

# Seminar "Smarte Objekte und smarte Umgebungen"

## Identitätsmanagement

Teil1: Einführung und die „ideale Sicht“ - Systeme aus der Forschung  
Teil2: Die angewandte Sicht - Industrielle Systeme (Marcel Beer)

Bettina Polasek

# Das Schlagwort „Identitätsmanagement“

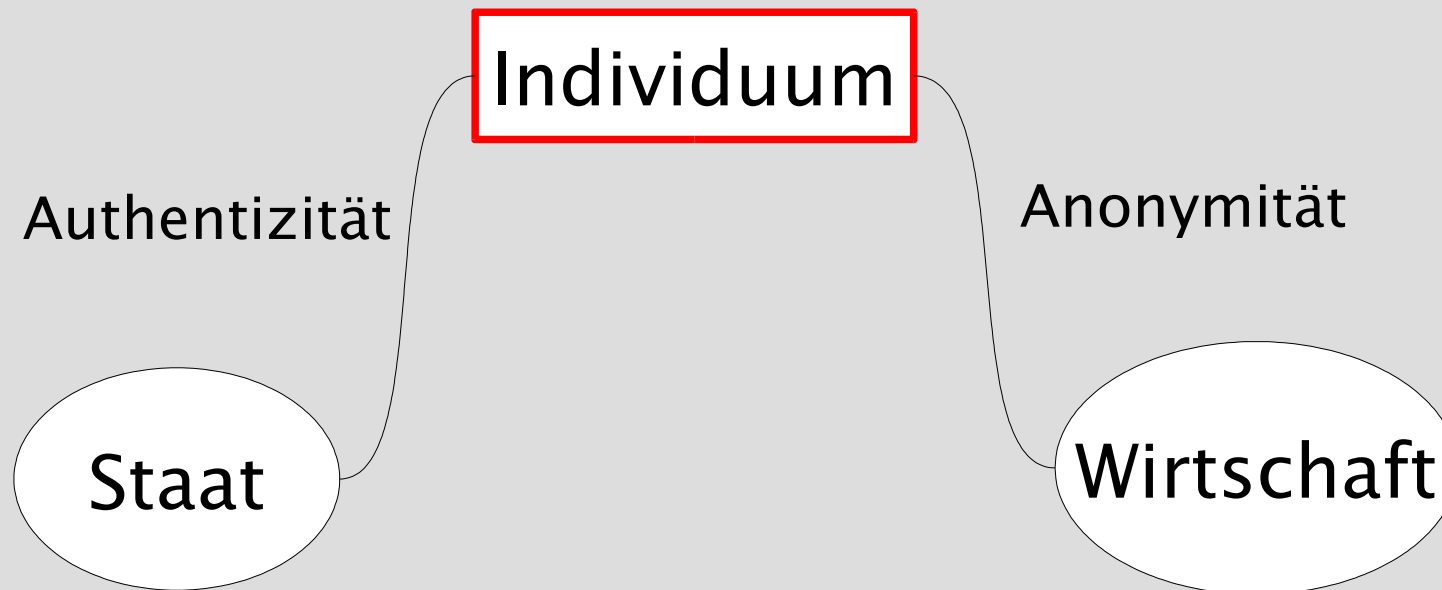
- *„Greater confidence about the identity of individuals, particularly in electronic contexts, is aimed at preventing financial, welfare and benefit fraud, protecting national borders and increasing national security, as well as better profiling customers or clients to better target services and goods.“* (Malcolm Crompton, Federal Privacy Commissioner, *„Proof of ID Required? Getting Identity Management Right“*)
- *„Many of us can imagine how much more convenient it would be to have fewer PINs, passwords, and plastic cards, for example.“* (Malcolm Crompton, Federal Privacy Commissioner, *„Proof of ID Required? Getting Identity Management Right“*)

IM – die Lösung für alle e-Probleme?

# Übersicht

- Einleitung: Was ist Identitätsmanagement?
  - Grundsätze des IM
- Zwei Systeme aus der Forschung
  - ATUS – A Toolkit for Usable Security
  - DRiM – Dresden identity Management
- Probleme von IM
- Schlussfolgerungen

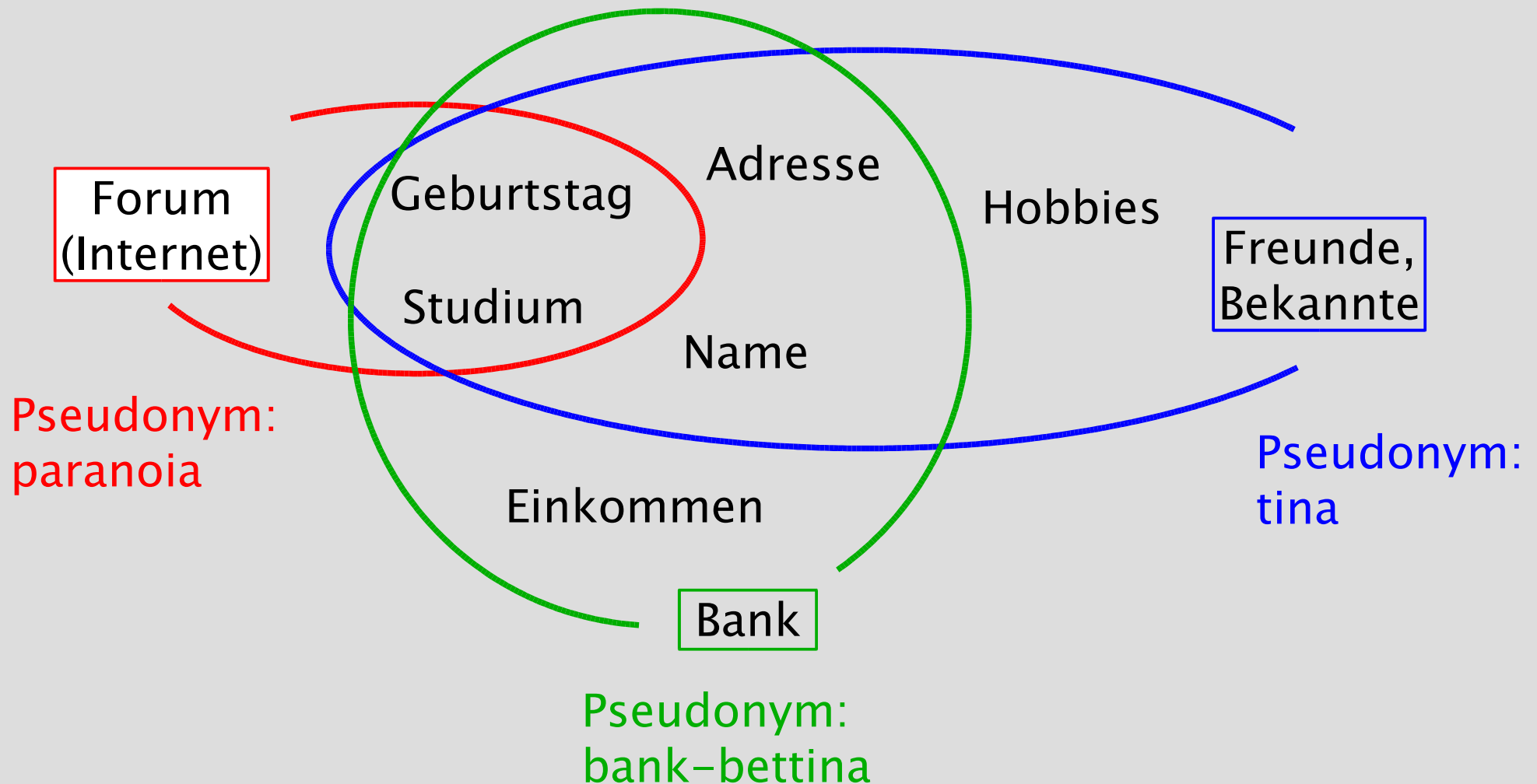
# Grundidee hinter dem Begriff Identitätsmanagement



# Vier Grundsätze des IMs

- Pseudonyme, Teilidentitäten
- Authentizität, Anonymität
- Privatheit, Vertrauen
- Benutzer-Kontrolle

# Pseudonyme und Teilidentitäten



# Authentizität Anonymität

- Nachweisen einer Eigenschaft, ohne Preisgabe der Anonymität
- Trusted Third Parties
- Beispiel: Führerschein
- „Authentifizierung“ ist **nicht gleich** „Anonymität aufgeben“!

# Privatheit (Privacy) Vertrauen

- Kommunikationspartner vertrauen, Kommunikationskanal schützen
- Privacy Policies
- Beispiel:
  - Ich bekomme wirklich das, was ich mit meiner Kreditkarte bezahlt habe
  - Ich weiss, dass meine Daten nicht zweckentfremdet werden



# Benutzer-Kontrolle

- Kontrolle über das IM-System
- Überblick über Pseudonyme, persönliche Daten und Kommunikation
- Hinweise, Warnungen bei Verletzung der Privatheit
- Leichte Konfiguration, intuitive Bedienung
  - gute Standardeinstellungen

# Weitere Anforderungen

- Mobilität, Verfügbarkeit
- Benutzerfreundlichkeit
  - notwendige Konfiguration
- Verlässlichkeit des Systems
- Standards
  - P3P

# Übersicht

- Einleitung: Was ist Identitätsmanagement?
  - Grundsätze des IM
- **Zwei Systeme aus der Forschung**
  - ATUS – A Toolkit for Usable Security
  - DRiM – Dresden identity Management
- Probleme von IM
- Schlussfolgerungen

# ATUS – A Toolkit for Usable Security

- System der Albert-Ludwigs-Universität Freiburg, Institut für Informatik und Gesellschaft
- *„The iManager. It supports the user to obtain the desired security and to control his / her personal data.“*  
([http://tserv.iig.uni-freiburg.de/telematik/forschung/projekte/kom\\_technik/atus/idm.html](http://tserv.iig.uni-freiburg.de/telematik/forschung/projekte/kom_technik/atus/idm.html))

# ATUS – Demo

[http://tserv.iig.uni-freiburg.de/telematik/forschung/projekte/kom\\_technik/atus/idm-demo/index.html](http://tserv.iig.uni-freiburg.de/telematik/forschung/projekte/kom_technik/atus/idm-demo/index.html)

# ATUS – Funktionalität

- Agiert zwischen Netzwerk und Applikation
  - für email, www, etc.
  - Netzwerk-Interface für Anwendungen (Socket)
- Sicherheitsmechanismen als Plug-Ins realisiert
  - Kryptographie, digitale Unterschriften
- Filter Funktionalität
  - alle ein- und ausgehende Daten werden gescannt (?)
  - HTML Formulare vor-ausgefüllt
- Datenbanken
  - z.Bsp. Für „Rules“

# ATUS – Zusammenfassung

- Fokus auf Benutzer-Schnittstelle
  - Klare Übersicht über Identitäten
- Unterstützt wesentliche IM Grundsätze
  - Benutzer-Kontrolle
  - Teilidentitäten, Pseudonyme
  - Privatheit, Zurechenbarkeit mittels Kryptographie
  - Anonymität, Authentizität

# DRiM – Dresden Identity Management

- System der Technischen Universität Dresden, Fakultät Informatik
- *„Im Projekt DRiM werden Grundlagen, Techniken und Einsatzszenarien für ein datenschutzgerechtes Identitätsmanagement erforscht.“*  
(<http://drim.inf.tu-dresden.de/index.de.html>)



# DRiM – Funktionalität

- Paket mit SSONET (Sicherheit und Schutz in offenen Datennetzen)
  - Java-Bibliothek zum Aufbauen mehrseitig sicherer TCP-IP-Verbindungen
  - Applikationen müssen auf API aufbauen
  - Alle Beteiligten müssen DRiM unterstützen
- Verhandlung der Sicherheitsbedingungen
  - Sicherheitskonfiguration, Unterstützung von P3P
- Anonymes Surfen
  - <http://anon.inf.tu-dresden.de/>

# DRiM – IDMAN

- IDMAN – der Identitätsmanager
- Pseudonyme
  - Nutzung: einmalig, wiederverwendbar
  - digitale Signatur
- PKI – Identitätstreuhänder
  - Registrierungsphase: offline
  - Zertifikate anfordern: online

# DRiM – ATUS

- Forschungsprojekte, Prototypen
- Aufgebaut auf den 4 Grundsätzen

## DRiM

- Sicherheits-orientiert
- *application framework*

## ATUS

- Benutzer-orientiert
- *extended firewall*

# Probleme von IM

- Schlechtes IM:  
„eine Nummer pro Person“ - System
  - Leichtes Zusammenführen der Daten
- Sicherheit der Daten
  - Attacken
- Wer bietet IM-Systeme an?
  - Vertrauen der Benutzer
- Abhängigkeit

# Schlussfolgerungen

- IM gestern: kein Thema
- IM heute: grosses Thema
  - leichtere Verwaltung elektronischer Daten
- IM morgen: IM in einer smarten Umgebung?
  - Kein klarer Wechsel zwischen digitaler und realer Welt → Kontexterkenkung!
  - Vertrauen in Alltagsgegenstände?

# Ende Teil 1

- Fragen?
- Weiter geht's mit  
Teil2: Die angewandte Sicht -  
Industrielle Systeme (Marcel Beer)
- Anschliessend:  
Diskussion