Wireless Sensor Networks and Privacy

UbiSec & Sens

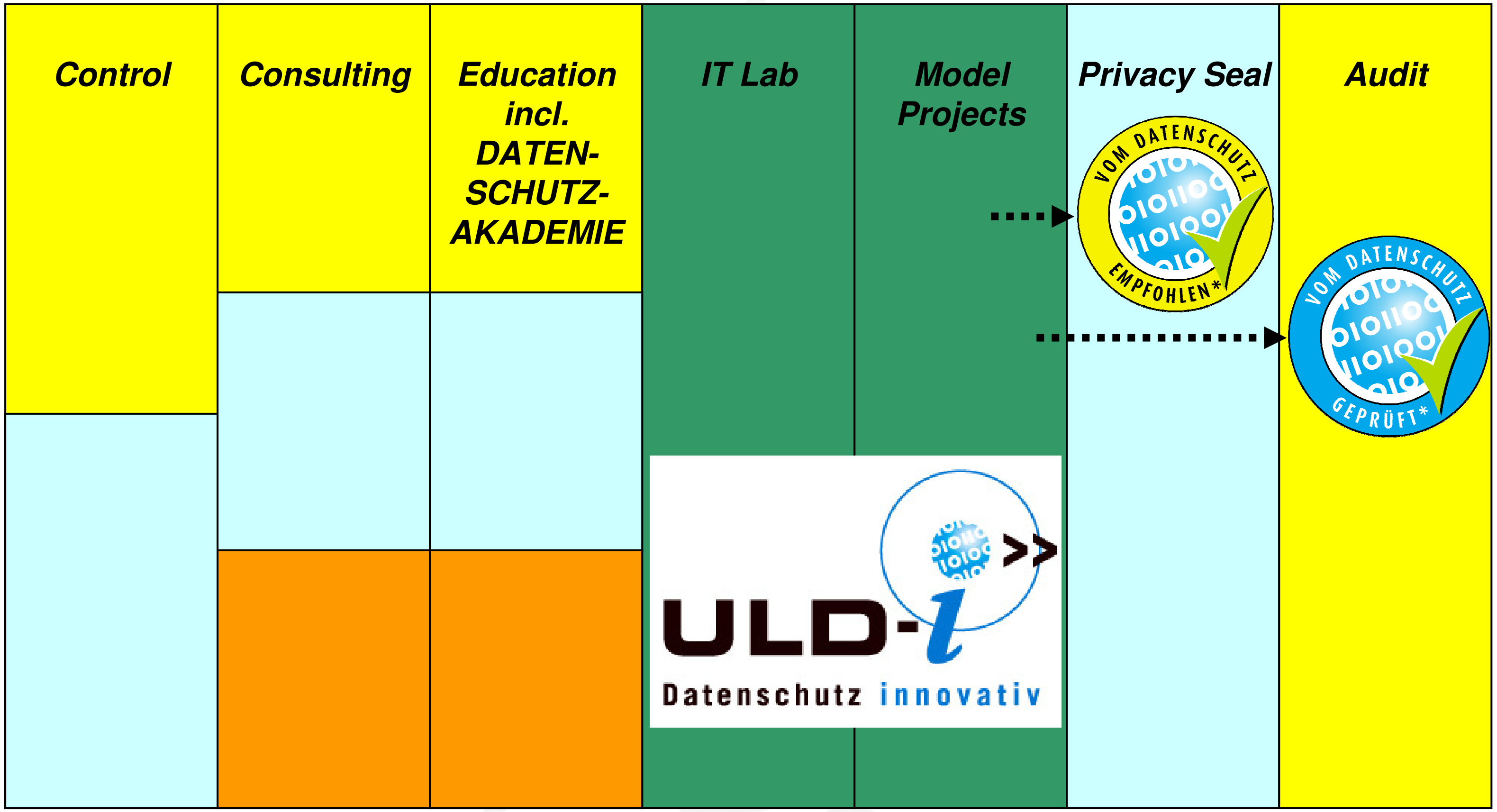
Workshop Aachen 7.2.2008

Agenda

- ULD – who we are and what we do
- Privacy and Data Protection – concept and terminology
- Privacy and Security technologies – a dilemma?
- Wireless Sensor Networks – privacy issues
  - WSN General Issues
  - UbiSec & Sens Applications

ULD – who we are and what we do

The Seven Pillars of ULD



Control

Consulting

Education incl. DATENSCHUTZ-AKADEMIE

IT Lab

Model Projects

Privacy Seal

Audit

Primary Addressees:

🟨 Administration

🟦 Business

🟧 Citizens

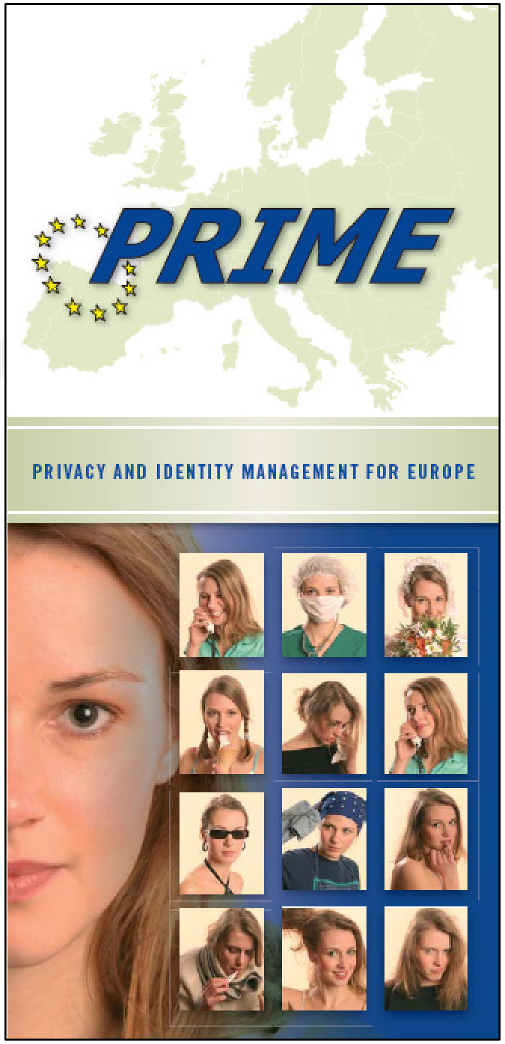
🟩 Business, R&D, Administration

PRIME
Privacy and Identity Management for Europe

Identity Management

PRIME – Privacy and Identity Management for Europe

- Objective: Development of a privacy-enhancing IMS
- 20 co-operation partners from business and academia
- Budget: ~16 Mio €
- Duration: Mar 2004 – May 2008
- EU Funding:
  6th Framework IST
- www.prime-project.eu


PRIME

PRIVACY AND IDENTITY MANAGEMENT FOR EUROPE

Identity Management

FIDIS – Future of Identity in the Information Society
(Network of Excellence)

- 24 co-operation partners mainly from academia
- Budget: ~5.5 Mio €
- Duration: Apr 2004 – Mar 2009
- EU Funding:
  6th Framework IST
- www.fidis.net

PrimeLife

- Objective: Bringing sustainable privacy and identity management to future networks and services
- 14 co-operation partners from business and academia
- Budget: ~10 Mio €
- Duration: Mar 2008 – Feb 2010
- EU Funding:
  7th Framework IST

European Privacy Seal

EuroPriSe – European Privacy Certification Scheme

introducing a European Privacy Seal for IT-products and services that have proven privacy compliance in a two-step certification procedure

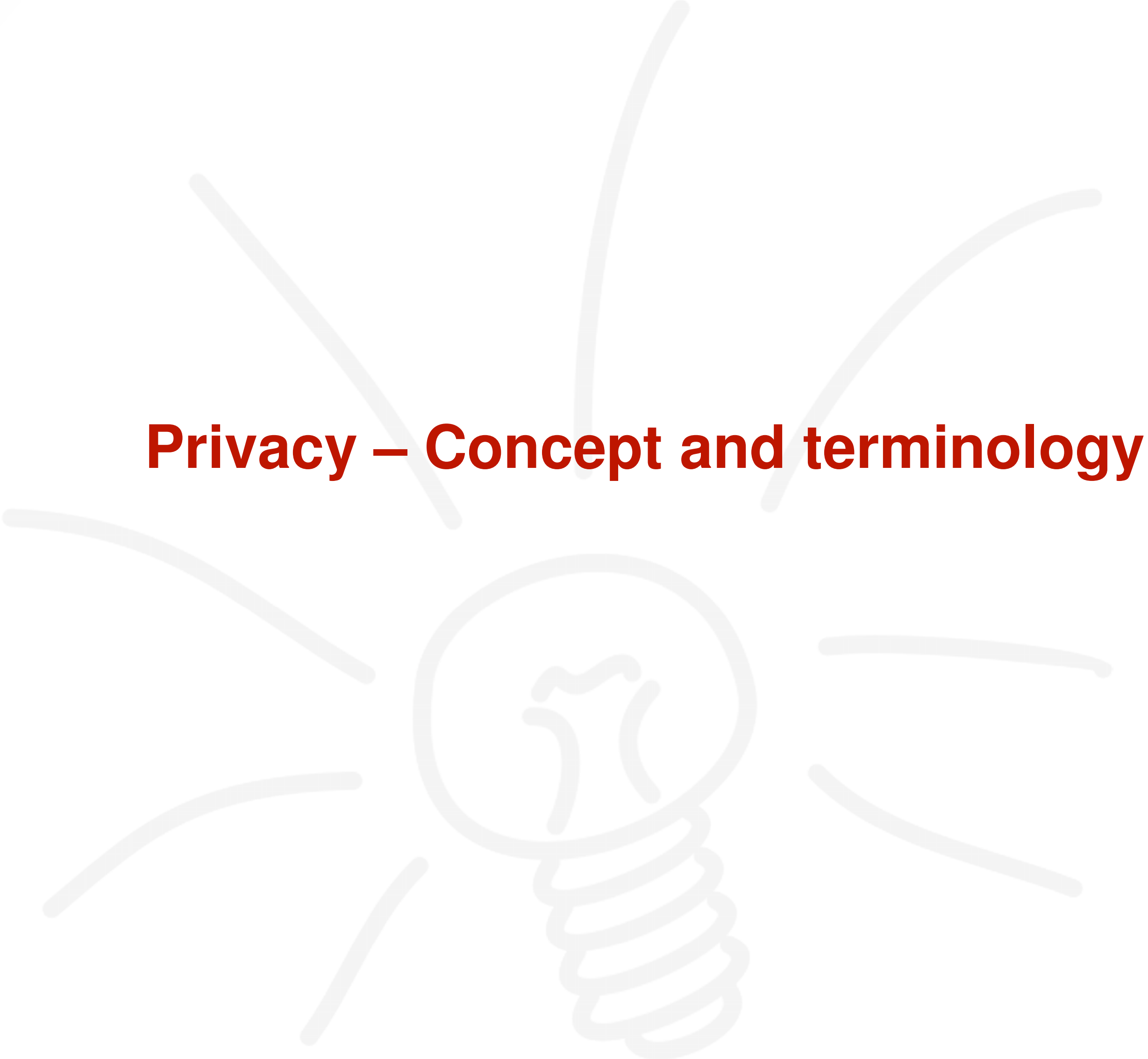
- Co-operation partners: 9 partners from 8 EU countries
- Budget: ~1,2 Mio €
- Duration: June 2007 – November 2008
- Funding: eTAN programme

Project on Security Research and Technology

PRISE – Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted criteria for European Security Technology Research

- Co-operation partners: Austrian Academy of Science, Danish Board of Technology, Norwegian Board of Technology
- Budget: ~800,000 €
- Duration: Feb 2006 – May 2008
- Funding: PASR (Preparatory Action on the enhancement of the European industrial potential in the field of Security research)

Privacy – Concept and terminology



Privacy and Data Protection – Concept and Terminology

Data Protection:

- Harmonized by EU law: Directives 1995/46/EC and 2002/58/EC
- protection against unlawful processing of personal data
- **personal data**: any information relating to an identified or identifiable person
- Principles:

  Legitimacy

  Purpose Binding

  Transparency

  Proportionality (necessity?)

  Data security (overlap with IT-Security)

  Quality of Data

  Control: supervision by DP Commissioner, certification of products and processes

Privacy and Data Protection – Concept and Terminology

Privacy:

- Wider concept than data protection
- Protection of private sphere:

  bodily private sphere (terrahertz scanning, body temperature, behaviour etc)

  home,

  privileged conversations e.g. with spouse, priest, lawyer

- protects undisturbed development and exercise of individual life style

- Privacy is a fundamental human right for democracy: it guarantees other fundamental rights like right to assemble, freedom of association, freedom of expression

Privacy and Data Protection – Concept and Terminology

Main questions:

- who is
- processing
- which data
- for which purpose and
- under which law / legal basis?
- How can I control this?
- Is there room for “control” in homeland security applications?

Mapping requirement:

- data controller?
- processing
- types of data and data flows

transparency

- Definition of purpose prior to collection and processing
- Legitimacy
- User control as a Privacy Enhancing Technology (PET)
- Is there room for “control” in homeland security applications?

Privacy and Security Technologies – a dilemma?

Privacy and Security Technologies

Privacy aims at:

- unlinkability
- transparency
- control by the user
- data minimization

Security technologies aim at:

- detecting suspicious or punishable behaviour
- linking information to individual
- sometimes: covert data collection and processing
- limited control by suspect
- data retention, data fusion, data analysis

Privacy and Security Technologies

- Exemption in Art. 13 of Directive 1995/46/EC:

  "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for [in this directive] when such a restriction constitutes a necessary measures to safeguard

  national security

  defence

  public security

  the prevention, investigation, detection, and prosecution of criminal offences […]."

Wireless Sensor Networks – Privacy Issues

Wireless Sensor Networks – Privacy Issues

General privacy issues with wireless sensor networks:

Feature	Mapping data processing step	Problem	Relevant privacy principles
Sensors	Data Collection	unobserved, remote data collection, tracking & profiling	transparency, necessity, legitimacy
Communication	Data Transmission	unobserved by data subject	transparency, data security, legitimacy, purpose binding
Data processing	Data use	data processing in backend systems; function creep	legitimacy, purpose binding, transparency
Data Storage	Data Storage	retention period, access control, linking of data from different sources	legitimacy, purpose binding, data security
Analysis and Decision Making	Analysis of data	linking of data from different sources	transparency, proportionality, legitimacy

Wireless Sensor Networks – Privacy Issues
UbiSec & Sens Applications

- Do sensors collect **data which can be linked to an individual?**

  Application I Agriculture: no

  Application II Road Service: yes → system calculates road status according to current **location of driver**; if connected to fixed network and payment required for service: identification of user intended?!

  Application III Homeland Security: if sensors measure only chemical or bio-chemical value of surroundings and not e.g. body heat: no; if **optical or acoustic sensors** are used: usually yes

Wireless Sensor Networks – Privacy Issues
UbiSec & Sens Applications

- **What types of data are collected?**

  Personal Data and special categories of personal data?

  special categories: communication traffic data, location data, biometric data

  sensitive data (special requirements): personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life

Application II Road Service: location of driver, possibly also speed and payment data

Application III Homeland Security: chemical values, acoustic data (conversations)?, optical data (movement, face impression)?

Wireless Sensor Networks – Privacy Issues
UbiSec & Sens Applications

- If special categories of data are collected, are they **separated** from other personal data?
- If sensitive data is processed are there safeguards for higher protection of this type of data in place?
- What is the **purpose** for which the technology will be used and data be processed?
- Does the WSN collect and process **not more data** than the minimum required for the purpose for which it is collected?
- Can the WSN be used for **other purposes** than the initially intended purpose?

  Self-calibrating? Customization substantial effort?
- Does the WSN allow for or aim at **transmission** of collected data **to third party**, e.g. by means of an interface?
- Is a **unique identifier** processed?
- Are **sources** of data recorded?

Wireless Sensor Networks – Privacy Issues
UbiSec & Sens Applications

- Are **logging procedures** implemented wrt data collection (time stamp), data access, data transmission, data use?
- Is personal data pseudomized?
- Is the purpose for which the data was collected recorded and "linked" with the data?
- Does the WSN allow allocation of **different access rights** for different sets of data which were collected for different purposes?
- What **checks** are implemented to ensure that further processing is not incompatible with the original purpose?
- Does the WSN comprise an **automated individual decision** (Art. 15 of 45/95/EC)? [no person shall be subject to a decision which produces legal effects concerning him or significantly affects him and which is solely based on an automated processing of data intended to evaluate certain personal aspects relating to him, such as […] his conduct…]

Wireless Sensor Networks – Privacy Issues UbiSec & Sens Applications

- Is it possible to set and later change automated **retention periods** / data deletion?
- Is data **reviewed** for whether it is still necessary for the purpose for which it was collected?
- Does use of the WSN affect an **undefined number of individuals** regardless of whether the individual is suspected of any wrongdoing?
- Is data collected, processed or stored **secretly** / unobserved or are individuals being made aware of their personal data being processed?
- Does the WSN allow for **rectification** of incorrect data?
- Does the WSN enable checking the **accuracy** of personal data with the **data subject concerned**?
- Are procedures in place to detect **breaches of security**?

Wireless Sensor Networks – Privacy Issues
UbiSec & Sens Applications

- Is **encryption** used to protect personal data? How are keys handled?
- How is **unauthorized copying** of personal data prevented?
- Does the WSN comprise mechanisms to prevent **accidental loss** of data?
- Does the WSN allow for destruction of data no longer needed?

Thank you for your attention

Maren Raguse
LD64@datenschutzzentrum.de
www.datenschutzzentrum.de
+49-431/988-1284