Privacy-Enhancing Technologies (PETs)

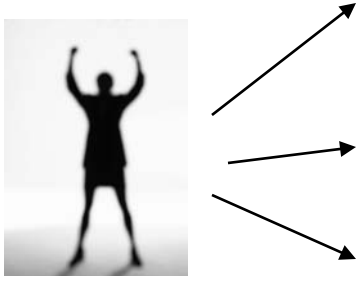
Simone Fischer-Hübner

Stockholm, 26th October 2010

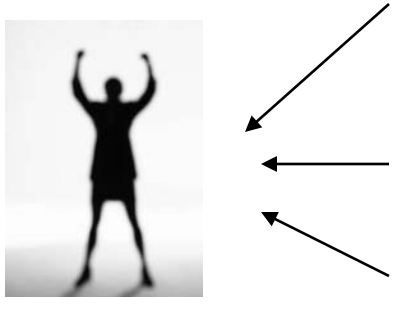
I. Introduction to Privacy & PETs

Privacy Dimensions

- Informational self-determination



- Spatial privacy



Basic Privacy principles
(implemented in EU-Directive 95/46/EC)

- Legitimisation by **law, informed consent** (Art. 7 EU Directive)
- **Data minimisation** (Art. 6 I c, Art. 7)
- **Purpose specification** and **purpose binding** (Art. 6 I b)
  - ”Non-sensitive” data do not exist !
- **Transparency**, rights of data subjects

Classifications of PETs

1. PETs for minimizing / avoiding personal data
(-> Art. 6 I c., e. EU Directive 95/46/EC)
(providing Anonymity, Pseudonymity, Unobservability, Unlinkability)

- At communication level:
  - Mix nets, Onion Routing, TOR
  - DC nets
  - Crowds,...
- At application level:
  - Anonymous Ecash
  - Private Information Retrieval
  - Anonymous Credentials,...

2. PETs for the safeguarding of lawful processing
(-> Art. 17 EU Directive 95/46/EC)

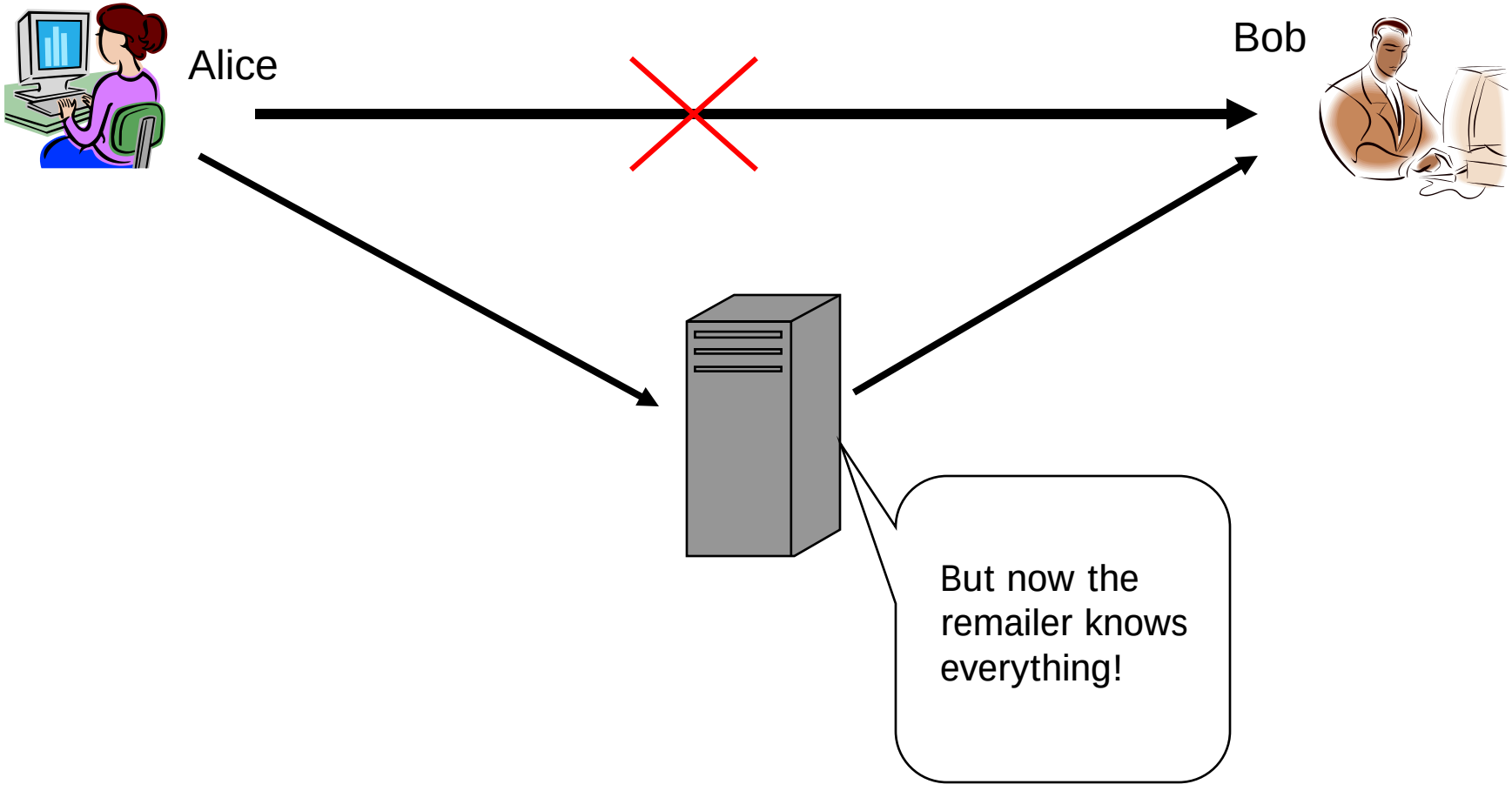
- P3P, Privacy policy languages
- Encryption,...

3. Combination of 1 & 2

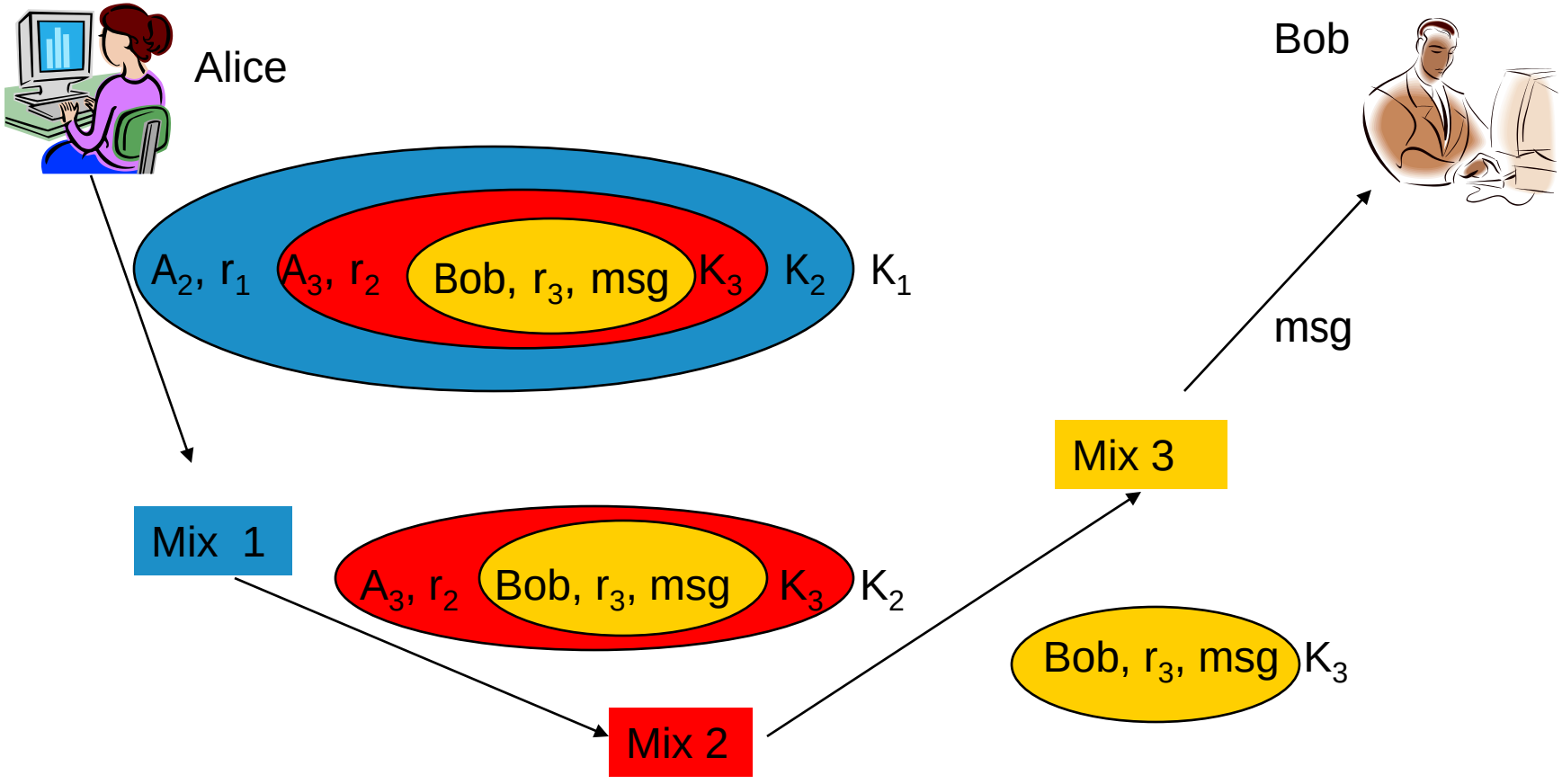
- Privacy-enhancing Identity Management (PRIME, PrimeLife)

Privacy and Identity Management for Europe

II. Anonymous Communication Technologies

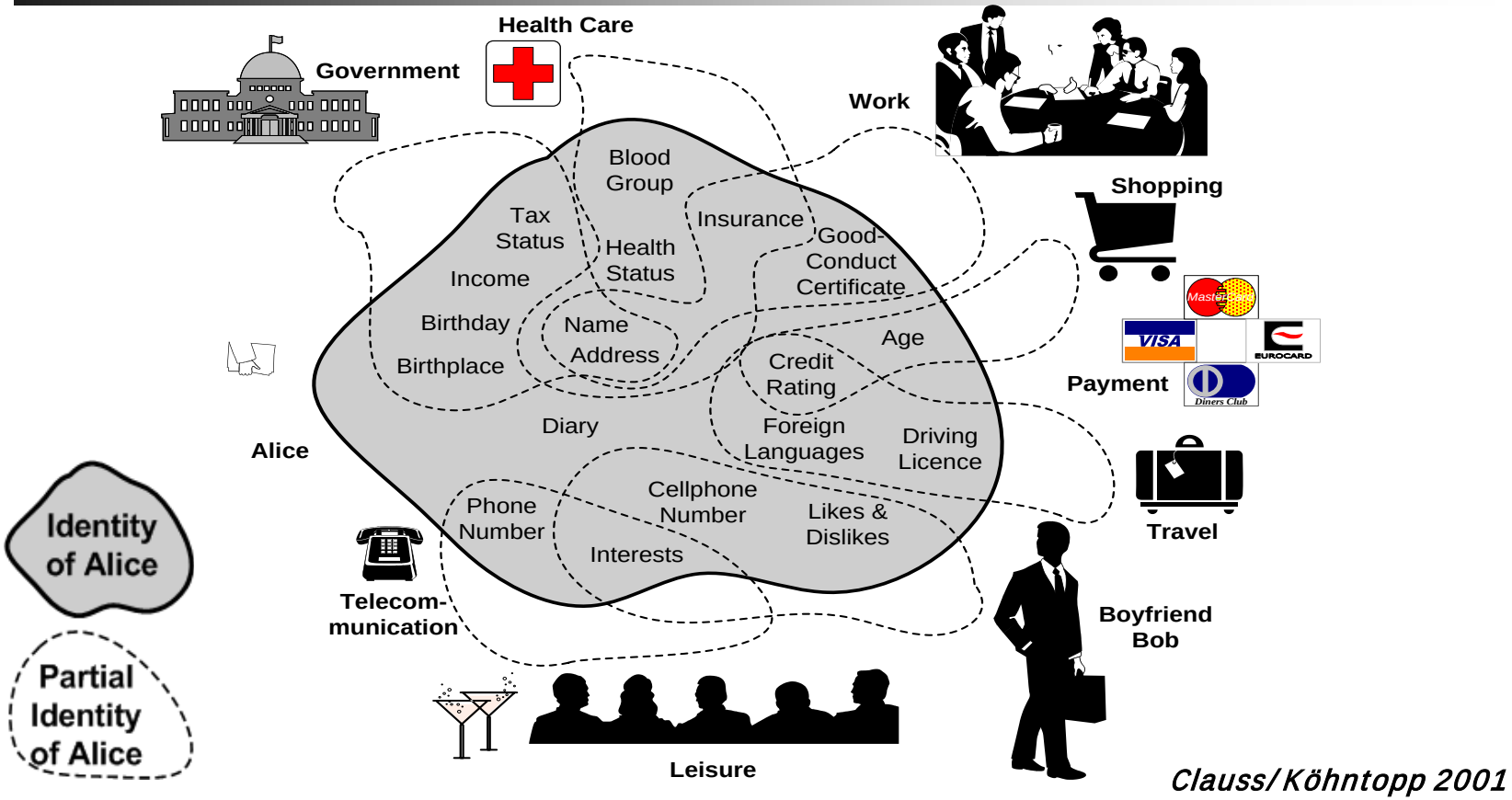


Mix-nets (Chaum, 1981)



K_i: public key of Mix_i, r_i: random number, A_i: address of Mix_i

III. Privacy-enhancing Identity Management (IDM)



Audience segegration: User reveal different (partial) identities based on their current roles/relationships

Viability of privacy-enhancing IDM has been demonstrated by PRIME

Integrated approach providing:

- Data Minimisation
  - Anonymous communication, anonymous credentials, privacy-enabling authorisation model
- Assurance & Life Cycle Management
  - Assurance control, privacy & trust policy negotiation & enforcement (sticky policies), obligation management
- Transparency
  - Data track,...

PRIME
Privacy and Identity Management for Europe

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

PRIME/PrimeLife Architecture – Key Elements

1 Data Minimisation

2 Assurances & Data Life Cycle Management

The following slides were kindly provided by Dieter Sommer/IBM Research

1 Data Minimisation

How service providers can authorise users while users retain their privacy

Traditional Model

Request of service

Please log in!

Username = jane.doe

Password

Ok, the requestor is Jane Doe
Address = Paradeplatz, 8001 Zurich, Switzerland
Birth date = 01 June 1979
Email = Jane.doe@mail-provider-xyz.com
Credit card details = (VISA, 1234 5678 9012, …)
And so on…

Other profiling data: Detailed interest profiles, browsing behavior, detailed mouse movement profiles, complete history of interactions over the last 3 years, derived data and much more

External linkable data: Potentially everything that is linkable to Jane Doe's identity

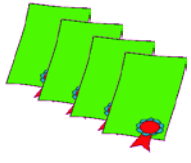
PRIME/PrimeLife Model

PRIME Console

PRIME Middleware

Request of service

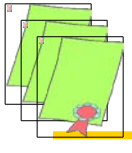
Please provide us with either of the following
- Your pseudonym with us
- A valid service subscription
- A valid service subscription and

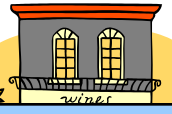


Pseudonym = X768932…86
Proof = 5634..u758

Statement = Subscription.Type
Proof = 7862…8970

Statement = Subscription.Type
Proof = 7658…5634





Ok, the … **X768932…86**

Ok, the … has a **valid**

Ok, the requestor has a **valid subscription**. That means, she has paid for the service and can access it.

The requestor has provided relevant certified attributes to enable service customization.

In between the extremes!

Data minimisation

isn’t the answer to everything

[there are many scenarios where identifying data are just required]

2 Assurances & Data Life Cycle Management

How users establish trust in service providers and
how service providers enforce their promises for data handling

nal Model

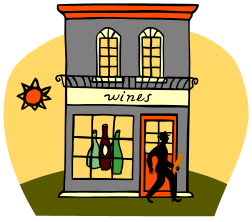
Well, I don't know anything about this service provider…

There's not much choice than just providing the data…

Let's hope that these are not those bad privacy-infringing guys one reads about in the news every other day…

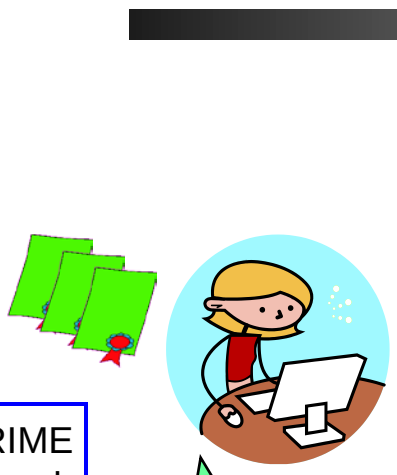
eate an account

Please provide
Name, street, zip code & city, country, birth date, email address, credit card details, personal preferences on X, …



Here's what you have requested:
Jane Doe, Paradeplatz, 8001 Zurich, Switzerland, 1978-06-01
Jane.doe@mail-provider-xyz.com, VISA, 1234 5678 9012, …

PRIME/PrimeLife Model



PRIME Console

PRIME Midd

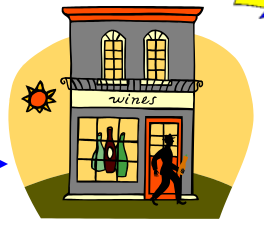
This service provider seems to be ok!
[Trust evaluation:
They have appropriate seals, are not blacklisted and provide PRIME functionality…]

The data handling policy is acceptable (meeting my preferences)

White/Blacklist Provider

White/Blacklist query

Ok



Privacy Seal

Request of **service**

Data request; data handling proposal
Provide me with: name, address, birth date, email address, credit card details, personal preferences on X, …

Evaluation of request

Request of **trust & assurance data and evidence**

We can offer the following:
- EuroPriSe privacy seal
- We are running a PRIME/PrimeLife-enabled system including data minimization support and privacy obligation management. We have encrypted data storage …
- …

Data handling policy*
Here is what you have requested:
Jane Doe, Paradeplatz, 8001 Zurich, Switzerland, 1978-06-01
Jane.doe@mail-provider-xyz.com,
(VISA, 1234 5678 9012), Y, …

Negotiation

Sticky policy

Customer Data

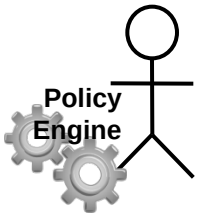
Structure of PrimeLife Policy Language (Neven et al.)

Personal Data (PD)

Non-certified

Certified: cards

Data Subject



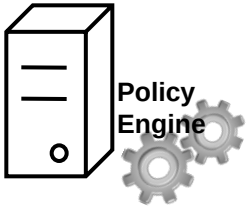
request resource

request personal data

personal data

resource

Data Controller



Resources

Non-personal content, services,…

Collected personal data

SAML

Specific Policy:

over specific personal data (e.g. birth date)

- **Access control policy (ACP):**
  who can access (e.g. PrivacySeal silver)
- **Data handling preferences (DHPrefs):**
  how is to be treated when revealed
  - **Authorizations** (e.g. marketing purposes, forwarded to PrivacySeal gold)
  - **Obligations** (e.g. delete after ≤2y)

Generic Preferences:

DHPrefs over implicitly revealed personal data (e.g. IP address, cookies,…)

- **Authorizations** (e.g. admin purposes)
- **Obligations** (e.g. delete after ≤2y)

XACML

Specific Policy:

over specific resource (e.g. BuyService)

- **Access control policy (ACP):**
  who can access
  - cards to possess (e.g. ID card)
  - personal data to reveal (e.g. nationality)
  - conditions to satisfy (e.g. age>18)
- **Data handling policy (DHP):**
  how revealed personal data will be treated
  - **Authorizations** (e.g. marketing purposes)
  - **Obligations** (e.g. delete after 1y)

Generic Policy:

DHP over implicitly revealed personal data (e.g. IP address, cookies,…)

- **Authorizations** (e.g. admin purposes)
- **Obligations** (e.g. delete after 1y)

PrimeLife

http://www.primelife.eu/

Started: 01 March 2008, **Ends**: June 2011, **Total EC Funding**: 10.200,000 €

- Bringing Sustainable Privacy and Identity Management to Future Networks and Services
  - Fundamentally understanding privacy-enhancing identity management ‘for life’
  - Bringing Privacy to the future web/social networks
  - Research on Policies, HCI, Infrastructures
- Beyond data minimization:
  - Address data-intensive scenarios and user-generated content (Web 2.0, virtual communities such as Friendster, SecondLife)
- Make privacy-enhancing identity management widely available:
  - Infrastructures, Open Source, and Standards
  - Cooperation with other Projects (Master, TAS3, SWIFT,...),
  - Education (summer schools, ...)

Questions ?

http://www.cs.kau.se/~simone/