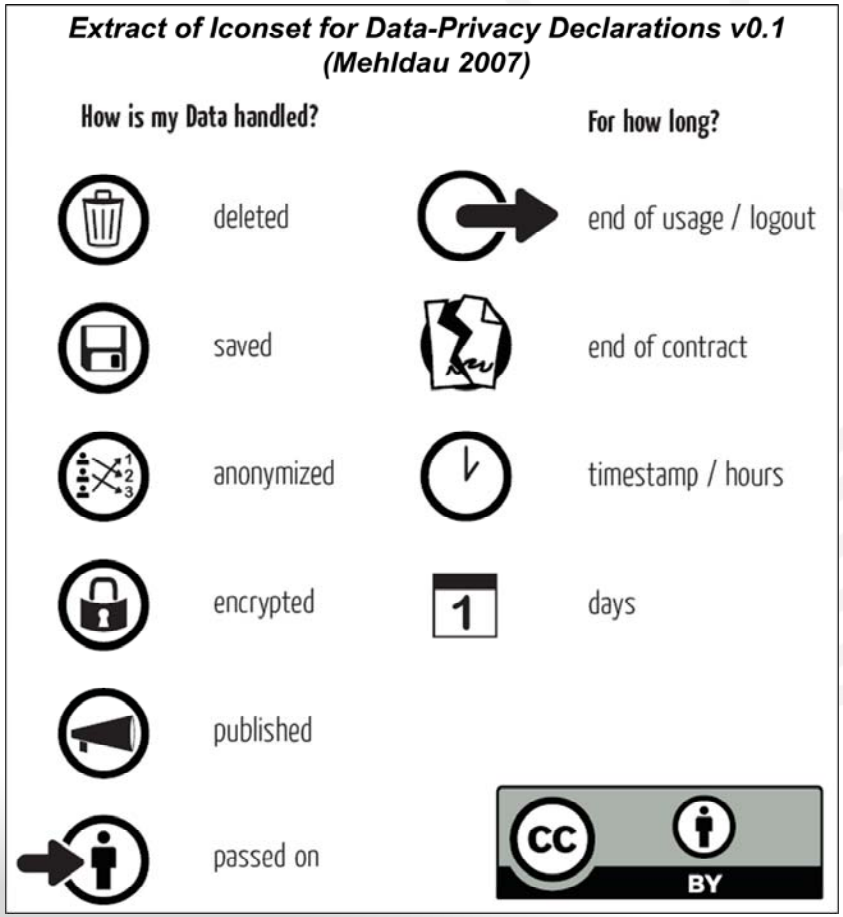
- **Examples in privacy-enhancing identity management:**
  - Showing privacy policies: conditions of data processing
  - Trustworthiness of transaction partners
  - History function
  - Support of exercising privacy rights
  - Security feed
  - Tutorials, demonstrations and simulations

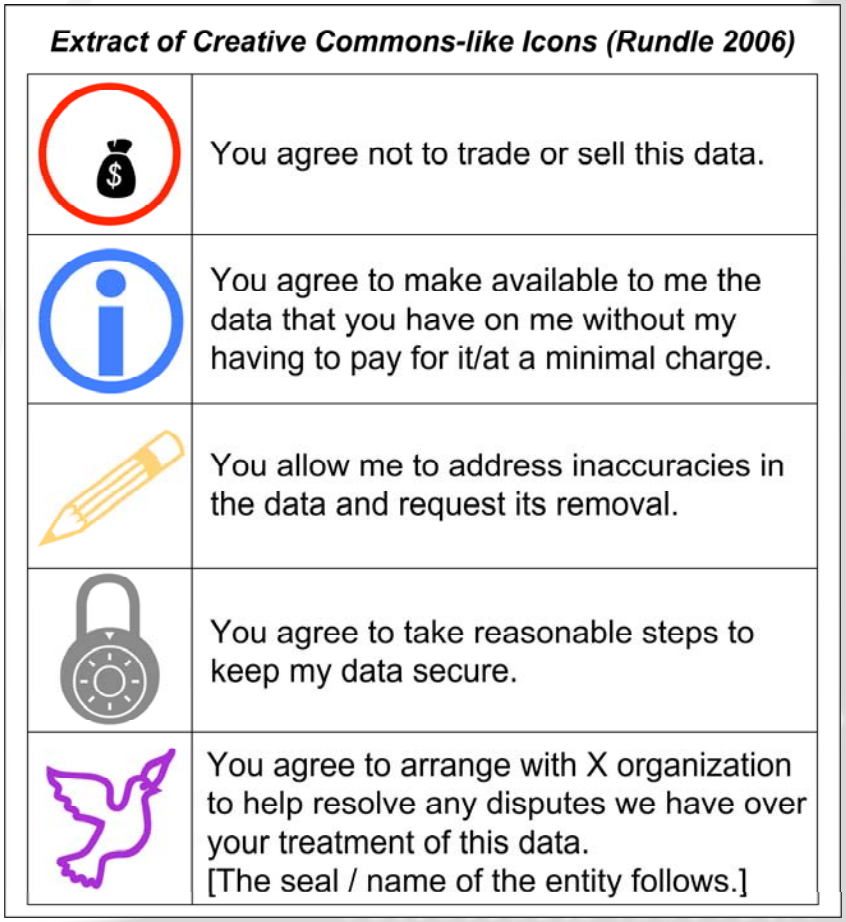
  - Server-side: full audit trail

ULD-i >>
Datenschutz innovativ

Understandable Privacy Policies

- **Jurisdiction:**
  Differences in law (data protection & law enforcement)
- **Transparency on data processing**

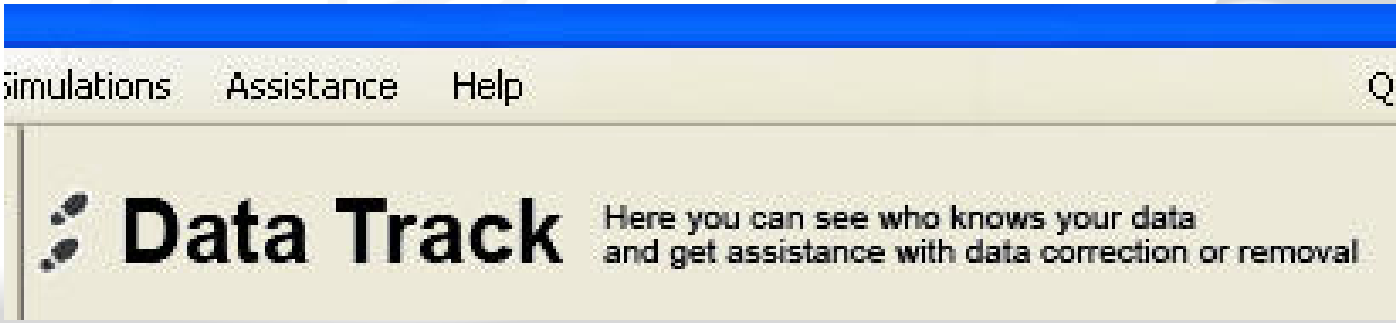




Online Help Functions

- **Support for exercising one's privacy rights, i.e.,**
  - **to request …**
    - **… access to personal data**
    - **… rectification of inaccurate personal data**
    - **… erasure of illegally stored data**
  - **to give or withdraw consent**
  - **to ask for further information on data processing**

- **Challenge: exercising rights under pseudonym**



Security Feed

- Demand of Security Breach Notification Acts
- Information on security & privacy incidents and threats
- Implemented as RSS feed

ULD-i
Datenschutz innovativ

Privacy-Enhancing Identity Management Concepts for Privacy-Enhancing Security Technologies?

Transparency functionality

	Objective in Privacy-Enhancing IDM	Security functionality
Various pseudonyms and private credentials	Protection against unauthorized linkage	
Anonymous communication infrastructure	Protection against unauthorized identification	
Policies	Make clear conditions for data processing	
Support to exercise privacy rights	Empower users, establish contacts to DPA / consumer protection	
Security feed	Inform people concerned on breaches	
Server-side: full audit trail		

Transparency functionality

	Objective in Privacy-Enhancing IDM	Security functionality
Various pseudonyms and private credentials	Protection against unauthorized linkage	Prevent misuse, enable authorized singularized linkage
Anonymous communication infrastructure	Protection against unauthorized identification	
Policies	Make clear conditions for data processing	
Support to exercise privacy rights	Empower users, establish contacts to DPA / consumer protection	
Security feed	Inform people concerned on breaches	
Server-side: full audit trail		

Transparency functionality

	Objective in Privacy-Enhancing IDM	Security functionality
Various pseudonyms and private credentials	Protection against unauthorized linkage	Prevent misuse, enable authorized singularized linkage
Anonymous communication infrastructure	Protection against unauthorized identification	Enable authorized singularized identification
Policies	Make clear conditions for data processing	
Support to exercise privacy rights	Empower users, establish contacts to DPA / consumer protection	
Security feed	Inform people concerned on breaches	
Server-side: full audit trail		

Transparency functionality

	Objective in Privacy-Enhancing IDM	Security functionality
Various pseudonyms and private credentials	Protection against unauthorized linkage	Prevent misuse, enable authorized singularized linkage
Anonymous communication infrastructure	Protection against unauthorized identification	Enable authorized singularized identification
Policies	Make clear conditions for data processing	Ditto; e.g., information on jurisdiction
Support to exercise privacy rights	Empower users, establish contacts to DPA / consumer protection	
Security feed	Inform people concerned on breaches	
Server-side: full audit trail		

Transparency functionality

	Objective in Privacy-Enhancing IDM	Security functionality
Various pseudonyms and private credentials	Protection against unauthorized linkage	Prevent misuse, enable authorized singularized linkage
Anonymous communication infrastructure	Protection against unauthorized identification	Enable authorized singularized identification
Policies	Make clear conditions for data processing	Ditto; e.g., information on jurisdiction
Support to exercise privacy rights	Empower users, establish contacts to DPA / consumer protection	Extension to “security bodies” possible: defined processes for access, better acceptance
Security feed	Inform people concerned on breaches	
Server-side: full audit trail		

Transparency functionality

	Objective in Privacy-Enhancing IDM	Security functionality
Various pseudonyms and private credentials	Protection against unauthorized linkage	Prevent misuse, enable authorized singularized linkage
Anonymous communication infrastructure	Protection against unauthorized identification	Enable authorized singularized identification
Policies	Make clear conditions for data processing	Ditto; e.g., information on jurisdiction
Support to exercise privacy rights	Empower users, establish contacts to DPA / consumer protection	Extension to “security bodies” possible: defined processes for access, better acceptance
Security feed	Inform people concerned on breaches	Use channel for communication to users *after* surveillance
Server-side: full audit trail		

Transparency functionality

	Objective in Privacy-Enhancing IDM	Security functionality
Various pseudonyms and private credentials	Protection against unauthorized linkage	Prevent misuse, enable authorized singularized linkage
Anonymous communication infrastructure	Protection against unauthorized identification	Enable authorized singularized identification
Policies	Make clear conditions for data processing	Ditto; e.g., information on jurisdiction
Support to exercise privacy rights	Empower users, establish contacts to DPA / consumer protection	Extension to “security bodies” possible: defined processes for access, better acceptance
Security feed	Inform people concerned on breaches	Use channel for communication to users *after* surveillance
Server-side: full audit trail	**Auditability, transparency on data quality, possibility to find errors and correct them**	

Melange of security objectives

- Prevention of misuse beforehand
  - Better authentication against identity theft
  - Know the degree of accuracy & completeness of data and their sources
- Protection of non-criminals (also against espionage) AND catching criminals
  - Support self-protection
  - Avoid mass surveillance
  - Keep data in own jurisdiction

For **individuals**
For **employees**
For **companies**

PRIVACY ≅ TRADE SECRETS

- Acceptance of society
  - Beware of criminalizing privacy-aware behavior
  - Provide transparency and checkability of law enforcement whenever possible

ULD-i
Datenschutz innovativ

What privacy-enhancing identity management cannot prevent

- Monitoring of people outside the scope of identity management
  - Biometric sensors
  - Video surveillance
  - RFID
- Collecting data voluntarily disclosed by users
- Non-favorable policies
  - But it can make them transparent
- Security breaches
  - But it can interpret information on security breaches

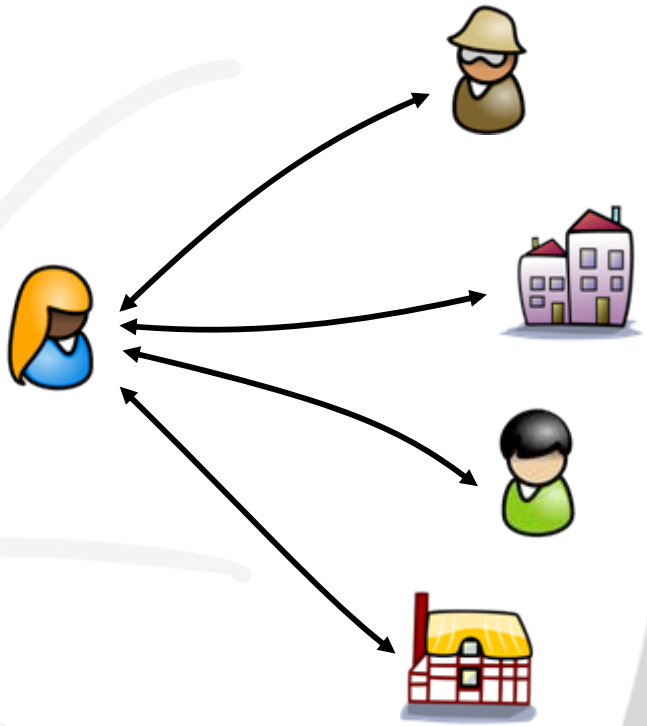
ULD-i
Datenschutz innovativ

Further information on PRIME

Closing Event:

21 July, 2008 in Leuven, Belgium

https://www.prime-project.eu/



Holistic approach:

- Legal, social & economic framework
- Architecture
- Prototype implementation of architecture & user interface
- Application demonstrators (Collaborative eLearning, LBS)
- Tutorials (general public, end-users, experts)
- Research in all areas

Launched in March 2008: Prime*Life!*

10 Million € FP7 Project

Duration: March 2008 – Feb 2011

Objectives:

- **Fundamentally understanding privacy-enhancing identity management “for life”**
- **Bringing privacy to the future web**
- **Making tools for privacy-enhancing identity management widely available – privacy live!**

http://www.primelife.eu/

incl. security

LinkedIn

facebook

myspace.com
a place for friends