# Joint ITU-T SG 17, ISO/IEC JTC 1/SC 27/WG 5 and FIDIS Workshop on Identity Management Standards

## Privacy and IdM
## Findings of the PRIME-Project

Jan Schallaböck

Independent Centre for Privacy Protection Schleswig-Holstein, Germany

30 September 2007, Lucerne, Switzerland

# A. Requirement: Informational Self-Determination

30 September 2007, Lucerne, Switzerland

"If anonymity of data is not entirely certain [...] individuals could be deprived of their autonomy (self-determination) and could be object to the will and control of others."

*BverfGE 61, 1 (101)*

# 1st Principle: Purpose Binding

30 September 2007, Lucerne, Switzerland

# 2nd Principle:<br>Deletion and Minimization of Data

30 September 2007, Lucerne, Switzerland

# 3rd Principle: Consent

30 September 2007, Lucerne, Switzerland

**“Sites should ask for identifying information, when there is some valid and defensible reason to do so. They should always ask for the minimum possible. They should keep it for the shortest possible time.”**

*Kim Cameron, Microsoft*

# Other principles:

- Access to data,
- Right to correction and deletion
- Transparency
- etc.

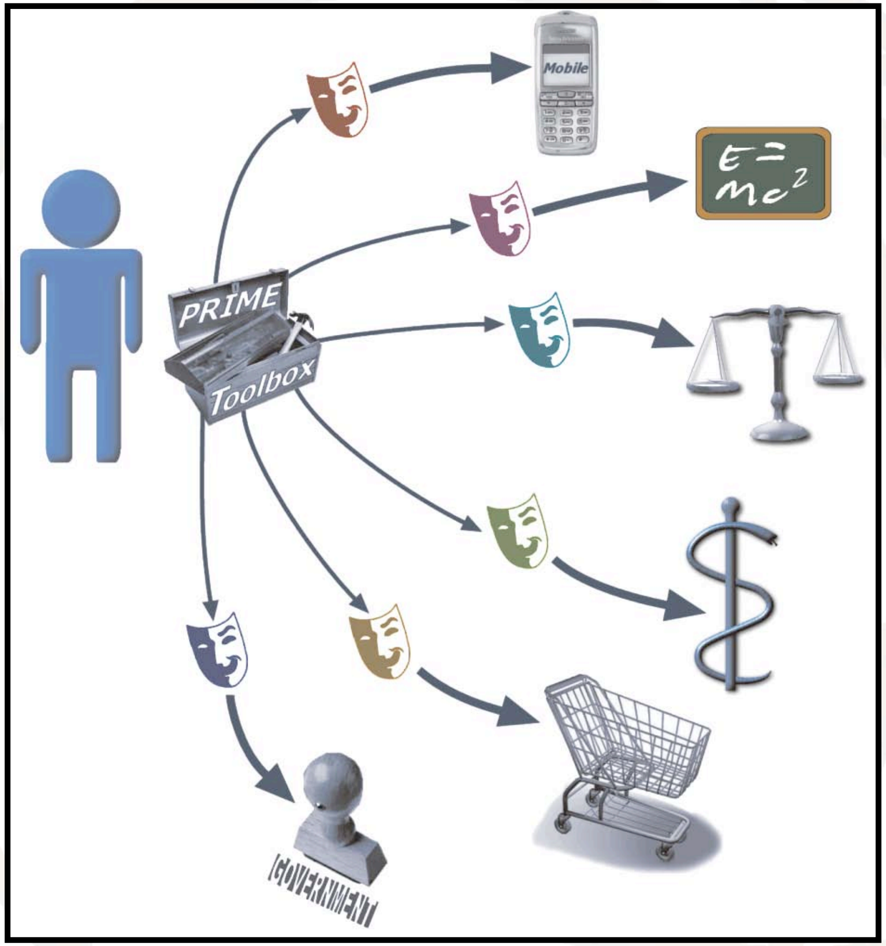
# B. Towards a Solution: Privacy Rights and Identity Management in Europe

The PRIME-Project

PRIME

30 September 2007, Lucerne, Switzerland

# The PRIME Approach



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

# PRIME Partners

IBM Belgium, B

IBM Zurich 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 and

T-Mobile, D

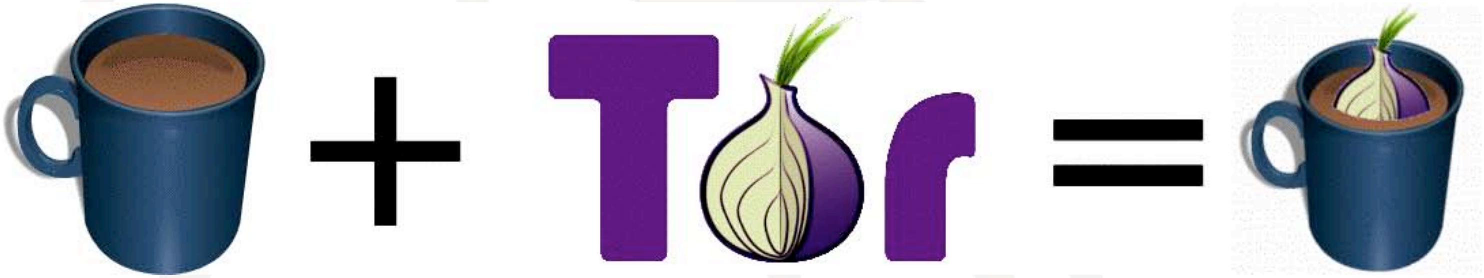
# PRIME Vision

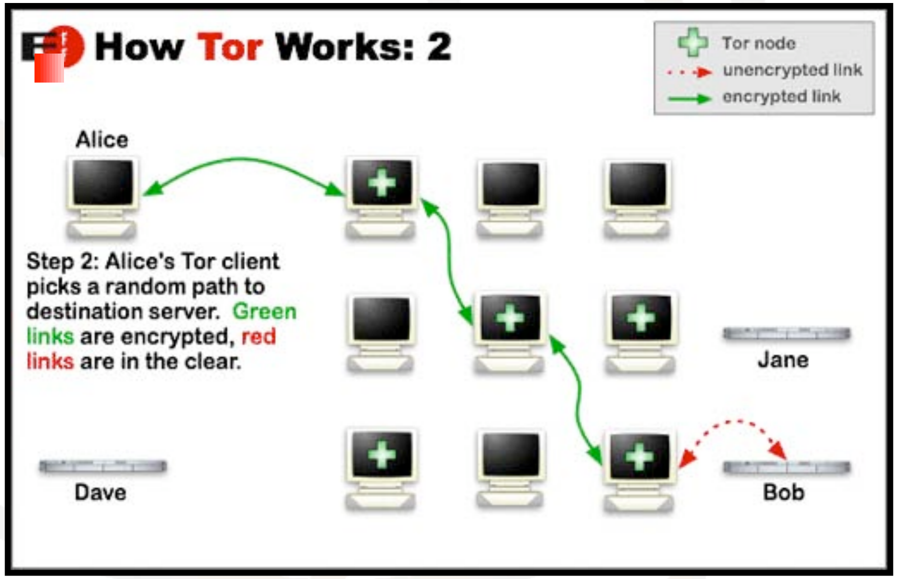
- Design starting from maximum privacy
- System usage governed by explicit privacy rules
- Privacy rules must be enforced, not just stated
- Trustworthy privacy enforcement
- Easy and intuitive abstractions of privacy for users
- Privacy integrated with applications

# Some core Elements of PRIME

- Data Minimization I: Onion Coffee
- Data Minimization II: Partial Identities
- Data Minimization III: Anonymous Credentials
- Purpose Binding: Policies
- Consent I: Purpose description
- Consent II: Reputation Mechanisms
- Right to Access and Trasperancy: Data Track

# Data Minimization I: OnionCoffee





## How Tor Works: 2

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

# Reducing Complexity

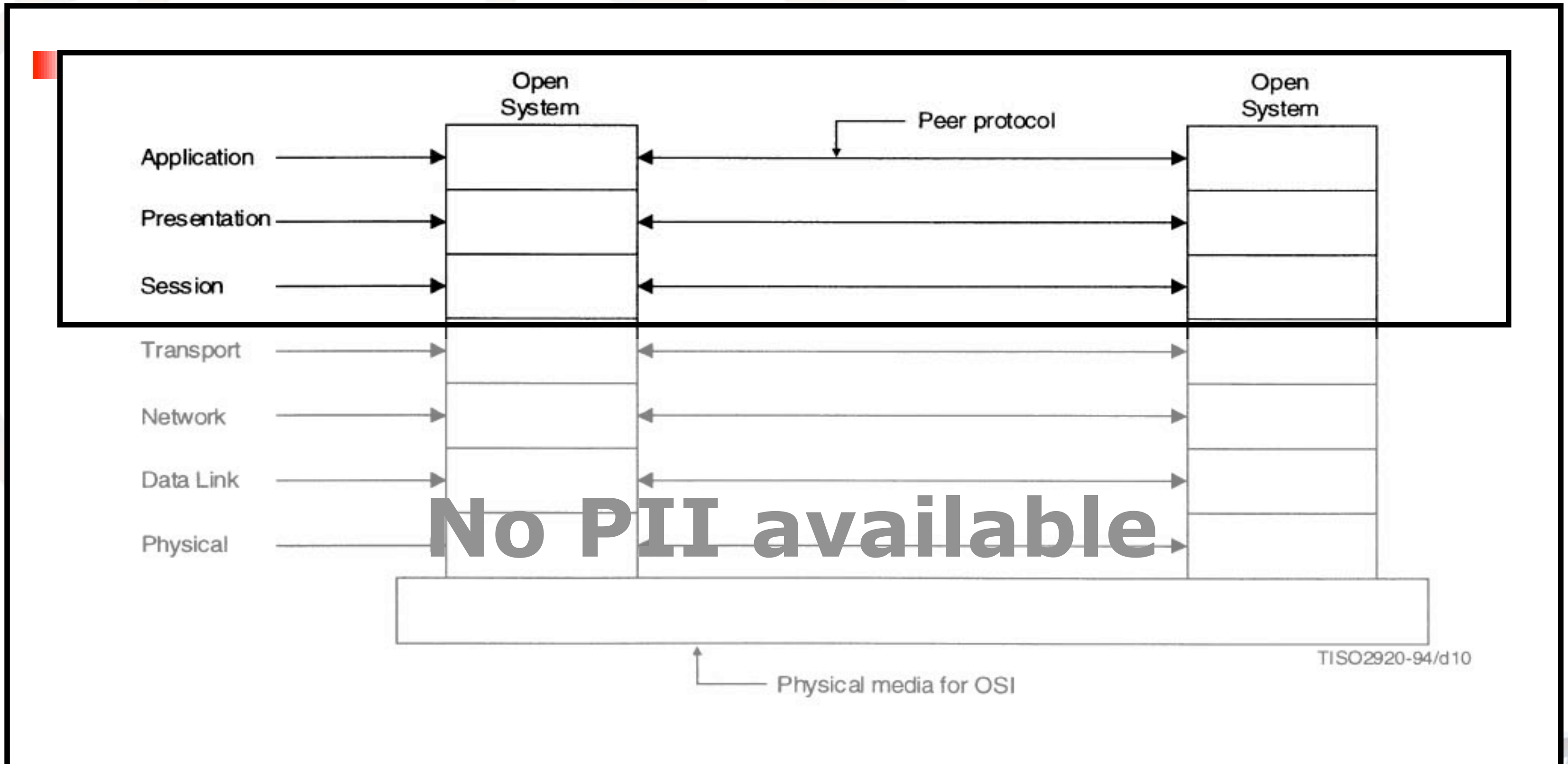
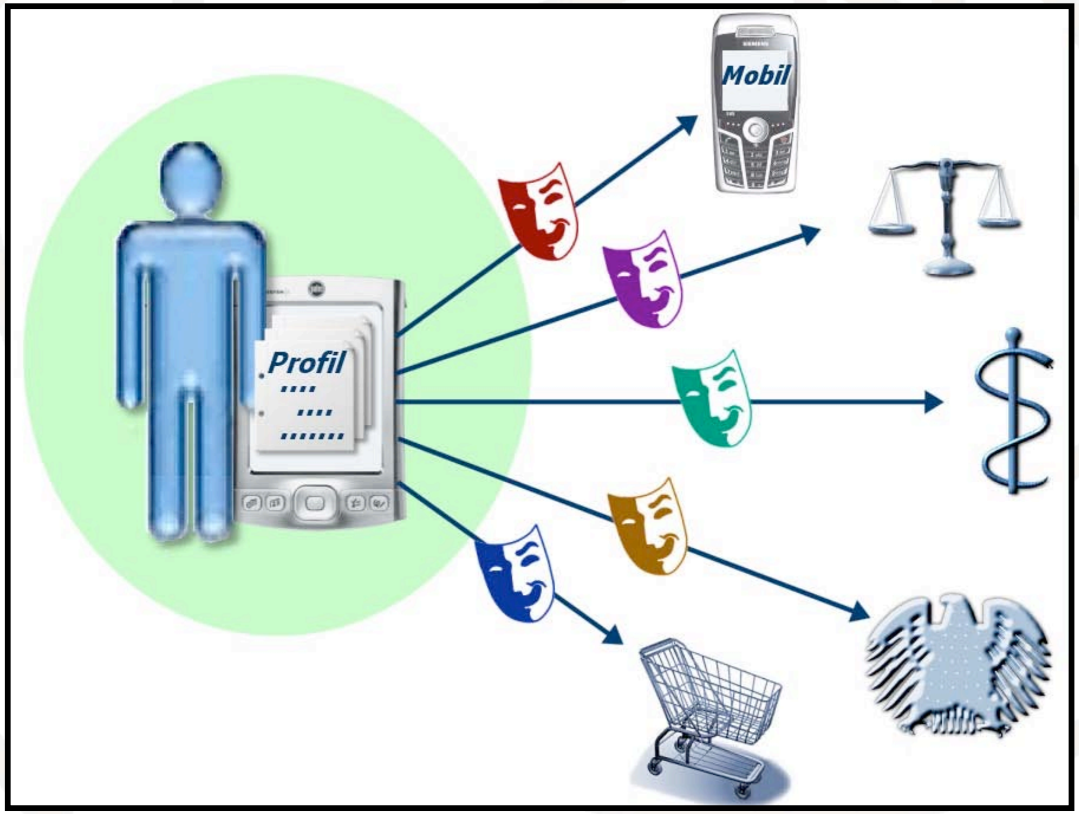
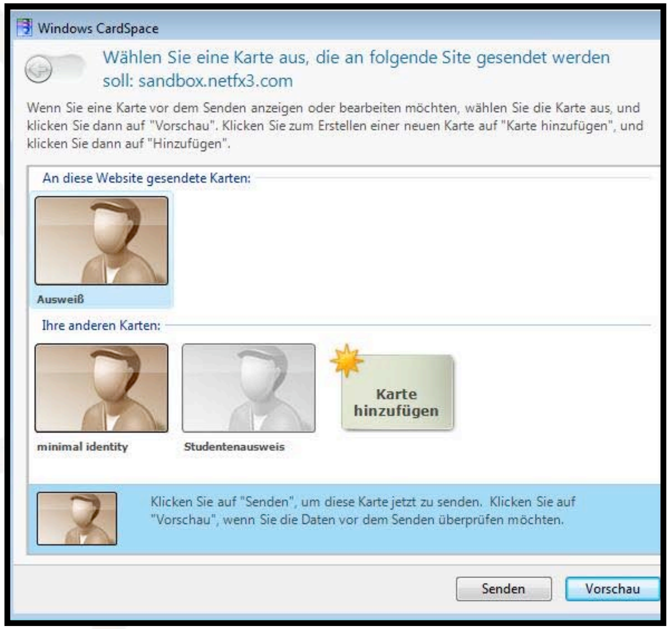


Figure 11 – Seven layer reference model and peer protocols

From: ISO/IEC 7498-1

# Data Minimization II: Partial Identities (Functional Differentiation)




Windows CardSpace

Wählen Sie eine Karte aus, die an folgende Site gesendet werden soll: sandbox.netfx3.com

Wenn Sie eine Karte vor dem Senden anzeigen oder bearbeiten möchten, wählen Sie die Karte aus, und klicken Sie dann auf "Vorschau". Klicken Sie zum Erstellen einer neuen Karte auf "Karte hinzufügen", und klicken Sie dann auf "Hinzufügen".

An diese Website gesendete Karten:

Ausweiß

Ihre anderen Karten:

minimal identity

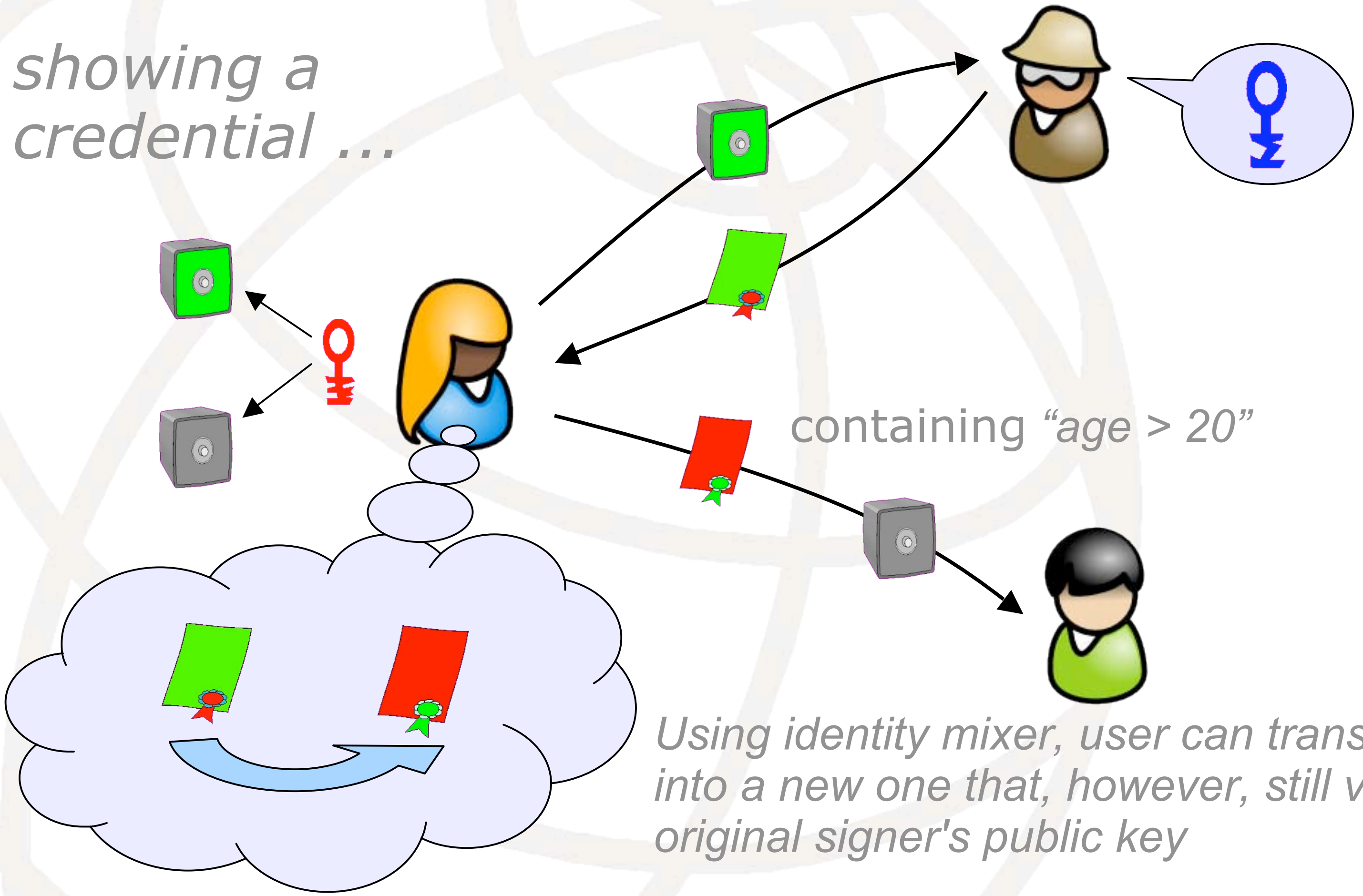
Studentenausweis

Karte hinzufügen

Klicken Sie auf "Senden", um diese Karte jetzt zu senden. Klicken Sie auf "Vorschau", wenn Sie die Daten vor dem Senden überprüfen möchten.

# Data Minimization III: Anonymous Credentials

*showing a credential ...*

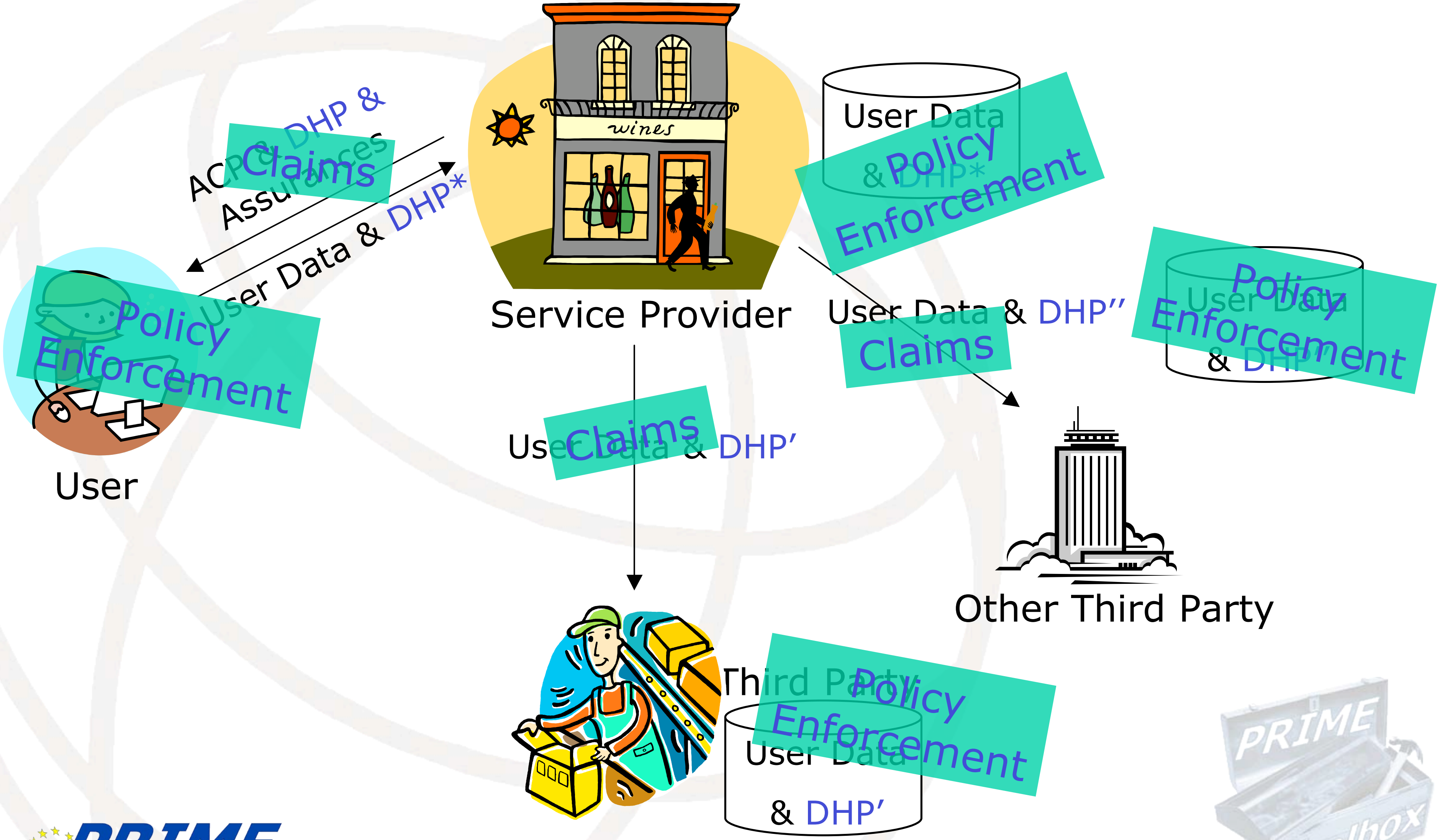


containing *“age > 20”*

*Using identity mixer, user can transform token into a new one that, however, still verifies w.r.t. original signer's public key*

*Slide by Jan Camenisch, IBM Research Zürich*

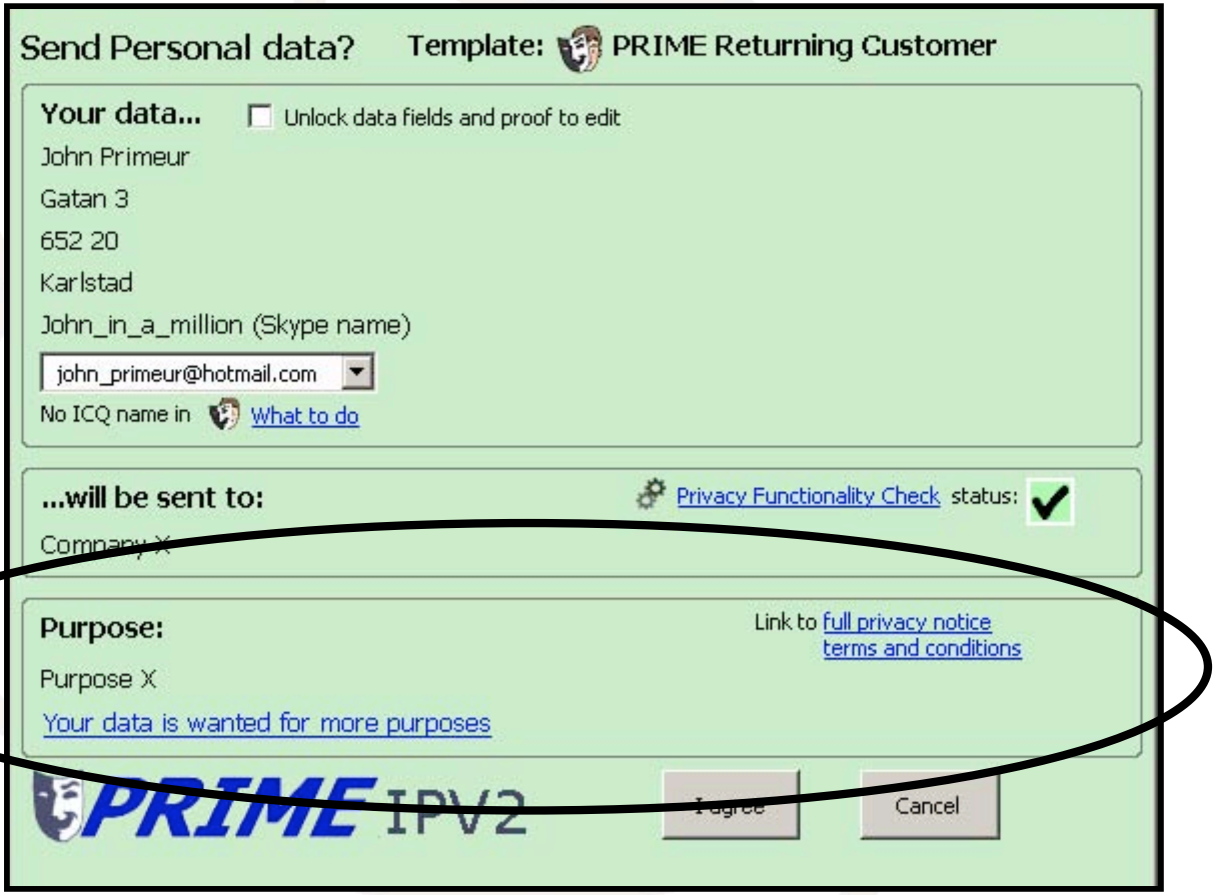
# Purpose binding: Policies



30 September 2007, Lucerne, Switzerland

*Slide by Dieter Sommer, IBM Research Zürich*

# Consent I: Purpose description



Send Personal data? Template: PRIME Returning Customer

Your data... □ Unlock data fields and proof to edit

John Primeur
Gatan 3
652 20
Karlstad
John_in_a_million (Skype name)
john_primeur@hotmail.com

No ICQ name in What to do

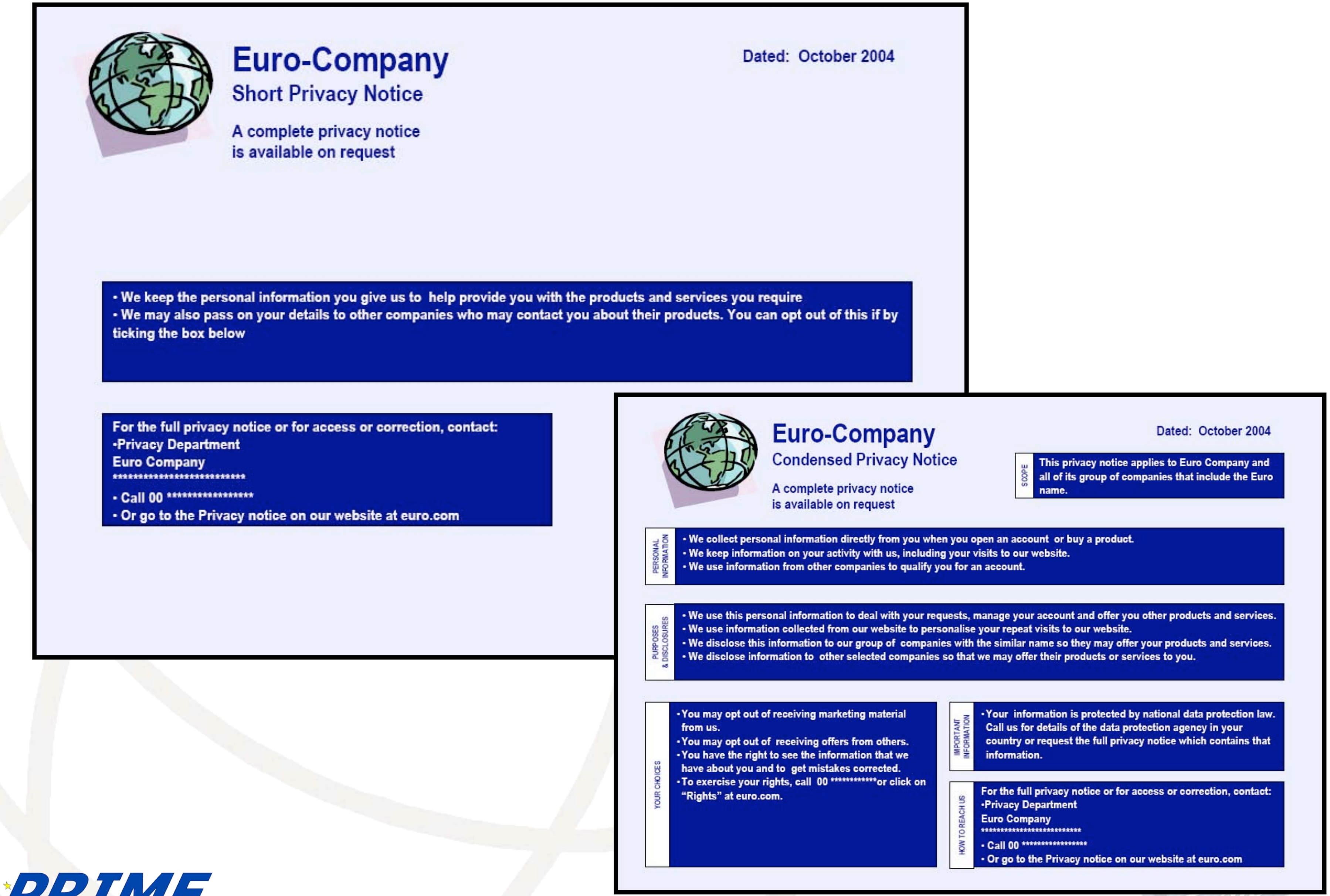
...will be sent to: Privacy Functionality Check status: ✓

Company X

Purpose: Link to full privacy notice terms and conditions

Purpose X

Your data is wanted for more purposes



## Euro-Company

### Short Privacy Notice

Dated: October 2004

A complete privacy notice
is available on request

- We keep the personal information you give us to help provide you with the products and services you require
- We may also pass on your details to other companies who may contact you about their products. You can opt out of this if by ticking the box below

For the full privacy notice or for access or correction, contact:
•Privacy Department
Euro Company
**************************
- Call 00 ******************
- Or go to the Privacy notice on our website at euro.com

## Euro-Company

### Condensed Privacy Notice

Dated: October 2004

A complete privacy notice
is available on request

SCOPE

This privacy notice applies to Euro Company and all of its group of companies that include the Euro name.

PERSONAL INFORMATION

- We collect personal information directly from you when you open an account or buy a product.
- We keep information on your activity with us, including your visits to our website.
- We use information from other companies to qualify you for an account.

PURPOSES & DISCLOSURES

- We use this personal information to deal with your requests, manage your account and offer you other products and services.
- We use information collected from our website to personalise your repeat visits to our website.
- We disclose this information to our group of companies with the similar name so they may offer your products and services.
- We disclose information to other selected companies so that we may offer their products or services to you.

YOUR CHOICES

- You may opt out of receiving marketing material from us.
- You may opt out of receiving offers from others.
- You have the right to see the information that we have about you and to get mistakes corrected.
- To exercise your rights, call 00 ************or click on "Rights" at euro.com.

IMPORTANT INFORMATION

- Your information is protected by national data protection law. Call us for details of the data protection agency in your country or request the full privacy notice which contains that information.

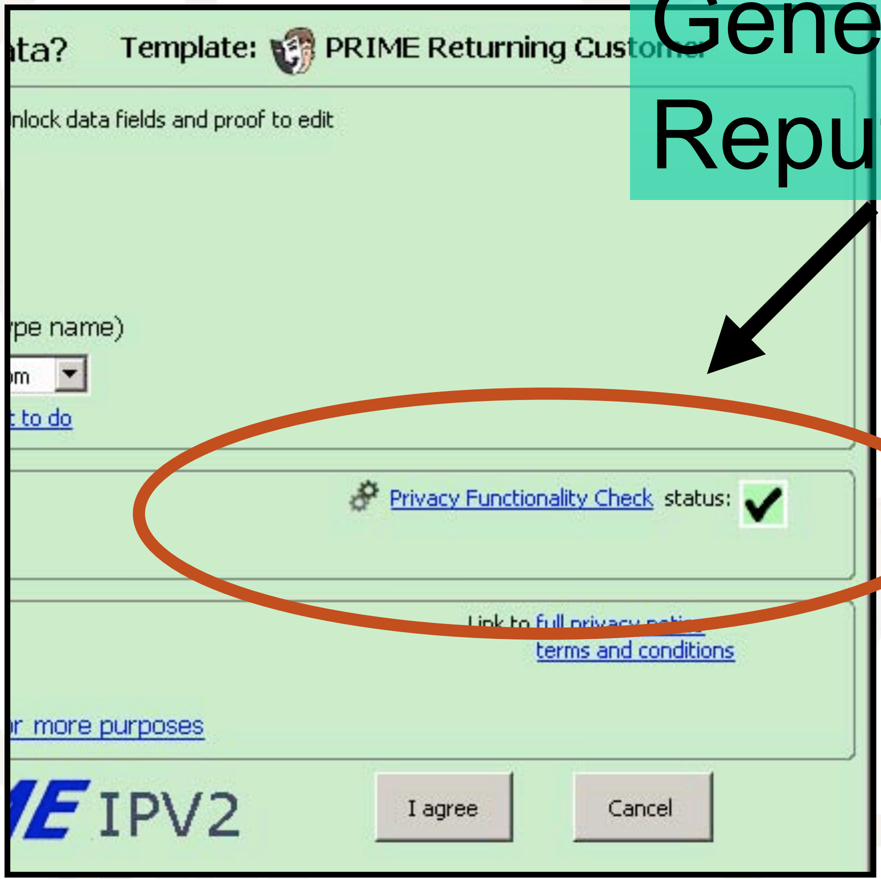
HOW TO REACH US

For the full privacy notice or for access or correction, contact:
•Privacy Department
Euro Company
**************************
- Call 00 *****************
- Or go to the Privacy notice on our website at euro.com

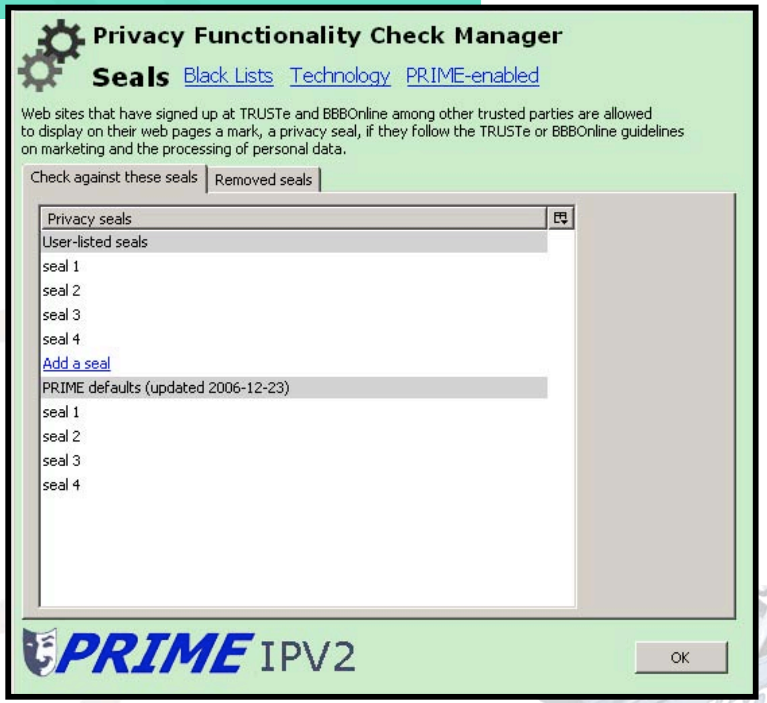
*From Annex to Oppion 100 of Art. 29 Working Party*

# Consent II: Reputation Mechanisms

Generic Reputation Area



ta?
Template: PRIME Returning Customer
nlock data fields and proof to edit
pe name)
m
to do
Privacy Functionality Check status: ✓
Link to full privacy policy
terms and conditions
r more purposes
IE IPV2
I agree
Cancel



**Privacy Functionality Check Manager**

**Seals** Black Lists Technology PRIME-enabled

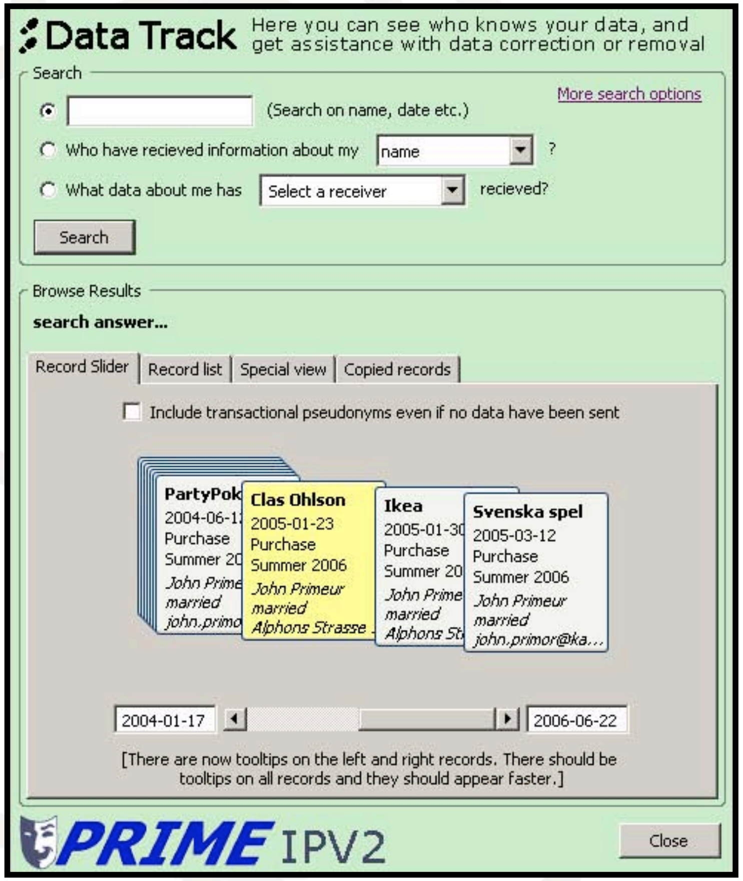
Web sites that have signed up at TRUSTe and BBBOnline among other trusted parties are allowed to display on their web pages a mark, a privacy seal, if they follow the TRUSTe or BBBOnline guidelines on marketing and the processing of personal data.

Privacy seals

User-listed seals
- seal 1
- seal 2
- seal 3
- seal 4
- Add a seal

PRIME defaults (updated 2006-12-23)
- seal 1
- seal 2
- seal 3
- seal 4

# Right to Access and Trasperancy: Data Track



Data Track Here you can see who knows your data, and get assistance with data correction or removal

Search

More search options

● (Search on name, date etc.)

○ Who have recieved information about my name ?

○ What data about me has Select a receiver recieved?

Browse Results

**search answer...**

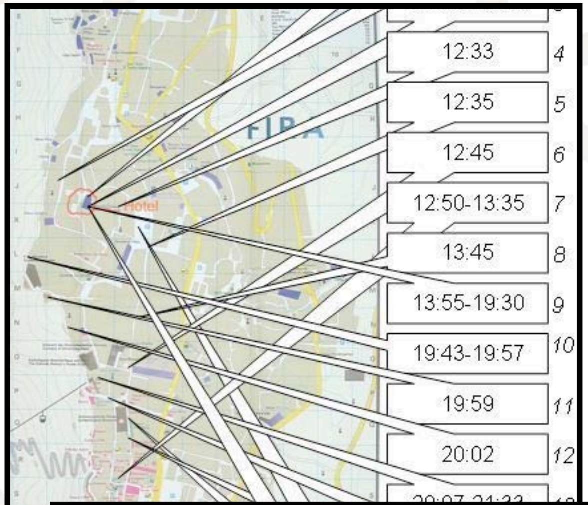
□ Include transactional pseudonyms even if no data have been sent

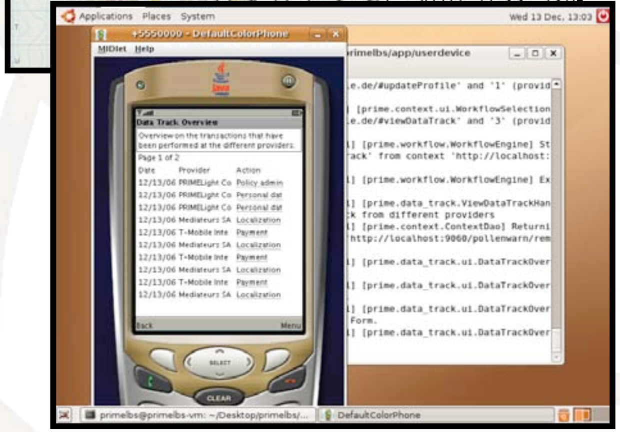
| PartyPok | Clas Ohlson | Ikea | Svenska spel |
|---|---|---|---|
| 2004-06-1 | 2005-01-23 | 2005-01-30 | 2005-03-12 |
| Purchase | Purchase | Purchase | Purchase |
| Summer 20 | Summer 2006 | Summer 20 | Summer 2006 |
| *John Prime* | *John Primeur* | *John Prime* | *John Primeur* |
| *married* | *married* | *married* | *married* |
| *john.primo* | *Alphons Strasse* | *Alphons St* | *john.primor@ka...* |

2004-01-17 2006-06-22

[There are now tooltips on the left and right records. There should be tooltips on all records and they should appear faster.]

# Prototype:
# Location Based Systems




Applications Places System
Wed 13 Dec, 13:03
+5550000 - DefaultColorPhone
MIDlet Help
rimelbs/app/userdevice
SELECT
CLEAR
Back
Menu
primelbs@primelbs-vm: ~/Desktop/primelbs/...
DefaultColorPhone

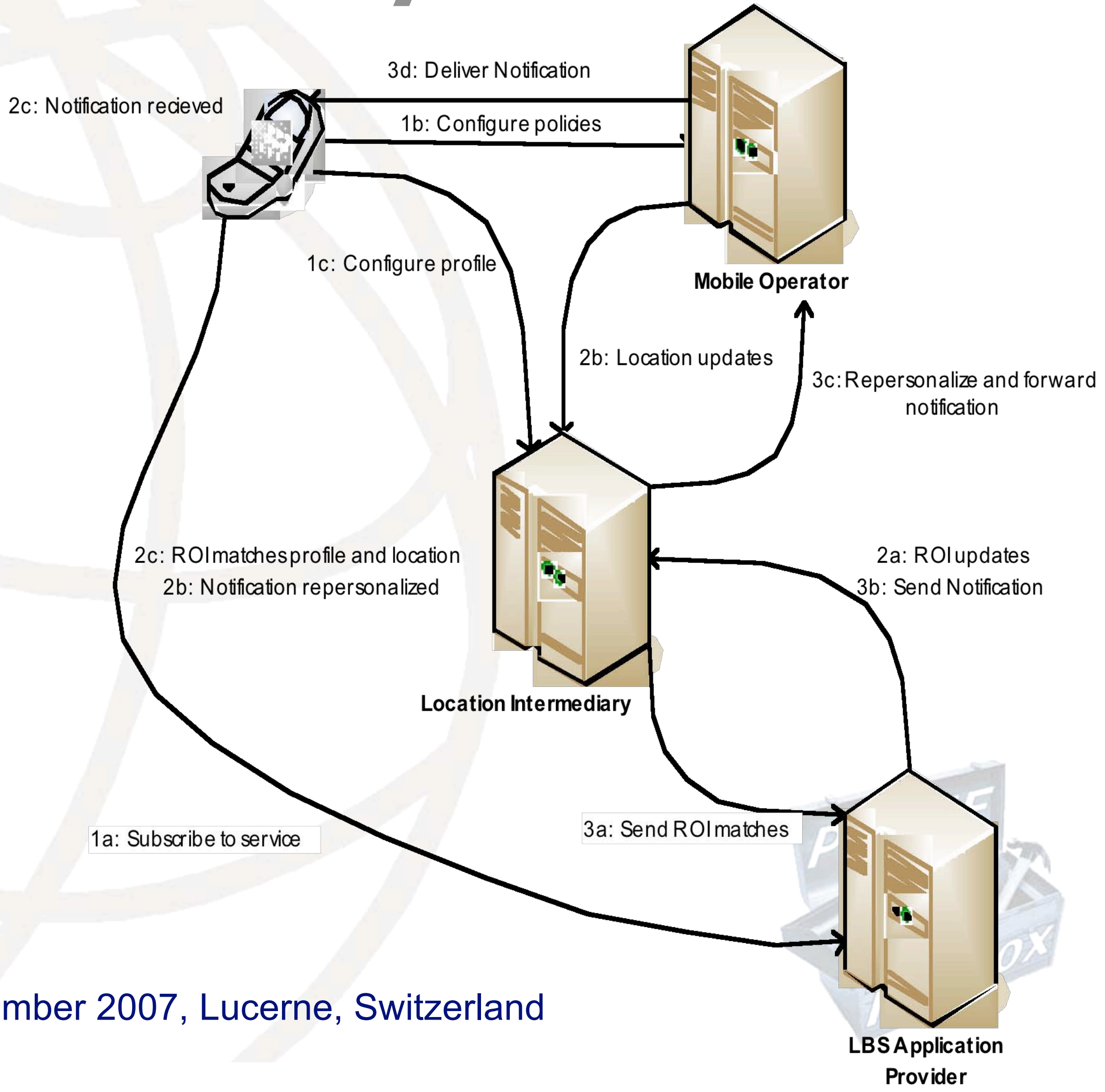
**Data Track Overview**

Overview on the transactions that have been performed at the different providers.

Page 1 of 2

| Date | Provider | Action |
|---|---|---|
| 12/13/06 | PRIMELight Co | Policy admin |
| 12/13/06 | PRIMELight Co | Personal dat |
| 12/13/06 | PRIMELight Co | Personal dat |
| 12/13/06 | Mediateurs SA | Localization |
| 12/13/06 | T-Mobile Inte | Payment |
| 12/13/06 | Mediateurs SA | Localization |
| 12/13/06 | T-Mobile Inte | Payment |
| 12/13/06 | Mediateurs SA | Localization |
| 12/13/06 | T-Mobile Inte | Payment |
| 12/13/06 | Mediateurs SA | Localization |

```
.e.de/#updateProfile' and '1' (provid

] [prime.context.ui.WorkflowSelection
.e.de/#viewDataTrack' and '3' (provid

1] [prime.workflow.WorkflowEngine] St
rack' from context 'http://localhost:

1] [prime.workflow.WorkflowEngine] Ex

1] [prime.data_track.ViewDataTrackHan
:k from different providers
1] [prime.context.ContextDao] Returni
'http://localhost:9060/pollenwarn/rem

1] [prime.data_track.ui.DataTrackOver

1] [prime.data_track.ui.DataTrackOver

1] [prime.data_track.ui.DataTrackOver
 Form.
1] [prime.data_track.ui.DataTrackOver
```



PRIME

30 September 2007, Lucerne, Switzerland

# Thank you for your attention!

Jan Schallaböck
LD103@datenschutzzentrum.de

**Regards and copyright attribution go to:**

- **Jan Camenisch and Dieter Sommer, IBM**
- **The Electronic Frontier Foundation**
- **Article 29 Working Party**
- **Kim Cameron, Microsoft**
- **ISO**

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