ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Personal Privacy in Ubiquitous Computing

Tools and System Support

Marc Langheinrich

Ubiquitous Computing und Privacy

Disappearing Computer Troubadour Projekt (10/02 - 05/03)

- **Problem anderer Leute**
  - „For [my colleague] it is more appropriate to think about privacy issues. It's **not really the case in my case**"
- **Privacy ist primär ein Sicherheitsproblem**
  - „All you need is **really good firewalls**"
- **Nur eine Frage der Selbstregulierung**
  - „ It's maybe about letting them find their **own ways of cheating**"
- **Inkompatibel mit Ubiquitous Computing Forschung**
  - „I think you can't think of privacy... **it's impossible**, because if I do it, I have troubles with finding [a] Ubicomp future"

Vorurteile?

- **Problem anderer Leute**
  - „For [my colleague] it is more appropriate to think about privacy issues. It's **not really the case in my case**"
- **Privacy ist primär ein Sicherheitsproblem**
  - „All you need is **really good firewalls**"
- **Nur eine Frage der Selbstregulierung**
  - „ It's maybe about letting them find their **own ways of cheating**"
- **Inkompatibel mit Ubiquitous Computing Forschung**
  - „I think you can't think of privacy... **it's impossible**, because if I do it, I have troubles with finding [a] Ubicomp future"

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Personal Privacy in Ubiquitous Computing

Tools and System Support

Marc Langheinrich

Beiträge der Dissertation

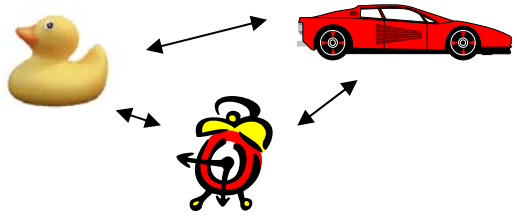
- **Analyse**
  - Was ist Privatheit/Privacy?
  - Wie wird diese von Ubiquitous Computing beeinflusst?
- **Technische Datenschutz-Infrastruktur (PawS)**
  - Privacy Beacons
  - Privacy Proxies
  - Privacy-Aware Database
- **Praxisbeispiel**
  - Privatheit und Funketiketten (RFID)

Beiträge der Dissertation

- **Analyse**
  - Was ist Privatheit/Privacy?
  - Wie wird diese von Ubiquitous Computing beeinflusst?
- **Technische Datenschutz-Infrastruktur (PawS)**
  - Privacy Beacons
  - Privacy Proxies
  - Privacy-Aware Database
- **Praxisbeispiel**
  - Privatheit und Funketiketten (RFID)

Ubiquitous Computing –
Implikationen für Privacy/Privatheit

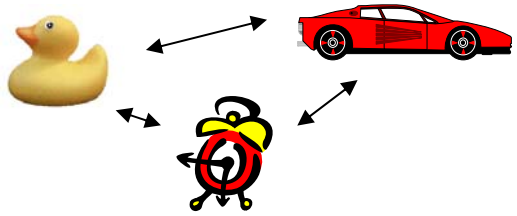
- **Datenerhebung**
  - Umfang (Allgegenwärtig, jederzeit)
  - Art (Unauffällig, unsichtbar)
  - Grund („Auf Vorrat“)
- **Datenarten**
  - Beobachtungsdaten statt Faktenwissen
- **Datenzugriff**
  - Das „Internet der Dinge“



Ubiquitous Computing –
Imp

Privacy ist nicht das Problem anderer Leute –
Privacy ist ein Kernproblem ubiquitärer Umgebungen

- **Datenerhebung**
  - Umfang (Allgegenwärtig, jederzeit)
  - Art (Unauffällig, unsichtbar)
  - Grund („Auf Vorrat“)
- **Datenarten**
  - Beobachtungsdaten statt Faktenwissen
- **Datenzugriff**
  - Das „Internet der Dinge“



Was ist „Privacy“?

- **Warum „Privacy“?**
  - Ungestörtheit

Louis D. Brandeis, 1856 – 1941

„The right to be let alone“ (1890)

Was ist „Privacy“?

- **Warum „Privacy“?**
  - Ungestörtheit
  - Intimität

Erving M. Goffman, 1922 – 1982

The Presentation of Self in Everyday Life (1959)

Was ist „Privacy“?

- **Warum „Privacy“?**
  - Ungestörtheit
  - Intimität
  - Entscheidungsfreiheit

Beate Rössler

Sicherung der Interpretationshoheit über mein Leben (2001)

Was ist „Privacy“?

- **Warum „Privacy“?**
  - Ungestörtheit
  - Intimität
  - Entscheidungsfreiheit
- **„Privacy“ Begrifflichkeit im Deutschen**
  - Privatheit, Privatsphäre
  - Datenschutz
  - Informationelle Selbstbestimmung

Was ist „Privacy“?

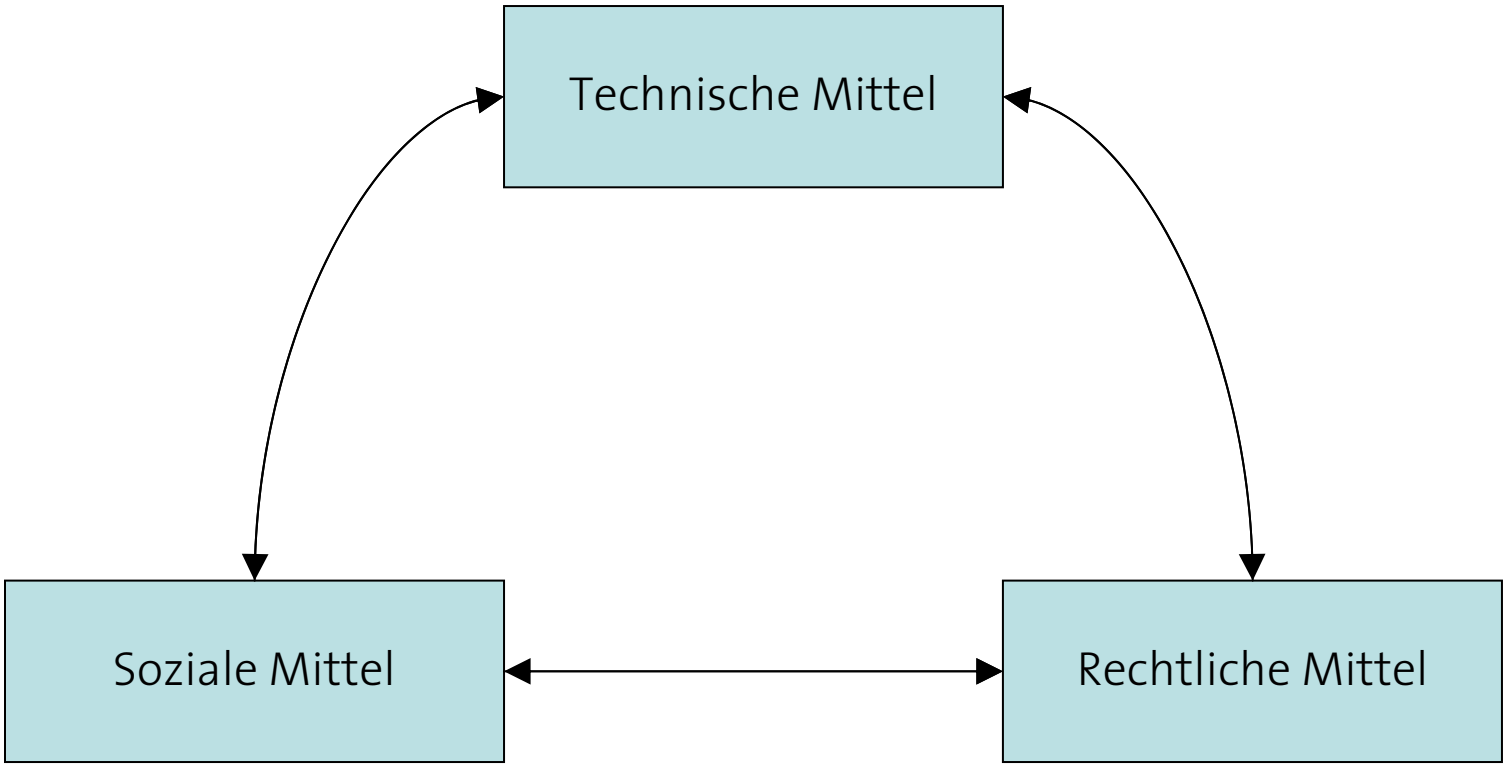
Privacy ist nicht nur ein Sicherheitsproblem – Datenaustausch und Übersicht sind wichtig!

- **Warum „Privacy“?**
  - Ungestörtheit
  - Intimität
  - Entscheidungsfreiheit
- **„Privacy“ Begrifflichkeit im Deutschen**
  - Privatheit, Privatsphäre
  - Datenschutz
  - Informationelle Selbstbestimmung

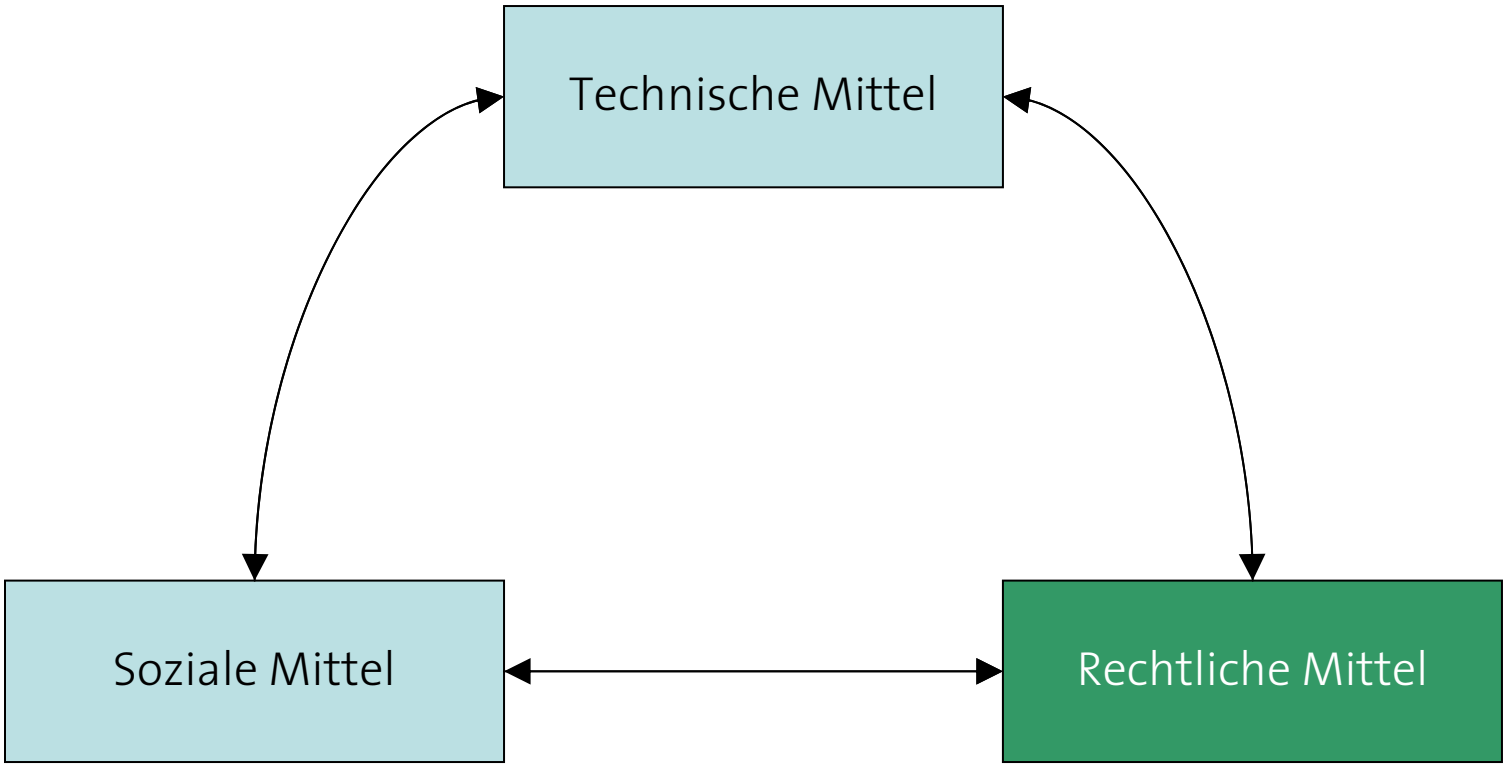
Beiträge der Dissertation

- **Analyse**
  - Was ist Privatheit/Privacy?
  - Wie wird diese von Ubiquitous Computing beeinflusst?
- **Technische Datenschutz-Infrastruktur (PawS)**
  - Privacy Beacons
  - Privacy Proxies
  - Privacy-Aware Database
- **Praxisbeispiel**
  - Privatheit und Funketiketten (RFID)

Lösungsraum



Lösungsraum



Grundlage: Fair Information Principles (FIP)

- **Aufgestellt von der OECD, 1980**
  - "Organisation für wirtschaftl. Zusammenarbeit u. Entwicklung"
  - Freiwillige Richtlinien für Mitglieder
  - Erleichterung des grenzüberschreitenden Informationsflusses
- **Fünf Prinzipien (vereinfacht)**
  1. Offenheit
  2. Datenzugriff und -kontrolle
  3. Datensicherheit
  4. Datensparsamkeit
  5. Einwilligung des Datensubjekts
- **Grundlage vieler Datenschutzgesetze weltweit**
  - Folgerung: Technische Lösung muss FIP unterstützen

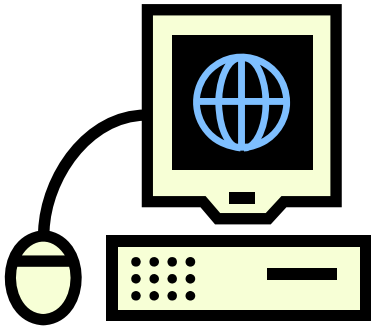
Grundlage: Fair Information Principles (FIP)

Privacy ist keine Frage der Selbstregulierung – Rechtlicher und sozialer Rahmen existieren!

- **Aufgestellt von der OECD, 1980**
  - "Organisation für wirtschaftl. Zusammenarbeit u. Entwicklung"
  - Freiwillige Richtlinien für Mitglieder
  - Erleichterung des grenzüberschreitenden Informationsflusses
- **Fünf Prinzipien (vereinfacht)**
  1. Offenheit
  2. Datenzugriff und -kontrolle
  3. Datensicherheit
  4. Datensparsamkeit
  5. Einwilligung des Datensubjekts
- **Grundlage vieler Datenschutzgesetze weltweit**
  - Folgerung: Technische Lösung muss FIP unterstützen

Technische Hilfsmittel

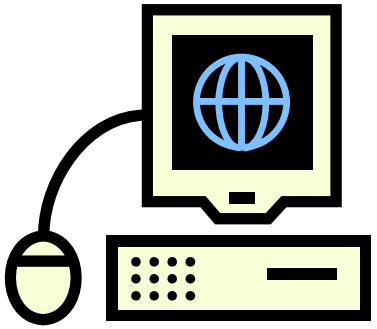
- **Privacy Enhancing Technologies (PETs)**
  - Verschlüsselung & Authentisierung
  - Anonymisierung & Pseudonymisierung
  - Zugriffskontrolle
  - Transparenz & Vertrauen



- **„Ubiquitous Computing – Ubiquitous Privacy“**
  - Überall, jederzeit, infrastrukturgestützt, automatisch, im Hintergrund, ohne Belästigung (A. Roßnagel)

Technische Hilfsmittel

- **Privacy Enhancing Technologies (PETs)**
  - Verschlüsselung & Authentisierung
  - Anonymisierung & Pseudonymisierung
  - Zugriffskontrolle
  - Transparenz & Vertrauen



- **„Ubiquitous Computing – Ubiquitous Privacy“**
  - Überall, jederzeit, infrastrukturgestützt, automatisch, im Hintergrund, ohne Belästigung (A. Roßnagel)

Grundlage: P3P

Platform for Privacy Preferences Project (W3C)

Platform for Privacy Preferences Initiative W3C®

- **Maschinenlesbare Datenschutzerklärung (Policy)**
  - Wer erhebt bzw. verarbeitet die Daten?
  - Welche Daten werden erhoben?
  - Zu welchem Zweck werden diese erhoben?
- **Basis-Datenschema**
  - Beispiel: **`user.home.postal.street`**
- **Web-Protokoll**
  - Zum Austausch zwischen Webserver und Browser

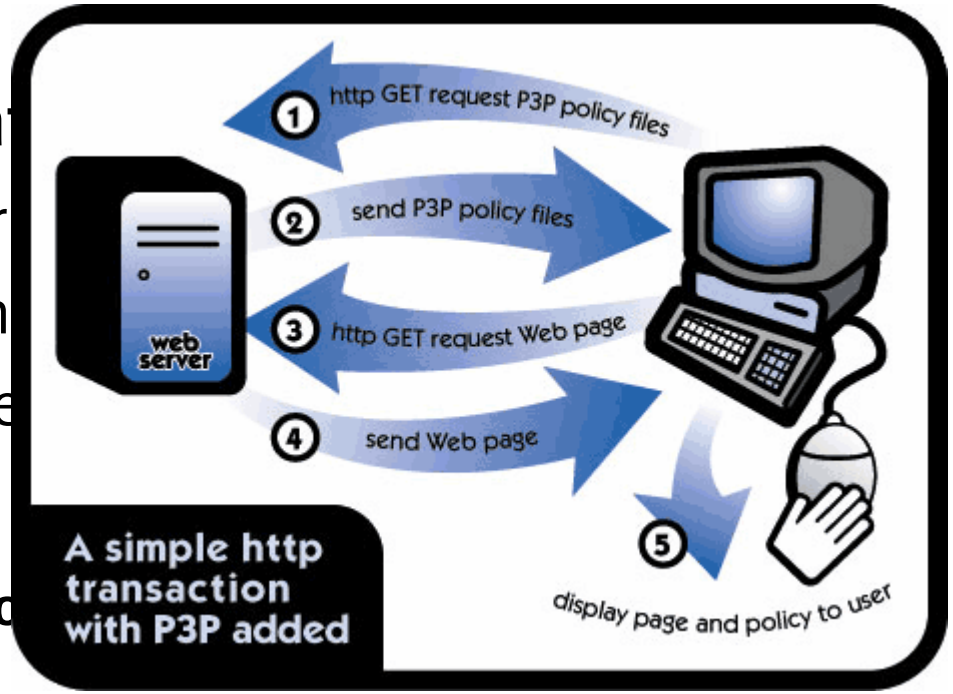
- **Lorrie Cranor, Marc Langheinrich, Massimo Marchiori, Joseph Reagle:** *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*. **W3C Recommendation, April 16, 2002.**

Grundlage: P3P

Platform for Privacy Preferences Project (W3C)

Platform for Privacy Preferences Initiative W3C

- **Maschinenlesbare Da**
  - Wer erhebt bzw. verar
  - Welche Daten werden
  - Zu welchem Zweck we
- **Basis-Datenschema**
  - Beispiel: **`user.home.po`**
- **Web-Protokoll**
  - Zum Austausch zwischen Webserver und Browser



Grafik © 2002 World Wide Web Consortium

- **Lorrie Cranor, Marc Langheinrich, Massimo Marchiori, Joseph Reagle:** *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*. **W3C Recommendation, April 16, 2002.**

```
<POLICY xmlns="http://www.w3.org/2000/P3Pv1"
        entity="TheCoolCatalog, 123 Main Street, Seattle, WA 98103, USA">
  <DISPUTES-GROUP>
    <DISPUTES service="http://www.PrivacySeal.org"
      resolution-type="independent"
     description="PrivacySeal, a third-party seal provider"
     image="http://www.PrivacySeal.org/Logo.gif"/>
    </DISPUTES-GROUP>
  <DISCLOSURE discuri="http://www.CoolCatalog.com/Practices.html" access="none"/>
  <STATEMENT>
    <CONSEQUENCE-GROUP>
      <CONSEQUENCE>a site with clothes you would  appreciate</CONSEQUENCE>
    </CONSEQUENCE-GROUP>
    <RECIPIENT><ours/></RECIPIENT>
    <RETENTION><indefinitely/></RETENTION>
    <PURPOSE><custom/><develop/></PURPOSE>
    <DATA-GROUP>
      <DATA name="dynamic.cookies" category="state"/>
      <DATA name="dynamic.miscdata" category="preference"/>
      <DATA name="user.gender"/>
      <DATA name="user.home." optional="yes"/>
    </DATA-GROUP>
  </STATEMENT>
  <STATEMENT>
    <RECIPIENT><ours/></RECIPIENT>
    <PURPOSE><admin/><develop/></PURPOSE>
    <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
      <DATA name="dynamic.clickstream.server"/>
      <DATA name="dynamic.http.useragent"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
```

y Preferences
t i v e

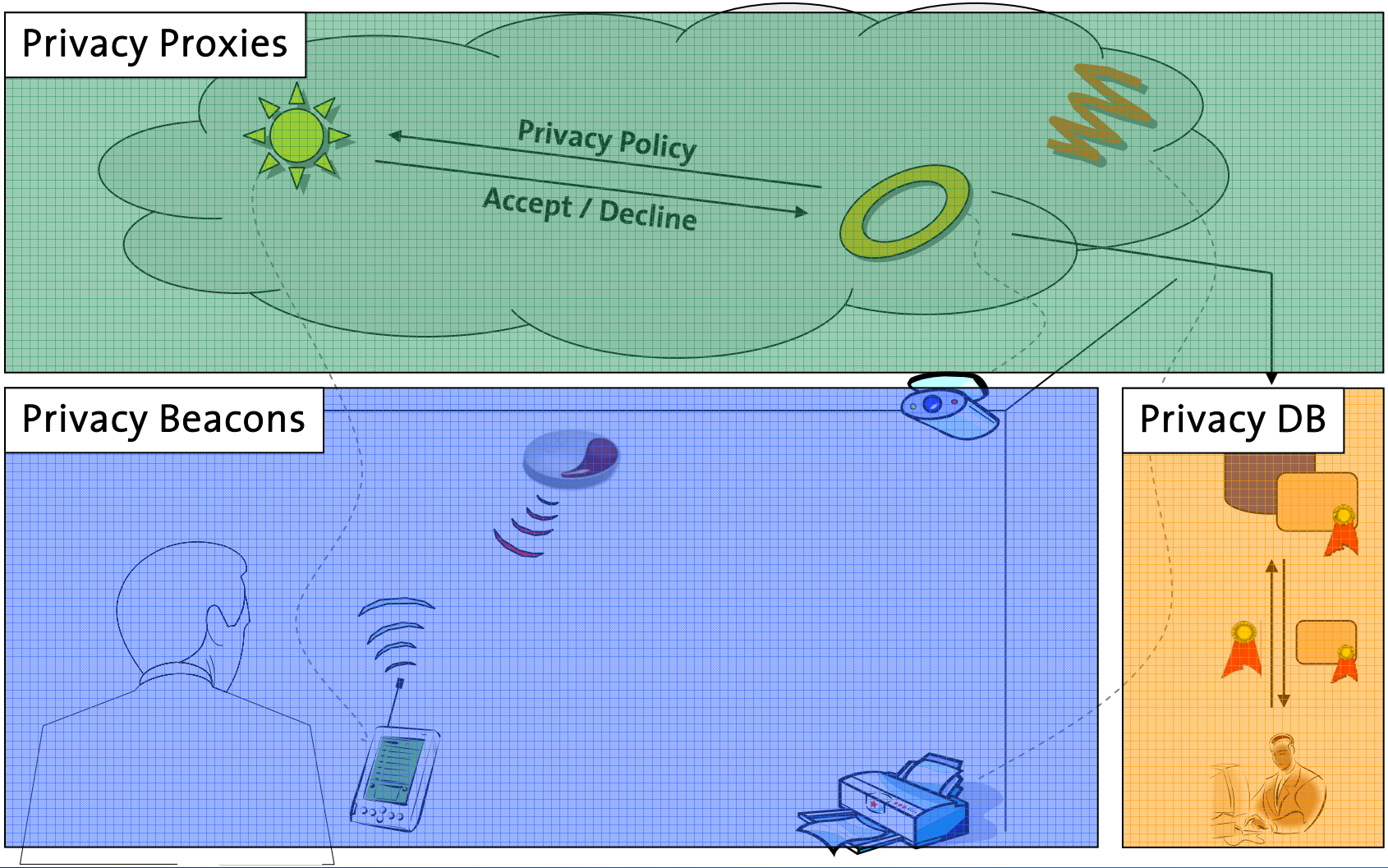
ide Web Consortium

wser

ferences 1.0 (P3P1.0)

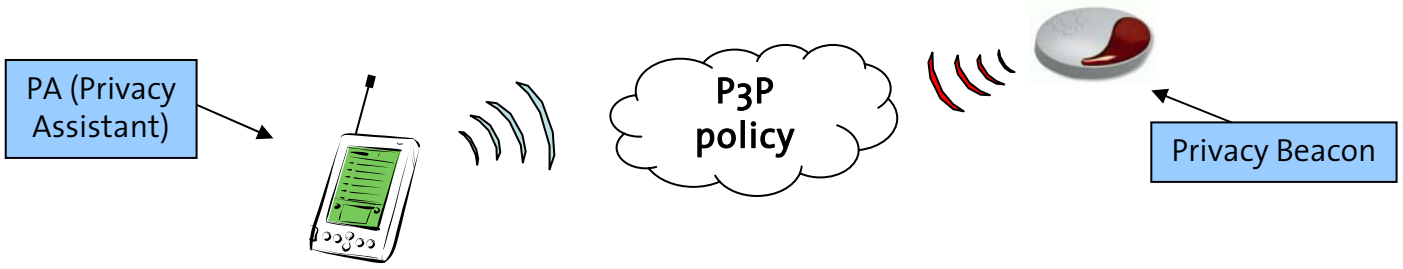
Specification. **W3C Recommendation, April 16, 2002.**

PawS – Ein „Privacy Awareness System"



1. Privacy Beacons

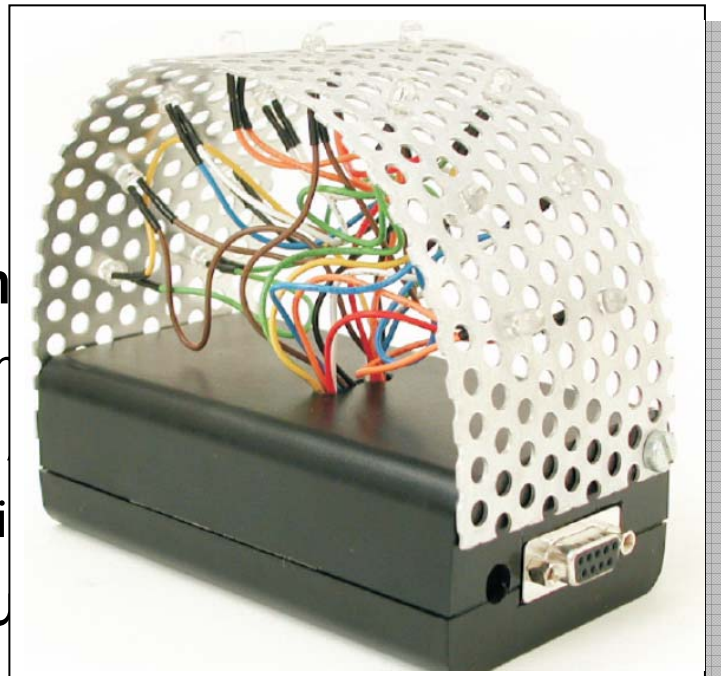
- **Kündigen (unmerkliche) Datenerhebung an**
  - Als “Protocol Beacons” Teil des Kommunikationsprotokolls
  - Als “Stand-alone Beacons” für Video, Audio und Sensoren
  - Empfang durch mobilen „Privacy Assistant“ (z.B. Armbanduhr)
- **Beschreibung der vorgesehene/durchgeführte Erhebung**
  - Format: Maschinenlesbare Datenschutzerklärungen („P3P++”)
  - Erweitert um Ubicomp-spezifische Felder (z.B. Sensordaten)



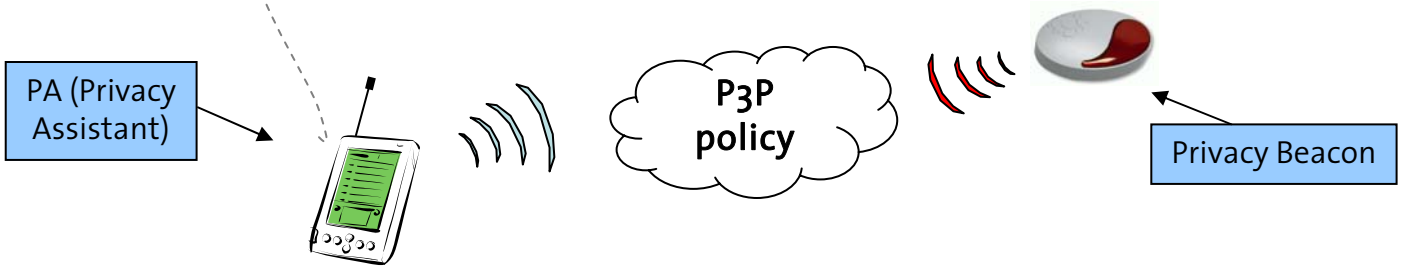
1.

- **Datenerh**
- **sehene/du**

Privacy-Assistant Prototyp

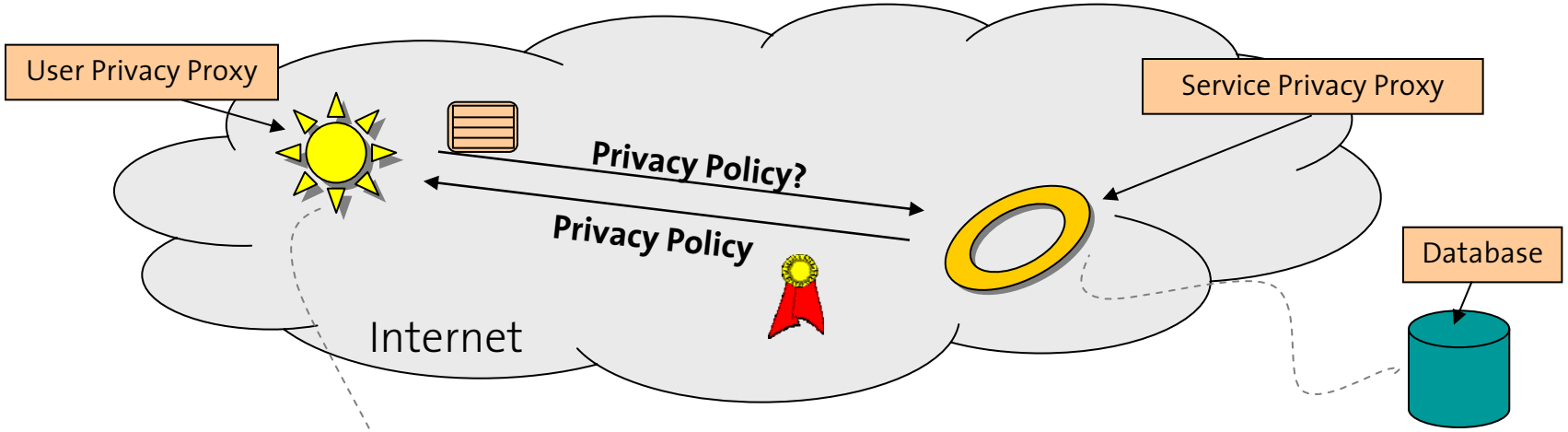


Privacy-Beacon Prototyp (IRREAL)



2. Privacy Proxies

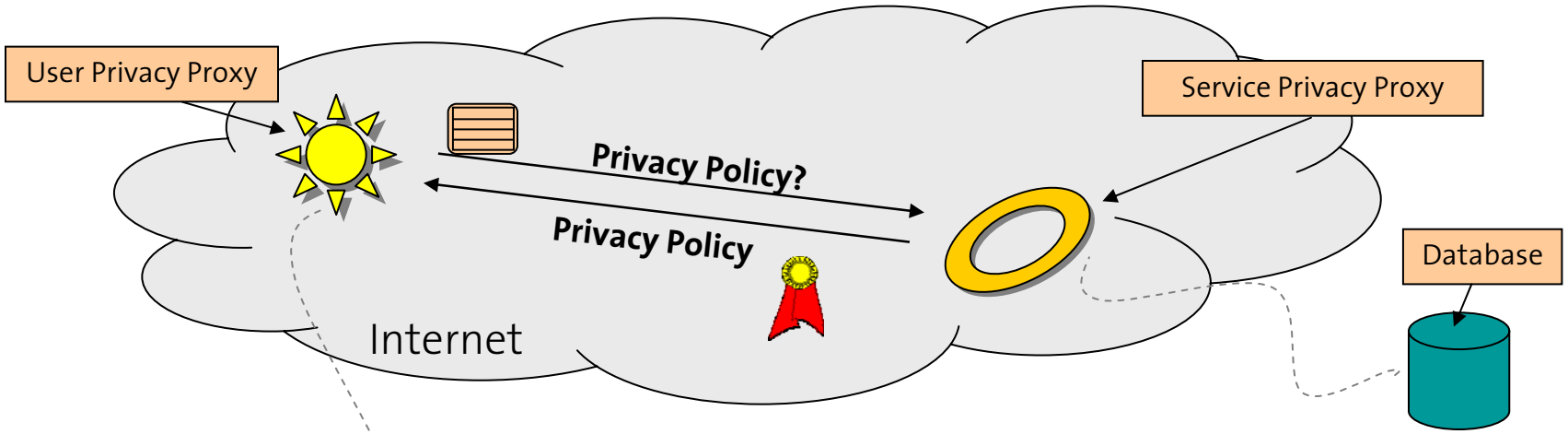
- **Service Proxy holt (wenn nötig) Einwilligung ein**
  - User Proxy vergleicht Nutzerpräferenzen mit Datenschutz-erklärung des Dienstanbieters
- **Zentraler Einstiegspunkt für Datenmanagement**
  - Unterstützt Aktualisierung und Löschung von Daten u. Verträgen



2. Privacy Proxies

Beispiel einer nutzer-initiierten Datenlöschung

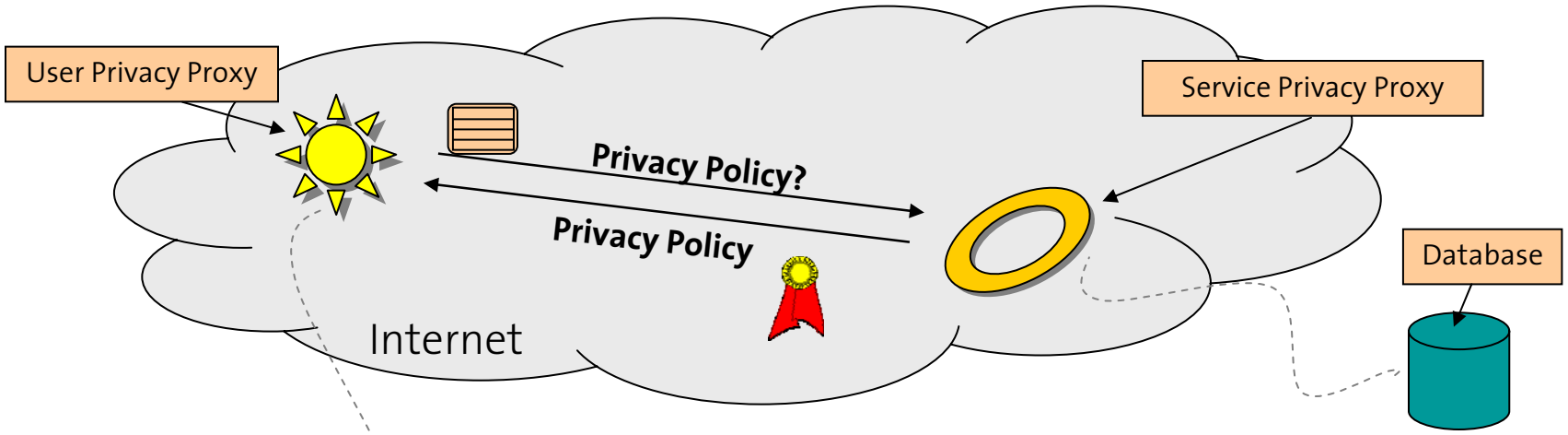
```
<DELETE>
  <DATA-GROUP>
    <DATA ref="#user.home-info.online.email"/>
    <DATA ref="#user.home-info.telecom.mobile"/>
    ...
  </DATA-GROUP>
</DELETE>
```



2. Privacy Proxies

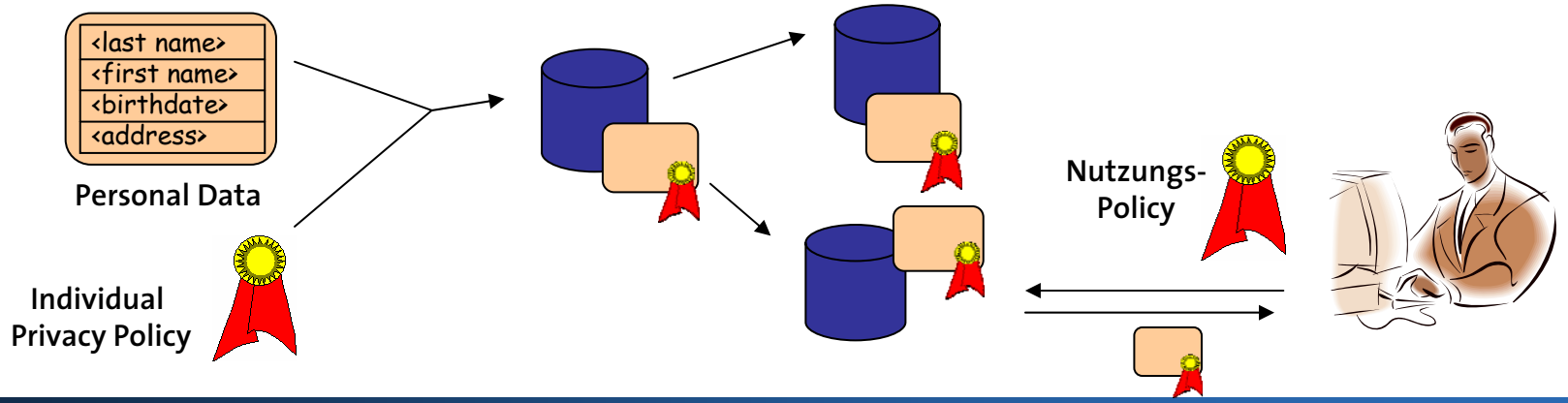
Beispiel einer service-initiierten Datenaktualisierung

```
<QUERY>
  <DATA-GROUP>
    <DATA ref="#user.location.submitted.symbolic.city"/>
    <DATA ref="#user.location.submitted.symbolic.street"/>
  </DATA-GROUP>
  <INFO discuri="http://service.example.com/locate/description.html">
    We need your current location in order to provide you with
    updated information as part of your WHERE_AM_I(tm)-subscription.
  </INFO>
</QUERY>
```



3. Privacy Aware Database

- **Speichert persönliche Daten gemeinsam mit P3P Policy**
  - Daten und Policy (Metadata) als logische Einheit
- **Jeder Datenzugriff benötigt Nutzungs-Policy**
  - Datenbank vergleicht erlaubte und geplante Nutzung
  - Daten mit unpassender Nutzung werden zurückgehalten
  - Jeder Datenzugriff wird vermerkt (Auditing)



3. Privacy Aware Database

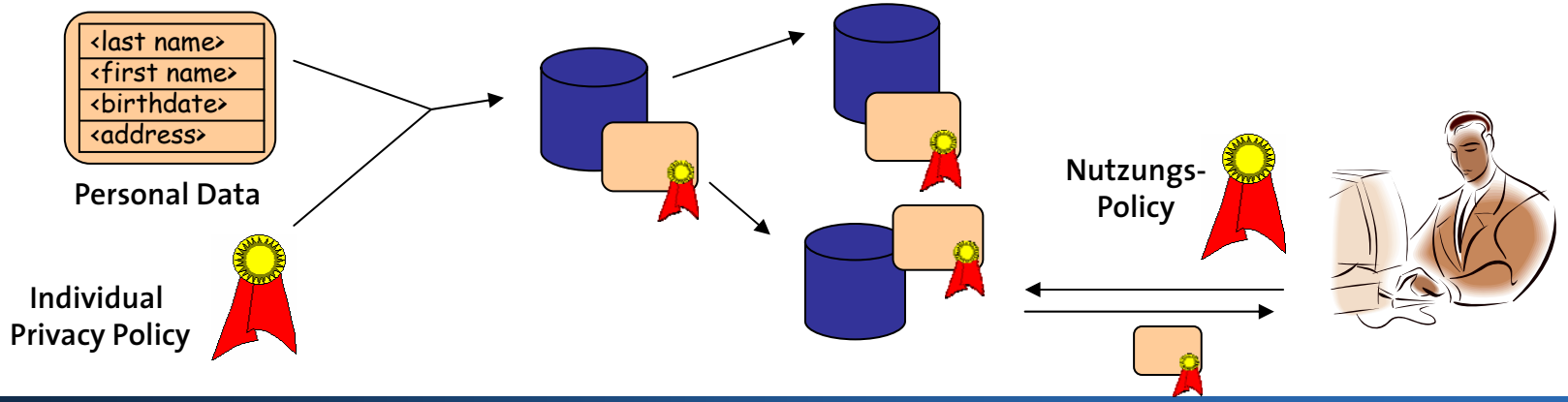
MarketingDept-Query : Table

Firstname	Lastname	Gender	Email	Street	Zip	City	State	Phone	BirthYear	BirthMonth	BirthDay	LastSeen
		m			98103	Seattle	WA					
		w			98123	Tacoma	WA					
		m	john@example.org	5432 Pine St NE	98089	Seattle	WA	(206) 342-2939	1976	February		01.01.2005 12:15:23
Jack	Doe	m	jack@example.org	1000 Main St.	10234	New York	NY					
Jane	Doe	w	jane@example.org	1000 Main St.	10234	New York	NY					

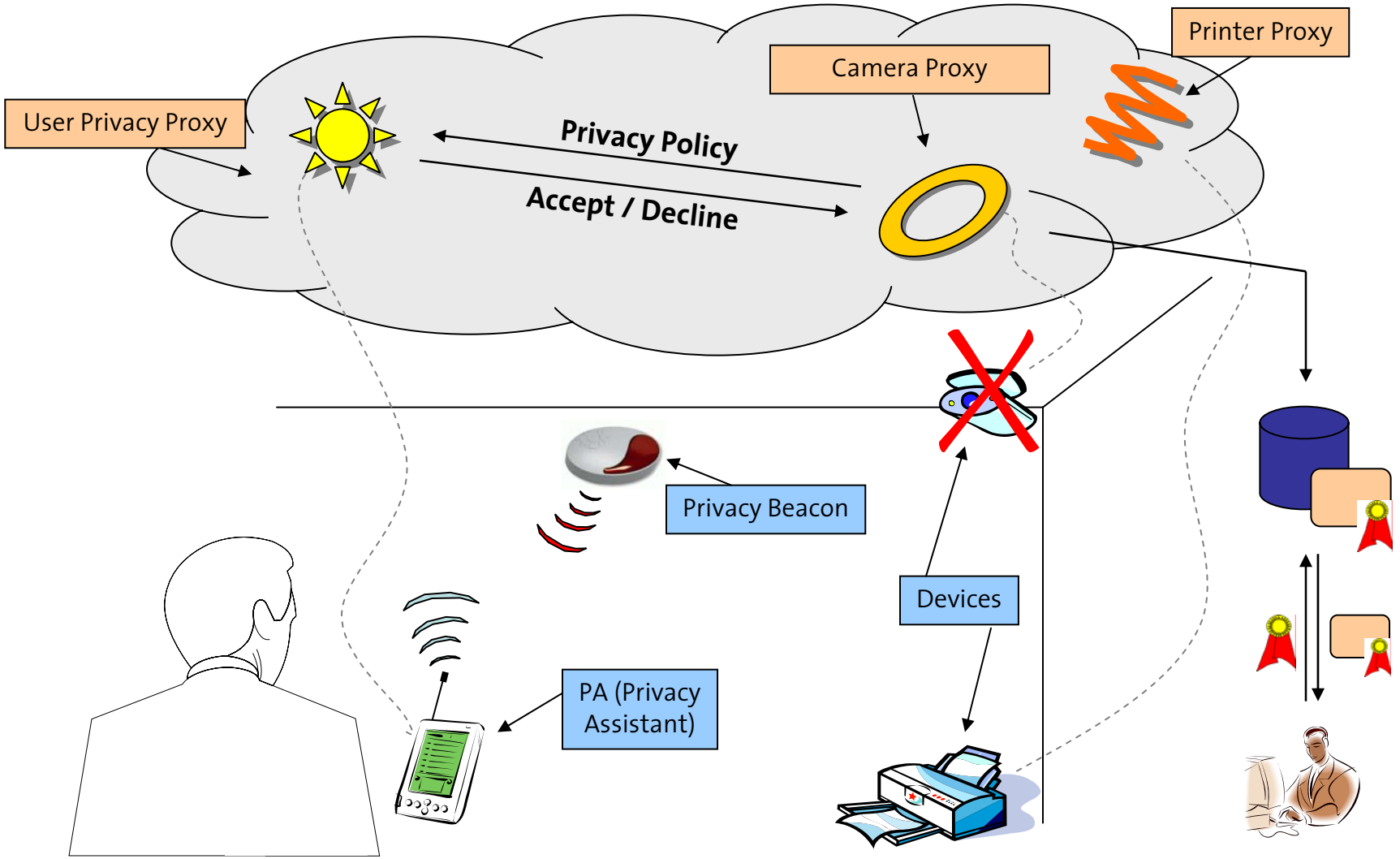
Record: 1 of 7831

Ergebnis einer nutzungsgefilterten Abfrage

- Datenbank vergleicht erlaubte un
- Daten mit unpassender Nutzung werden zurückgehalten
- Jeder Datenzugriff wird vermerkt (Auditing)

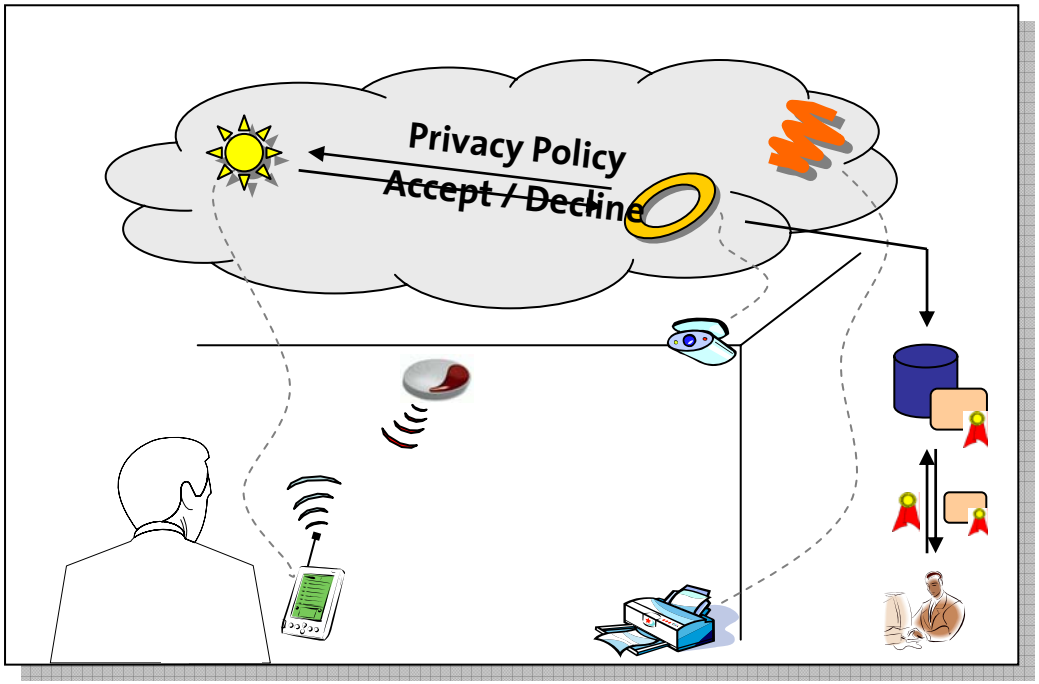


PawS Beispiel



PawS Implementation

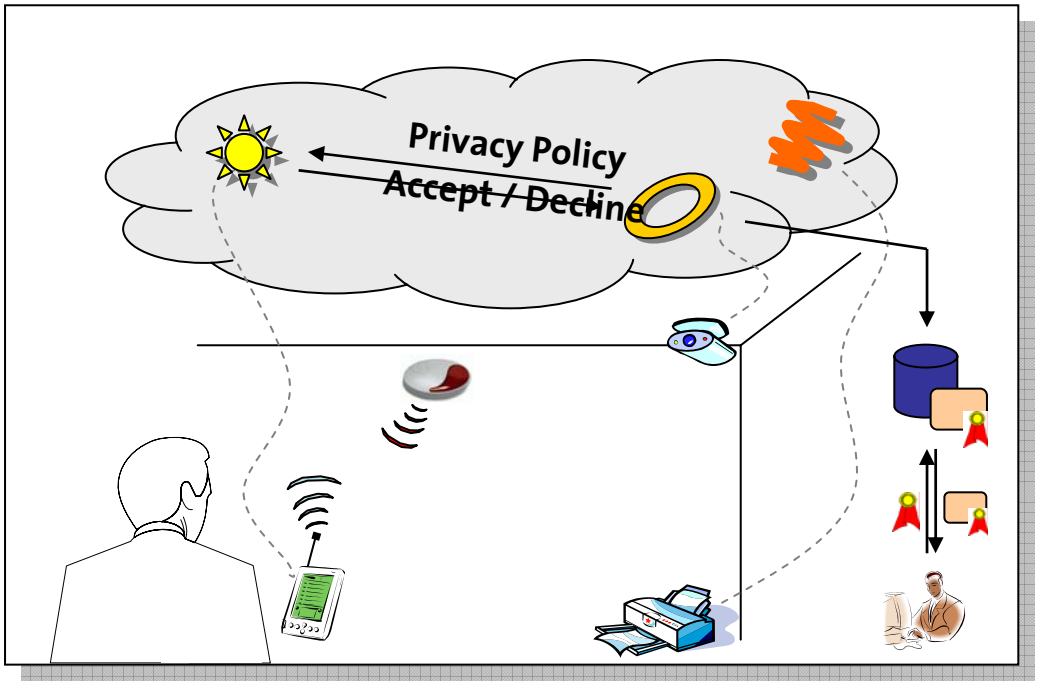
- **Privacy Database**
  - Oracle 8i, Java interface (no direct table access)
  - P3P policies cached for speed
- **Privacy Proxies**
  - Web service (Apache Tomcat)
  - SOAP, SSH, DSig
  - Extended P3P
- **Privacy Beacons**
  - IR Beacon (IRREAL)
  - Palm Tungsten C (WLAN)



PawS Implementation

Privacy ist vereinbar mit Ubiquitous Computing – technische Lösungen ermöglichen FIP in Ubicomp

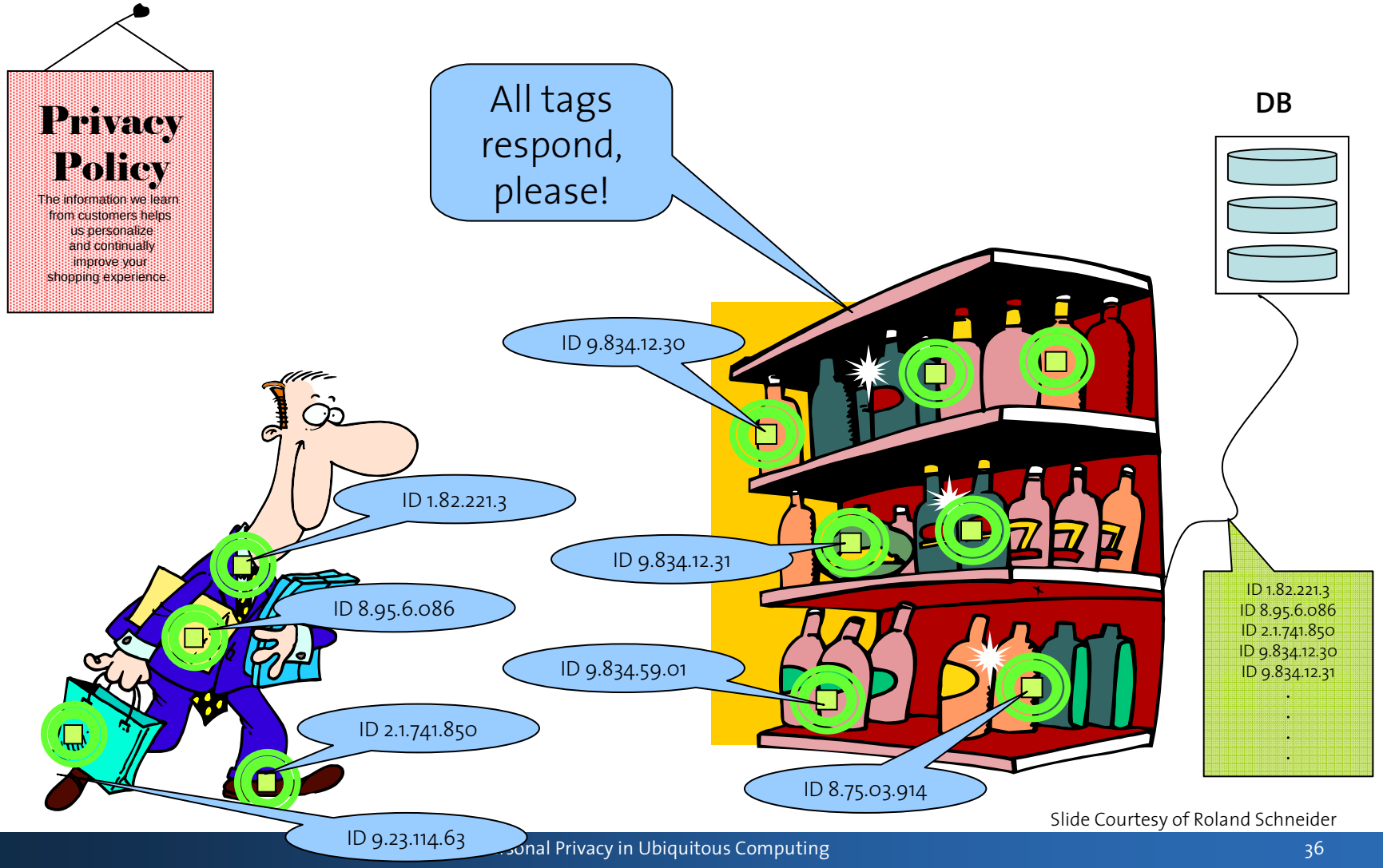
- **Privacy Database**
  - Oracle 8i, Java interface (no direct table access)
  - P3P policies cached for speed
- **Privacy Proxies**
  - Web service (Apache Tomcat)
  - SOAP, SSH, DSig
  - Extended P3P
- **Privacy Beacons**
  - IR Beacon (IRREAL)
  - Palm Tungsten C (WLAN)



Beiträge der Dissertation

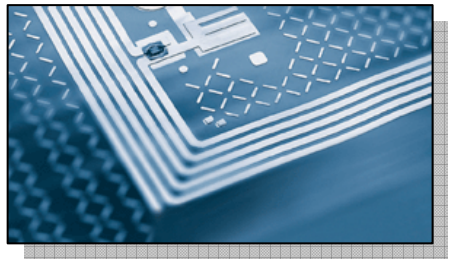
- **Analyse**
  - Was ist Privatheit/Privacy?
  - Wie wird diese von Ubiquitous Computing beeinflusst?
- **Technische Datenschutz-Infrastruktur (PawS)**
  - Privacy Beacons
  - Privacy Proxies
  - Privacy-Aware Database
- **Praxisbeispiel**
  - Privatheit und Funketiketten (RFID)

Heutige RFID Systeme

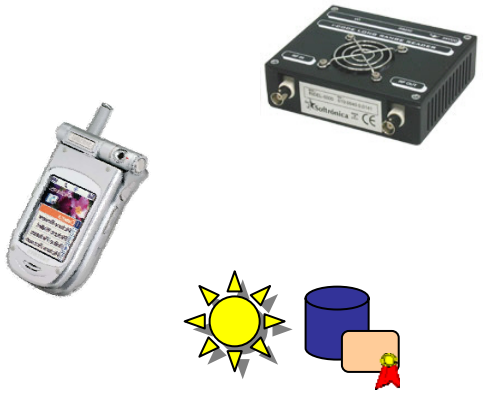


Slide Courtesy of Roland Schneider

RFID-PawS



- **Ziel: Fair Information Principles für RFID**
- **PawS im RFID Bereich**
  - Privacy Beacon: RFID-Lesergerät
  - Privacy Assistant: „Watchdog-Tag“
  - Privacy Proxies & Privacy Database
- **Anforderungen**
  - RFID-Standard Kompatibilität
  - Geringe Bandbreite



EPCglobal

- Christian Floerkemeier, Roland Schneider, Marc Langheinrich: Scanning with a Purpose – Supporting the Fair Information Principles in RFID protocols. UCS 2004, Tokyo, Japan, November 2004.

Beispiel: Openness in RFID-PawS

Protocol extension	Init round all	SUID flag	Round size	CRC-5	RPID	Purpose	Collection type	CRC-16
1 bit	6 bits	1 bit	3 bits	5 bits	96 bits	16 bits	2 bits	16 bits

- `Init_Round` **Befehl in ISO 18000 Part 6**
  - Definiert beginn eines Lesezyklusses (Aloha-basierte Antikollision)
  - Beinhaltet Parameter des Antikollisionsprotokolls
- **Neu: 130 Bits „Privacy-Header“ Extension**

Openness mittels ReaderPolicyID

Protocol extension	Init round all	SUID flag	Round size	CRC-5	RPID	Purpose	Collection type	CRC-16
1 bit	6 bits	1 bit	3 bits	5 bits	96 bits	16 bits	2 bits	16 bits

Header	Data Collector	Policy	Reader
8 bits	28 bit	24 bits	36 bits

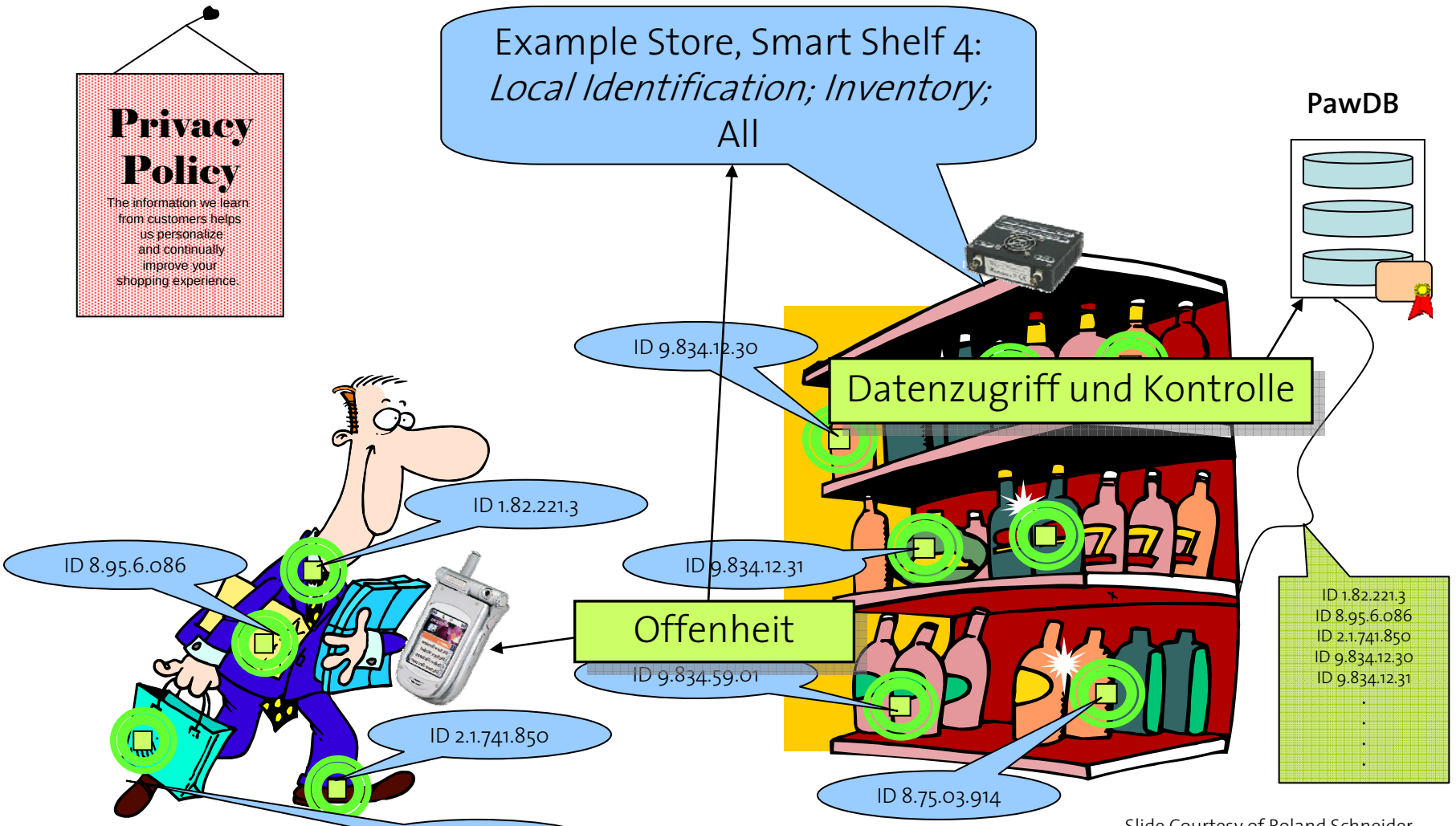
5F.4A886EC.8EC947.24A68E4F6

- **Jede Leseanforderung wird eindeutig zuordbar**
  - Datenerheber, Lesegerät und Datenschutzpolicy identifizierbar
  - Format analog EPC Standard (erleichtert Implementation)

RFID-PawS und die Fair Information Principles

Prinzip	Wird unterstützt durch...
Offenheit	Reader-Policy ID
Datenzugriff & -kontrolle	PawDB
Datensicherheit	(PawDB)
Datensparsamkeit	Tag Selection Mask, Purpose Declaration
Einwilligung des Subjekts	Watchdog-Tag

Heutige RFID Systeme (mit RFID-PawS)



Slide Courtesy of Roland Schneider

Zukünftige RFID-Systeme?

Slide Courtesy of Roland Schneider

Zusammenfassung

Beiträge der Dissertation

- **Analyse**
  - Was ist Privatheit/Privacy?
  - Wie wird diese von Ubiquitous Computing beeinflusst?

Marc Langheinrich: Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. **UbiComp 2001**, Oktober 2001

- **Technische Datenschutz-Infrastruktur (PawS)**
  - Privacy Beacons
  - Privacy Proxies
  - Privacy-Aware Database

Marc Langheinrich: A Privacy Awareness System for Ubiquitous Computing Environments. **UbiComp 2002**, September 2002

- **Praxisbeispiel**
  - Privatheit und Funketiketten (RFID)

Christian Floerkemeier, Roland Schneider, Marc Langheinrich: Scanning with a Purpose – Supporting the Fair Information Principles in RFID protocols. **UCS 2004**, November 2004

PawS: Grenzen und offene Fragen

- **Privacy Beacon Signal (Stand-alone Modus)**

  - Benötigt **Lokalisationsmodell** für Einsatz von Funktechnologie (WLAN, Bluetooth, Zigbee)
- **Privacy Assistant Nutzungsschnittstelle**

  - Nützlichkeit erst nach **Nutzerstudie** abwägbar
- **Beschränkt auf institutionelle Datenerhebungen**
  - Nur begrenzter Nutzen für **Peer Privacy** (z.B. Friend Finder Applikationen)

- **Sensordaten? Anonymität? …**

Ausblick

- **Kernproblem ubiquitärer Umgebungen**
  - Signifikante Verschärfung des Datenschutzproblems
  - Erfordert Lösungen auf allen Ebenen (Erhebung & Verarbeitung)
- **Privacy ist nicht nur ein Sicherheitsproblem**
  - Primär geht es um die Kommunikation mit anderen
- **Rechtlicher und sozialer Rahmen existieren**
  - Grundlage: Fair Information Principles
- **Technische Infrastruktur machbar**
  - Privacy Beacons, Privacy Assistants, Privacy Proxies, Privacy DB
  - Eingebettet in rechtliche und soziale Mechanismen

Verwandte Arbeiten

- **Privacy Infrastrukturen**
  - Myles et al. '03, Aura '03, Confab Toolkit '04
- **Nutzungsschnittstellen**
  - CSCW (Bellotti/Sellen '93, Neustaedter/Greenberg '03)
  - Peer Privacy (Aware Home Project, Confab Toolkit)
- **Identitätsmanagement**
  - *Identity Protector* '96, Leders *Faces* '02, Freiburg Identity Mngr '02
- **Privacy Databases**
  - k-anonymity '02, Hippocratic Databases '02, Enterprise P3P '02
- **Web Privacy, RFID Privacy, Location Privacy**