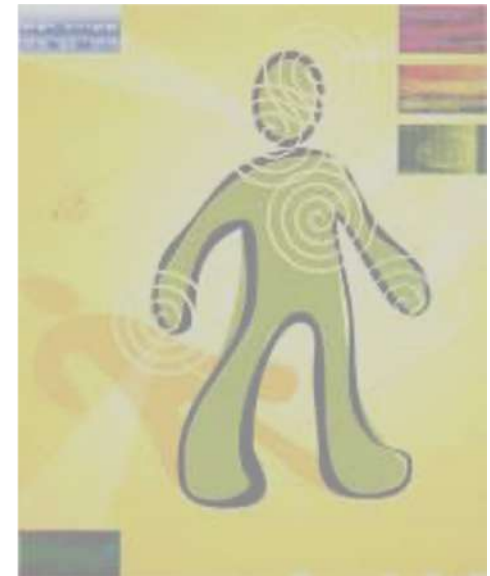


Information & Communication Security (WS 2020)

Identity Management

Prof. Dr. Kai Rannenberg

Chair of Mobile Business & Multilateral Security
Goethe-University Frankfurt a. M.



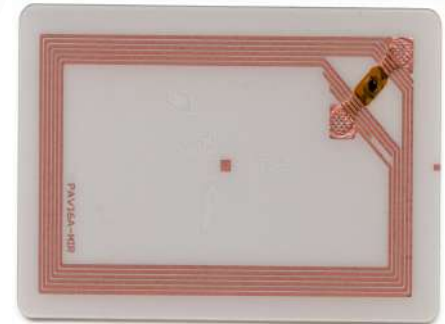
- Introduction
- Identity Concepts
 - Different Views of Identity
 - Working Definitions
- Identity Management
 - Functions
 - Systems
 - Types



THE UK IDENTITY CARD



**WITHOUT
IT YOU'RE
NO-ONE**



Identity-Related Technologies: Trends



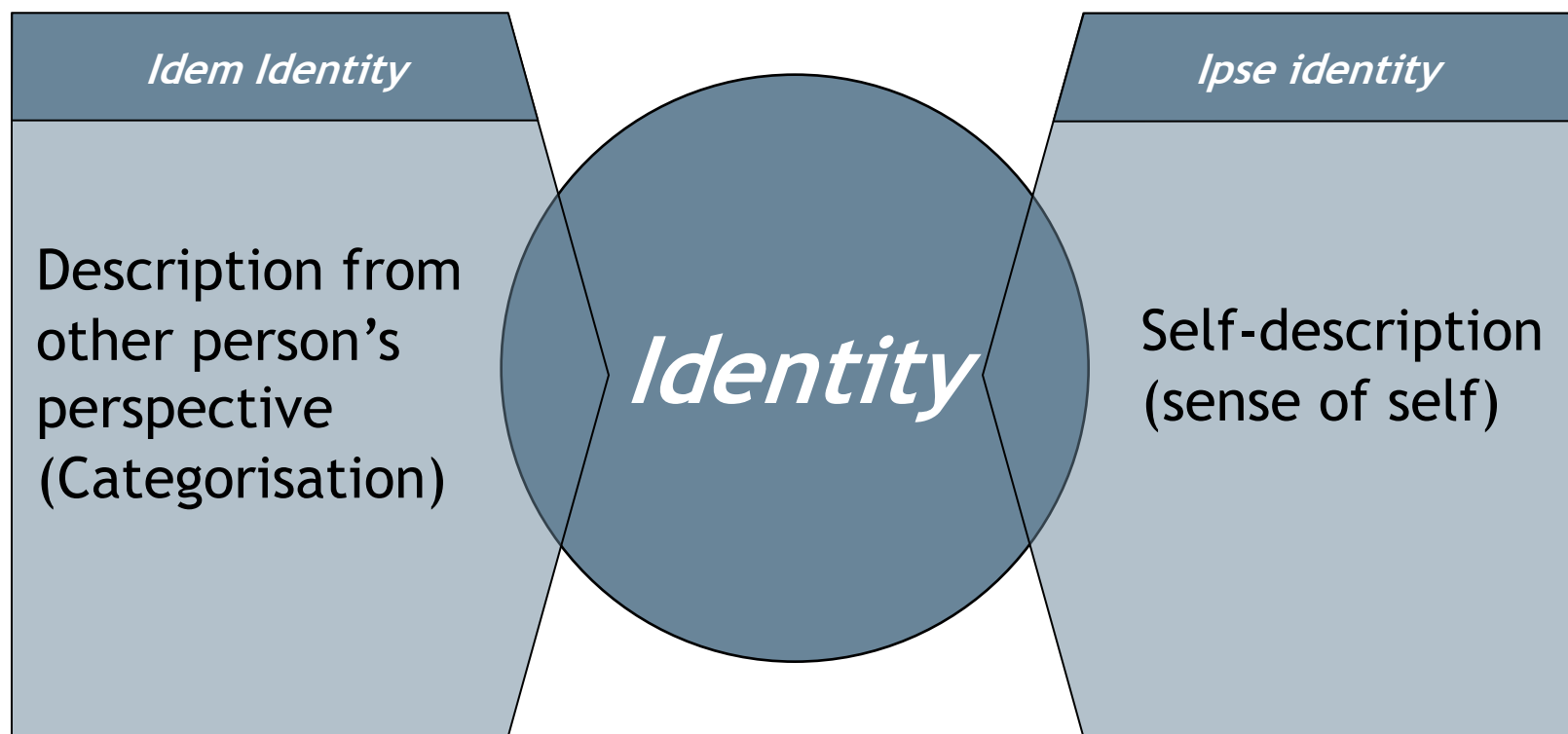
NATIONAL REGISTRATION IDENTITY NUMBER AND NAME OF HOLDER		PHOTOGRAPH OF HOLDER		DESCRIPTION OF HOLDER	
PT	8020			Place of Birth <i>Brighton Sussex</i>	
HALL				Date of Birth <i>28 December 1906</i>	
JAMES H.				Height <i>5'-10"</i>	
Signature of Holder <i>J. H. Hall</i>				Visible Distinctive Marks <i>NONE</i>	
LEFT HAND FINGERPRINTS (Plain impressions of four fingers)				RIGHT HAND FINGERPRINTS (Plain impressions of four fingers)	
		THUMBS—PLAIN IMPRESSIONS			
		Left Thumb	Right Thumb		



- Introduction
- Identity Concepts
 - Different Views of Identity
 - Mental vs. Procedural View
 - Implicit vs. Explicit View
 - View of Identity (Control) according to Durand
 - Working Definitions
- Identity Management
 - Functions
 - Systems
 - Types

Identity Concepts

Mental vs. Procedural View | 1



- **Mental identity** (ipse, I)
 - Researched by social/psychological sciences
 - Dynamically changing configuration reflecting, and shaped by, interactions between an individual and its environment
 - Private and endless task to go deeply in ones' own description:
 - “Only I can be responsible for acts done by me.”
 - “I remain myself by being faithful to my promises.”

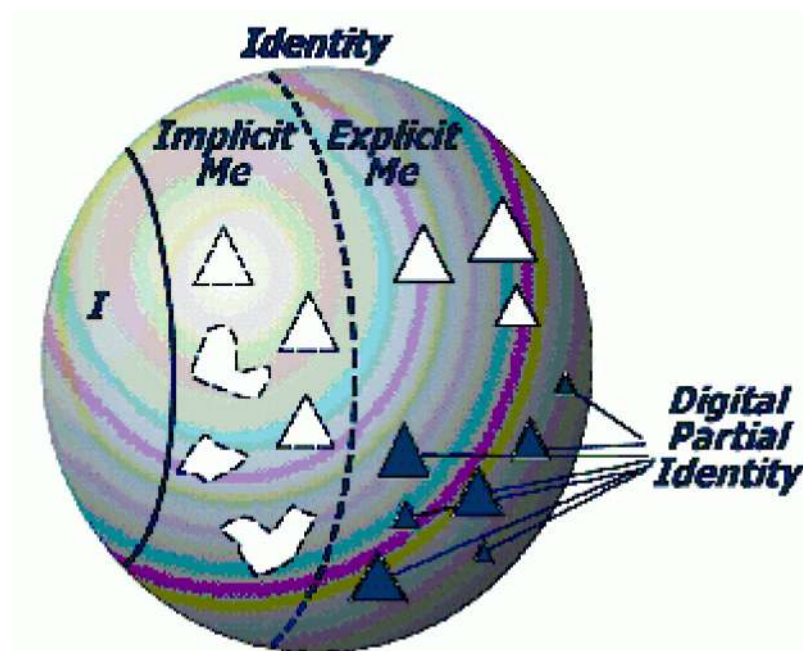
- **Procedural identity** (idem, Me)
 - Used by technical/administrative sciences
 - Collection of formalized characteristics, which enable identification and authentication necessary for social and economic relations, as well as dealings with the authorities.
 - E.g., a person's name, marital status, date of birth, height, colour of skin or eyes, number of children, nationality, educational and professional qualifications, etc.
 - The choice of these characteristics may depend on the context, i.e. controlling authority, functional needs, etc.

Identity Concepts

Implicit vs. Explicit View

The procedural identity (**Me**) can be further differentiated

- **The I**
the indeterminate first person perspective
- **Implicit Me**
how a person perceives her-/himself
- **Explicit Me**
how this person is perceived and represented



- ***Tier 1 (T1):*** True (‘My’) identity
- ***Tier 2 (T2):*** Assigned (‘Our’) identity
- ***Tier 3 (T3):*** Abstracted (‘Their’) identity
- The different tiers can be distinguished by the factor ‘control’ : ***Who controls the identity?***

Identity Concepts

Tier 1: True Identity

- *A Tier 1 (true - 'My') identity is my true and personal digital identity and is owned and controlled entirely by me, for my sole benefit.*
- *T1 identities are both timeless & unconditional.*

[Durand2003]

Identity Concepts

Tier 2: Assigned Identity

- A Tier 2 (assigned - ‘Our’) identity refers to our digital identities that are assigned to us by corporations (e.g. our ‘customer accounts’).
 - *Our* job title (assigned to us by our employer)
 - *Our* cell phone number (assigned to us by our mobile phone operator)
 - *Our* United Mileage Plus number (assigned to us by United Airlines)
 - *Our* social security number (assigned to us by the Government)
 - *Our* credit card number (assigned to us by our credit card companies)

[Durand2003]

Identity Concepts

Tier 3: Abstracted Identity

- A Tier 3 (abstracted - 'Their') identity is an abstracted identity in that it identifies us through our demographics and other reputation like attributes, but does not need to do so in a 1:1 manner.
 - T3 identities speak to the way in which companies aggregate us into different marketing buckets for the purposes of advertising or communicating with us.
 - E.g., we're either a 'frequent buyer' or a 'one time customer' etc.
 - T3's are typically based upon our behaviour in our interactions with business.
 - The entire CRM market caters to T3 identities.

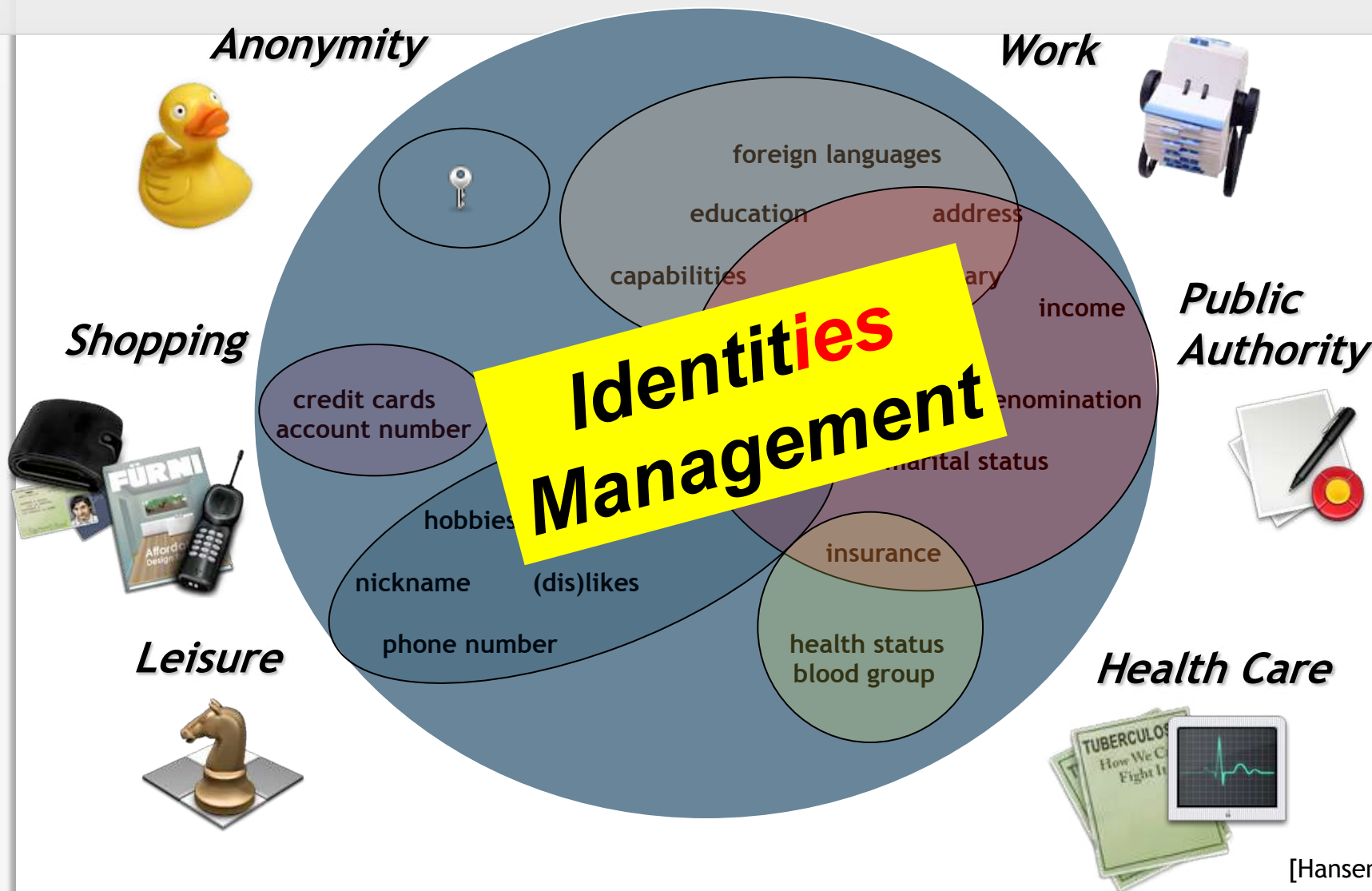
[Durand2003]

- Introduction
- Identity Concepts
 - Different Views of Identity
 - Mental vs. Procedural View
 - Implicit vs. Explicit View
 - View of Identity (Control) according to Durand
 - Working Definitions
- Identity Management
 - Functions
 - Systems
 - Types

- ***Identity:***
The characteristics (attributes) representing an acting entity
- ***Partial identity:***
A subset of the characteristics of an identity
- ***ISO/IEC 24760 “A framework for identity management”:***
 - **Identity** (partial identity): Set of **attributes** related to an **entity**
 - **Identifier:** attribute or set of attributes that uniquely characterizes an identity in a domain
- **Why are partial identities important?**
 - Different partial identities are assigned to and abstracted from an entity.
 - The identity of an entity consists of partial identities distributed over different partners of the entity.

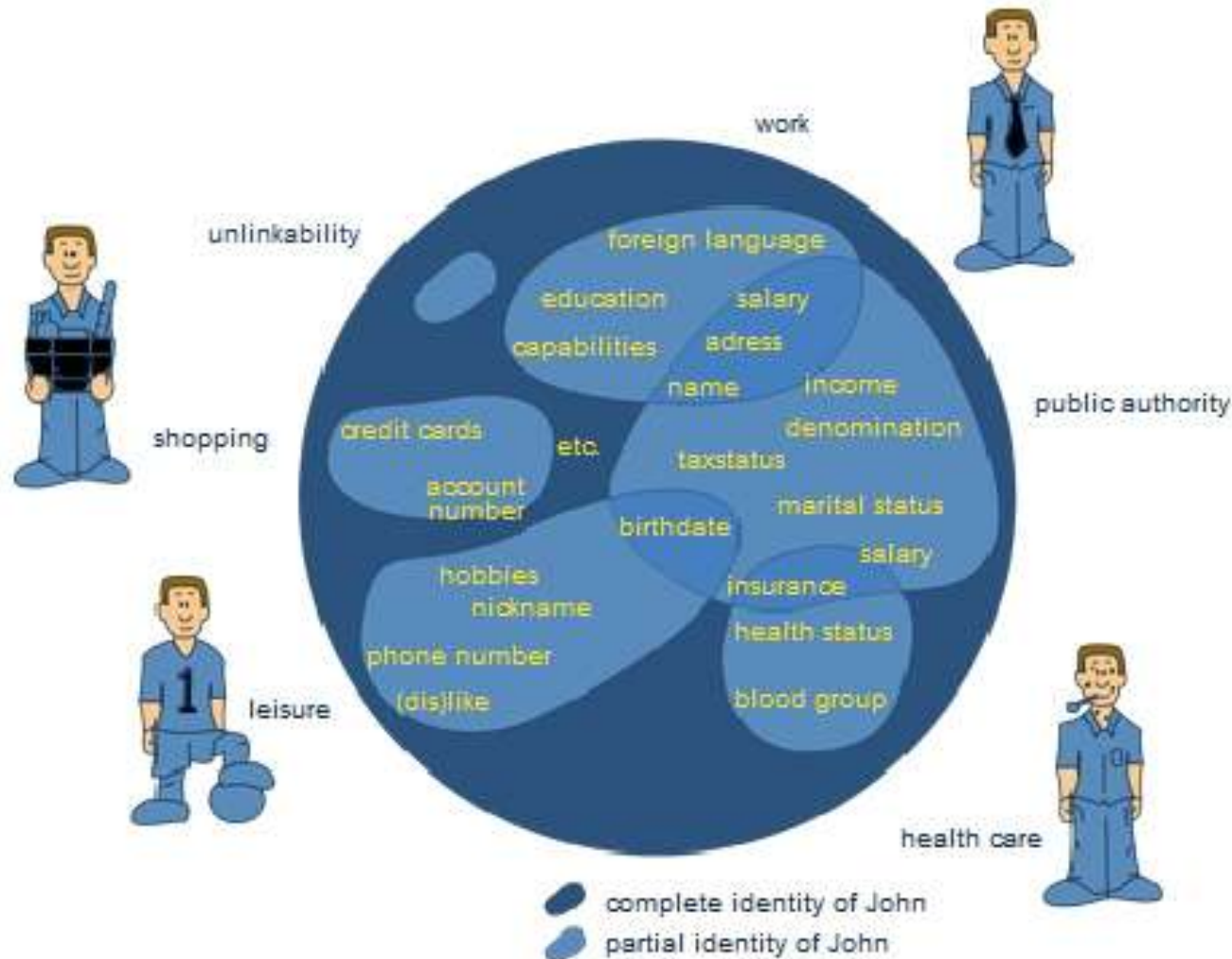
Identity Concepts

Partial Identities Illustrated | 1



Identity Concepts

Partial Identities Illustrated | 2



[PRIME 2006]

- Introduction
- Identity Concepts
- Identity Management
 - Functions
 - Systems
 - Types
 - Account Management
 - Profiling
 - Personal Identity Management

- Identity Management (IdM) is often used as a **buzz word** that can have many meanings
 - The management of accounts for employees, customers or citizens. These accounts containing those parts of an identity relevant for an organization (attributes, access rights, roles, ...)
 - Trend towards federations between organizations
 - The collection and analysis of data about individuals allowing for the extraction of useful knowledge on these individuals (profiling)
 - e.g., for marketing or law enforcement purposes
 - The possibility of an individual to manage its procedural identities with different organizations (partial identities) and in this way allowing it in to build a 'healthy' virtual socio-psychological identity.

Identity Management (IdM)

2 sides of a medal with enormous economic potential

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies

- **Organisations** aim to sort out
 - User Accounts in different IT systems
 - Authentication
 - Rights management
 - Access control
- **Unified identities** help to
 - ease administration
 - manage customer relations
- **Identity management systems**
 - ease single-sign-on by unify accounts
 - solve the problems of multiple passwords

- **People** live their life
 - in different roles (professional, private, volunteer)
 - using different identities (pseudonyms): email accounts, SIM cards, eBay trade names, chat names, social network names, ...)
- **Differentiated identities** help to
 - protect
 - privacy, especially anonymity
 - personal security/safety
 - enable reputation building at the same time
- **Identity management systems**
 - support users using role based identities
 - help to present the “right” identity in the right context

- **People** live their life
 - in different roles (professional, private, volunteer)
 - using different identities (pseudonyms): email accounts, SIM cards, eBay trade names, chat names, social network names, ...)
- **Differentiated identities** help to
 - protect
 - privacy, especially anonymity
 - personal security/safety
 - enable reputation building at the same time
- **Identity management systems**
 - support users using role based identities
 - help to present the “right” identity in the right context

- **Organisations** aim to sort out
 - User Accounts in different IT systems
 - Authentication
 - Rights management
 - Access control
- **Unified identities** help to
 - ease administration
 - manage customer relations
- **Identity management systems**
 - ease single-sign-on by unify accounts
 - solve the problems of multiple passwords

- Introduction
- Identity Concepts
 - Different Views of Identity
 - Mental vs. Procedural View
 - Implicit vs. Explicit View
 - View of Identity (Control) according to Durand
 - Working Definitions
- Identity Management
 - Functions
 - Systems
 - Types

- Provisioning, Enrolling, Choosing
- Binding with Attributes
- Certifying
- Changing
- Unbinding of Attributes
- Deleting
- ...?

- Introduction
- Identity Concepts
 - Different Views of Identity
 - Mental vs. Procedural View
 - Implicit vs. Explicit View
 - View of Identity (Control) according to Durand
 - Working Definitions
- Identity Management
 - Functions
 - Systems
 - Types

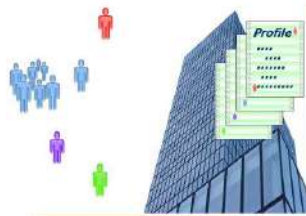
- Identity Management Systems (IdMS) are tools that support Identity Management activities. We distinguish
 - 1. Pure IdMS main objective is support of identity management functionality, e.g, MS CardSpace (former) Passport, Liberty, Shibboleth, OpenID, PingID, password managers, form fillers
 - 2. Systems/applications with another core functionality, but basing on some identity management functionality, e.g. GSM, PGP, eBay
 - 3. Systems/applications independent from identity management functionality, with some identity management functionality as add-on, e.g., HTML browsers, chat clients

Identity Management: Types of IdM (Systems)

Type 1



Type 2



Type 3



Account Management:
assigned identity
(= Tier 2)

Profiling:
derived identity
abstracted identity
(= Tier 3)

Management of
own identities:
chosen identity
(= Tier 1)

by organisation

by organisation

by user himself
supported by
service providers

➡ There are hybrid systems
that combine characteristics

- Tiers of Identity are ordered by the extent of control the individual has over the identity.
My > Our > Their
- Types of identity management are ordered by the (historic) appearance of the respective systems.

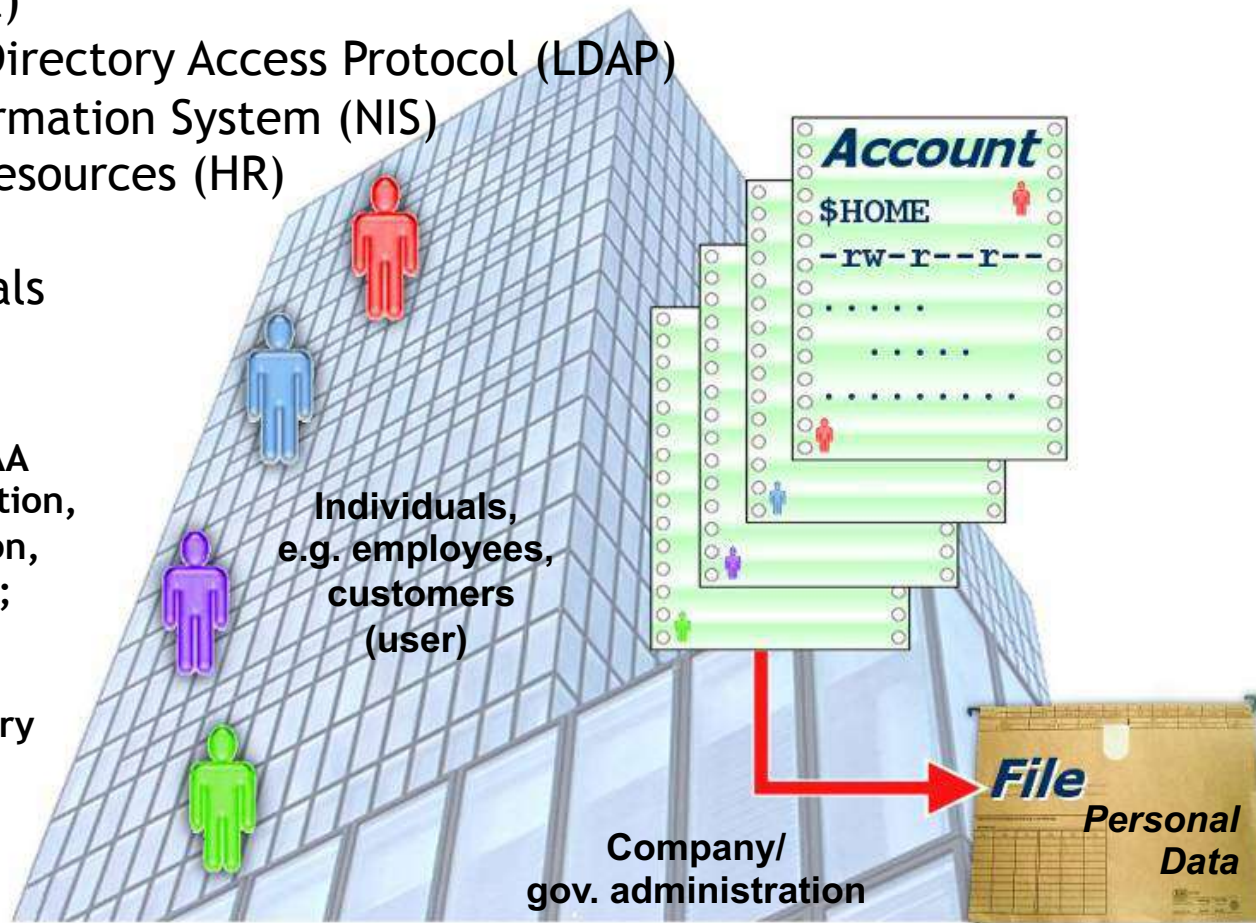
- Introduction
- Identity Concepts
- Identity Management
 - Functions
 - Systems
 - Types
 - Account Management
 - Single Sign On
 - Federated Identity Management
 - Profiling
 - Examples from CRM and the Internet
 - Dataveillance
 - Personal Identity Management
 - Communication Systems
 - Transaction Systems

Type 1: “Account Management”

- Identification and authentication (centralized storage of personal data)
- Lightweight Directory Access Protocol (LDAP)
- Network Information System (NIS)
- SAP Human Resources (HR)
- Groupware
- Intranet Portals

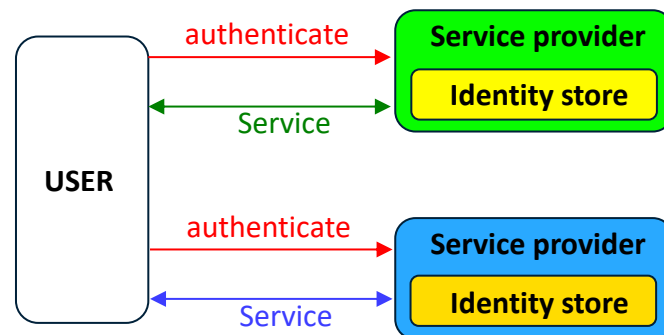
Purpose: AAA
(authentication,
authorisation,
accounting);

Means:
e.g. directory
services



[Hansen2005]


- Account provisioning
- Role & Policy Management
- Access Management
- Internal Single-Sign-On

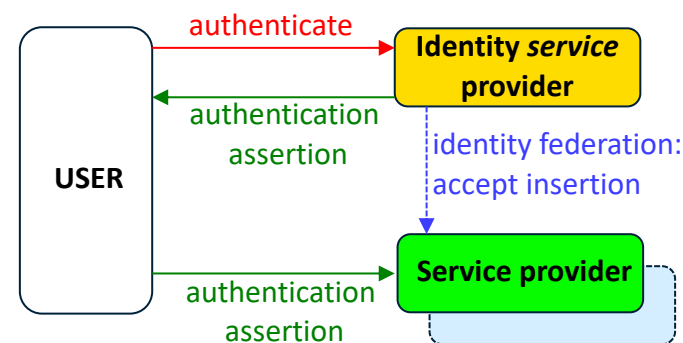


→ Authentication, Access Control


enterprise-wide infrastructure for
authentication and **authorization** and
accountability over full account live-cycle

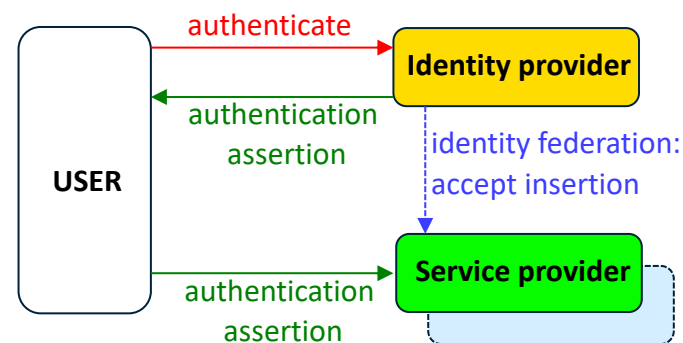
Federated Identity Management

- Inter-Company Single-Sign-On
- ‘Linking’ or ‘sharing’ of existing enterprise identities (accounts).
- The source party (identity provider) authenticates the user and vouches for the user to a relying party (service provider).
- Example:  OpenID
 - Decentralized web-based authentication system
 - 1 billion enabled user accounts (2014)
 - Accepted by more than 50.000 websites (2014)
 - Risks: Phishing, IdP masquerade, replay, DOS attacks



Federated Identity Management

- Inter-Company Single-Sign-On
- ‘Linking’ or ‘sharing’ of existing enterprise identities (accounts).
- The source party (identity service provider) asserts the authentication of the user and vouches for the user to a relying party (service provider).
- Example:  OpenID
 - Decentralized web-based authentication system
 - 1 billion enabled user accounts (2014)
 - Accepted by more than 50.000 websites (2014)
 - Risks: Phishing, IdP masquerade, replay, DOS attacks



Real World Examples 1

Identity at a Mobile Operator

- Mobile Network Operators already manage “identities”:
 - SIM = **Subscriber Identity* Module**
 - **≈7.9 billion SIM** subscribers (2016-09) (forecast to grow to **10 billion** by 2020)
 - More countries with SIM infrastructure (ca. 239, 2016-09) than McDonalds (118, 2016-09) and UN-members (193, 2016-0)
- **Relevance of identity management** grows
 - **Due to legal conditions** of location based services and the processing of personal data
 - “**Who** is allowed to localise **whom when** and **where?**”
- **Trusted party and intermediary role**
 - offers telecommunications providers new business opportunities
 - solves industry problems
 - minimising churn
 - price and tariff discrimination



** Note: In principle, SIM is related to identification.*

Real World Examples 2

Recent (Un)popular Approaches

- **Amazon (since 1994-07)**
 - 150 million paying prime users (4Q 2019)
- **eBay (since 1995-09)**
 - > 174 million active buyers (2Q 2020)
 - 25 million active sellers (2Q 2020)
 - Identity Change Management
- **Alibaba (1999-04)**
 - 726 million active online buyers (1Q 2020)
- **Microsoft Account (since 1999/07)**
 - Formerly known as Windows Live ID and Microsoft Passport
 - Early versions created much controversy
 - > 360 million registered [MS] participants
 - more or less active (> 1 billion authentications per day)



Real World Examples 3

Recent (Un)popular Approaches

- **Apple (since 2001)**
 - Devices/Services: 800 million unique users (2020)
 - Supported by iPhone spread
- **Google (since 2004)**
 - 1.5 billion monthly Gmail users (Q2 2020)
 - Started supporting OpenID in 2009-02
- **Facebook (since 2004-02)**
 - 2.6 billion monthly active users (Q2 2020)
- **Twitter (2006-03)**
 - 330 million monthly active users (Q1 2019)
 - 166 million monetizable daily active users: (Q1 2020)
- **Whatsapp (since 2009-02)**
 - 2 billion monthly active users (2020-04)



Real World Examples 4

Recent (Un)popular Approaches

- **Instagram (since 2010)**
 - > 1 billion monthly active users (Q2 2020)
- **WeChat (since 2011)**
 - > 1.2 billion monthly active users (Q1 2020)
- **Netflix (since 2007)**
 - 183 Million active subscribers (Q1 2020)



NETFLIX

PKI and Federated Identity

Idea:

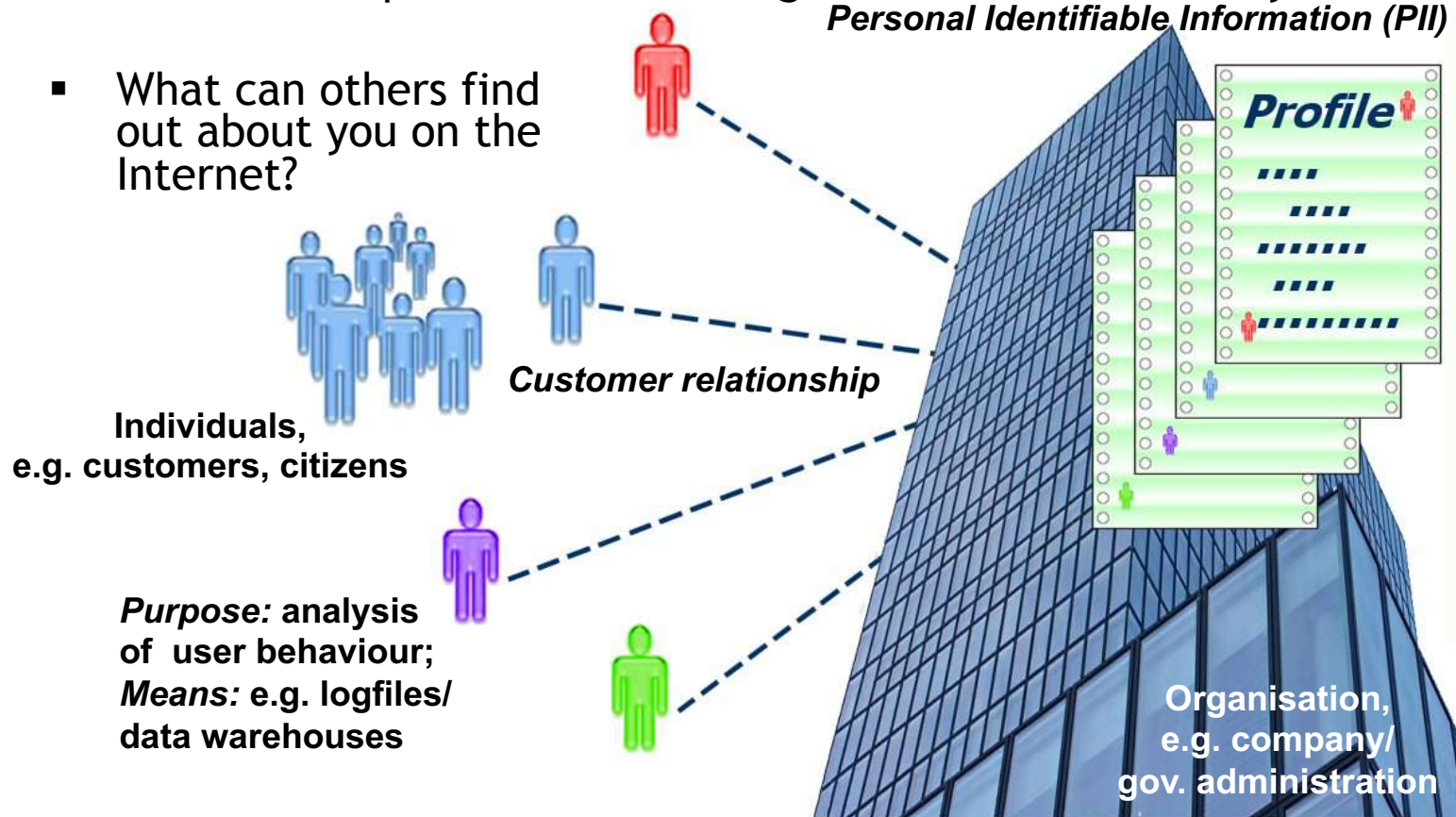
- Don 't do **strong authentication everywhere!**
- Get **strong authentication across domains** via federation within a particular user session.

Federation	PKI
Very good for assertions based on a recent/session authentication	Very good strong authenticator
Makes sense for re-use of authentication across multiple domains	Makes sense for secure access to a single domain
Most appropriate for internet-scale applications; high volume and dynamic infrastructure are considerations	Most often used to protect server-to-server or client-to-server conversations
Dynamic attribute support	Weak attribute sharing support
Enables dynamic partnering	Requires predetermined trust chains
Short-lived token	Persistent credentials

- Introduction
- Identity Concepts
- Identity Management
 - Functions
 - Systems
 - Types
 - Account Management
 - Single Sign On
 - Federated Identity Management
 - Profiling
 - Examples from CRM and the Internet
 - Dataveillance
 - Personal Identity Management
 - Communication Systems
 - Transaction Systems

Type 2: “Profiling”

- Analysis of virtual representations of a user
- What do companies and other organizations know about you?
Personal Identifiable Information (PII)
- What can others find out about you on the Internet?



- A Profile is is a type of knowledge consisting of patterns of correlated data and it is often built on data collected over a period of time.
- *Knowledge Discovery in Databases (KDD) can be applied to identity information*
 - **Step 1:** data collection; first level: physical
 - **Step 2:** data preparation; second level: empirical
 - **Step 3:** data mining; third level: syntactical
 - **Step 4:** interpretation; fourth level: semantic
 - **Step 5:** Determine actions; fifth level: pragmatic

[HilBac2005]

- *Purpose* is to discover potential
 - terrorists or criminals
 - insurance risks
 - new customers
 - potentially fraudulent employees
 - promising students
 - productive employees

all this is a **type of risk- or opportunity-assessment.**

Identity Management for customer loyalty

- Offering benefit for getting personal information from the customer (e.g. customer loyalty programs)
 - **Benefit:** Personalised promotions, general discounts, simplified service interaction etc.
 - **Personal information:** Preferences, socio-demographic data, service variables etc.
- Effort necessary for the customer results in **customer lock-in**.
- Users' input constitutes **switching costs** when changing to an alternative provider.
- Highly important in **electronic and mobile commercial settings** (competitors are not far away)
- May **decrease churn rates**
- Closer relation results in **higher value of the acquired customer** (for own or others' business purposes)



Example 2: Socio-demographics and milieus

Example of “Socio-demographical twins” shows the necessity of a different kind of segmentation model - the Sinus Milieus.

Typical Demographics of an “Established”

- Born 1948 and raised in Great Britain
- Married with two grown up kids
- Professionally successful
- Wealthy
- Leisure time spend in the Alps
- Likes dogs
- Famous and in the public eye



Prince Charles

Typical Demographics of an “Experimentalist”

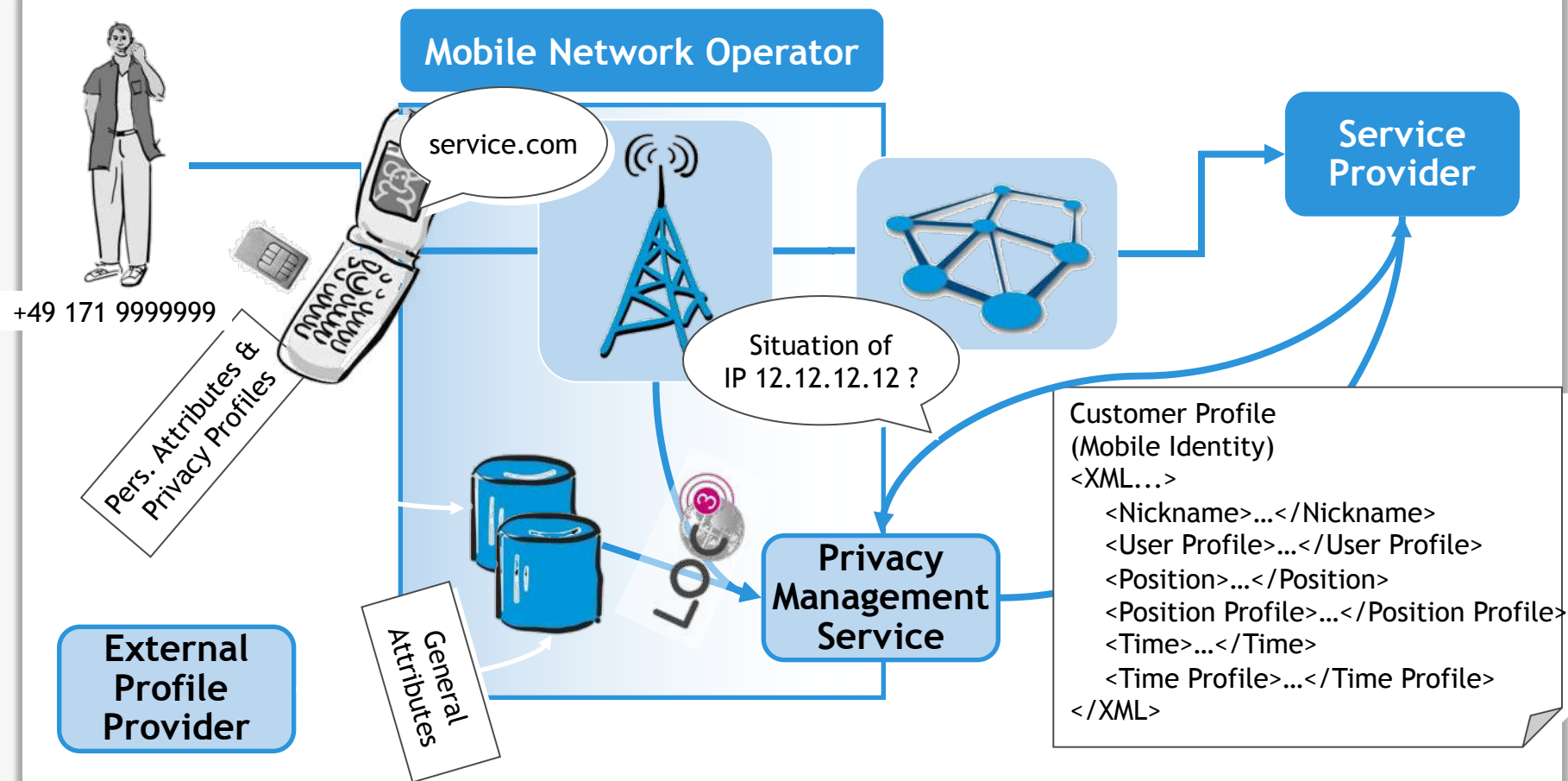
- Born 1948 and raised in Great Britain
- Married with two grown up kids
- Professionally successful
- Wealthy
- Leisure time spend in the Alps
- Likes dogs
- Famous and in the public eye



Ozzy Osbourne

[Deutsche Telekom 2005]

Example 3: Mobile (Digital) Identity



- Manual Profiling
 - www.google.com
- Automatic Profiling
 - www.zoominfo.com
- Deliberate Profiling
 - Networking Platforms e.g., www.xing.com
 - Job Exchange, Partner Search, e.g. love.com

André Deuker - Google-Suche - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://www.google.de/search?hl=de&q=Andr%C3%A9+Deuker&btnG=Google-Suche&meta=

Web [Bilder](#) [Maps](#) [News](#) [Shopping](#) [Mail](#) [Mehr ▼](#)

Google

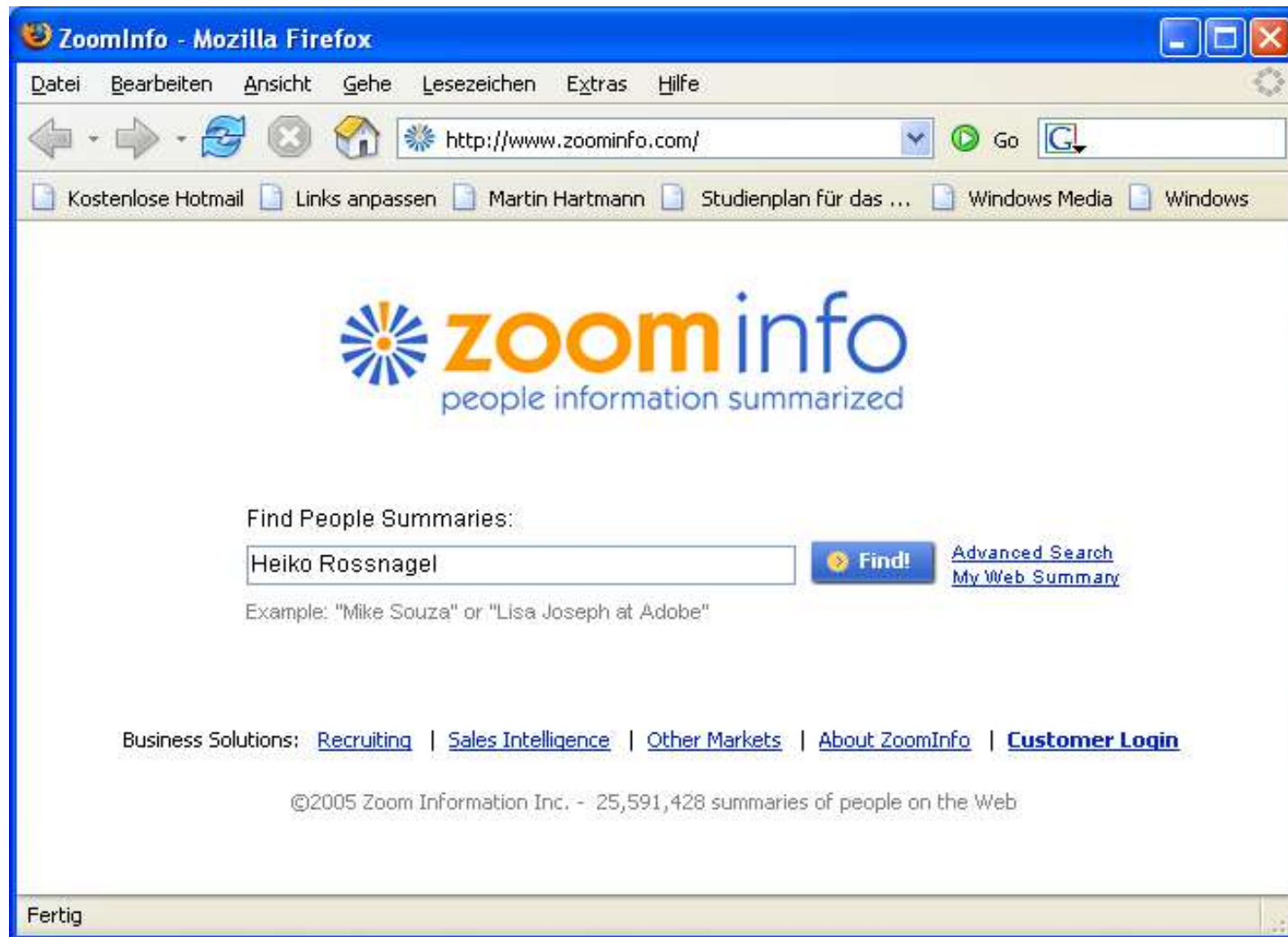
André Deuker [Erweiterte Suche](#)
[Einstellungen](#)

Suche: ☒ Das Web ☐ Seiten auf Deutsch ☐ Seiten aus Deutschland

Web Personalisiert Ergebnisse 1 - 10 von ungefähr 48.800 für **André Deuker**.

[André Deuker \(Professur f. BWL, insb. Wirtschaftsinformatik ...](#)
 Bild von **André Deuker ... Deuker, André**; Radmacher, Mike ... Royer, Denis; **Deuker, André** Komplexe Kommunikation - Der Einsatz von TYPO3 für ...
[www.whatismobile.de/personal/personaldetails.php?pernr=474](#) - 8k -
[Im Cache](#) - [Ähnliche Seiten](#) - [Notieren](#)

[Mike Radmacher \(Professur f. BWL, insb. Wirtschaftsinformatik ...](#)
Deuker, André; Radmacher, Mike Individualisierungsmöglichkeiten im Mobile TV - Ein werbebasierter Geschäftsmodellansatz In: Proceedings der 3. ...
[www.whatismobile.de/personal/personaldetails.php?pernr=465](#) - 19k -
[Im Cache](#) - [Ähnliche Seiten](#) - [Notieren](#)
[Weitere Ergebnisse von www.whatismobile.de »](#)



[My Network](#)
[Jobs and Careers](#)
[Groups](#)
[Events](#)
[Companies](#)

Basic

Premium benefits

-
-
-
-
-
-
-
-

[Activity](#)
[Business details](#)
[Contacts \(247\)](#)

Prof. Dr. Kai Rannenberg

Dr. rer. pol., Diplom-Informatiker

Professor, Department Director
Goethe University Frankfurt Chair for Mobile Business & Multilateral Security

60629 Frankfurt
Germany (Map)

▼ My notes and categories (tags) for Prof. Dr. Kai Rannenberg

About me

<http://www.m-chair.net>

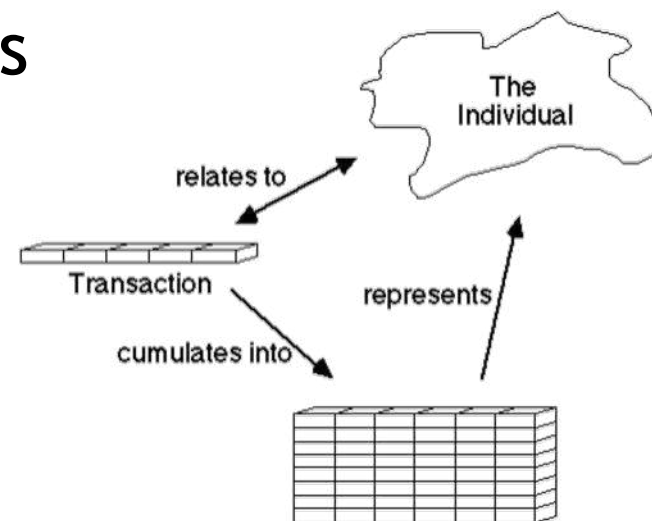
> more

Personal information

Organizations

GI, ACM, CEPIS LSI, IFIP TC 11 "Security and Privacy Protection in Information Processing Systems", IFIP WG 11.4 "Network & Distributed Systems Security", IFIP WG 11.6 "Identity Management", IFIP WG 9.6/11.7 "IT Misuse and the Law", IFIP WG 6.11 "Electronic Commerce - Communication Systems", ISO/IEC JTC 1/SC 27/WG 3 "IT Security Evaluation Criteria", ISO/IEC JTC 1/SC 27/WG 5 "Identity Management and Privacy Technologies", DIN-NI 27 "IT-Sicherheitsverfahren", ENISA Management Board

- Personal dataveillance
 - low data quality decisions
 - lack of subject knowledge of, and consent to, data flows
 - blacklisting and denial of redemption
- Mass dataveillance
 - dangers to individuals
 - dangers to society



[Clarke1994]

- Arbitrariness
- A contextual data merger
- Complexity and incomprehensibility of data
- Witch hunts
- Ex-ante discrimination and guilt prediction
- Inversion of the onus of proof
- Covert operations
- Unknown accusations and accusers and denial of due process

- Prevailing climate of suspicion
- Adversarial relationships
- Focus of law enforcement on easily detectable and provable offences
- Inequitable application of the law
- Decreased respect for the law and law enforcers
- Reduction in the meaningfulness of individual actions

- Reduction in self-reliance and self-determination
- Stultification of originality
- Increased tendency to opt out of the official level of society
- Weakening of society's moral fibre and cohesion
- Destabilisation of the strategic balance of power
- Repressive potential for a totalitarian government

You would like to know more about your data?

- For further examples, the following reality documentation might be of interest for you: “Wer hat meine Daten”.
- Excerpt: “Einige Dinge darf jeder wissen: Geburtstag, Wohnort und Beruf beispielsweise. Doch darüber hinaus sind von jedem von uns hunderte von Daten im Umlauf.

Jeder Kauf mit Kundenkarte, jeder Besuch auf Internetseiten hinterlässt Spuren, die von Datenhändlern begierig gesammelt, ausgewertet und verkauft werden. Vorlieben, Leidenschaften, selbst geheime Wünsche von jedem von uns werden gespeichert und in Umlauf gebracht, zu Nutzerprofilen zusammengefasst und transparent gemacht.”

- Introduction
- Identity Concepts
- Identity Management
 - Functions
 - Systems
 - Types
 - Account Management
 - Single Sign On
 - Federated Identity Management
 - Profiling
 - Examples from CRM and the Internet
 - Dataveillance
 - Personal Identity Management
 - Communication Systems
 - Transaction Systems

Personal Identity Management (Example ABC4Trust)

- Please watch the video linked below.
- <https://www.youtube.com/watch?v=utk4EyoaxAk>

- [ABC4TrustYoutube] <https://www.youtube.com/watch?v=utk4EyoaxAk>
- [BaMeHa2005] Martin Bauer, Martin Meints, Marit Hansen (eds.) (2005) FIDIS Deliverable D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems, <http://www.fidis.net/resources/deliverables/hightechid/#c1787>
- [BogBes2001] Bogdanowicz, Marc and Beslay, Laurent: Cyber-Security and the Future of Identity, IPTS Report 57, 2001, www.jrc.es/home/report/english/articles/vol57/ICT4E576.htm, available via <https://web.archive.org>
- [Clarke1994] Roger Clarke: The Digital Persona and its Application to Data Surveillance, Information Society 10(2), 1994, <http://www.rogerclarke.com/DV/DigPersona.html>
- [Durand2003] Andre Durand, Three Phases of Identity Infrastructure Adoption, <http://blog.andredurand.com/?p=146>
- [Durand2004] Andre Durand, Federated Identity & PKI Collide, <http://www.andredurand.com/?p=205>
- [Hansen2005] Marit Hansen, PRIME & FIDIS: European Projects on Identity and Identity Management, <http://www.digimagine.de/Hansen-Idmanage-20050308-print.ppt>, accessed 2007-03-02.
- [HilBac2005] Mireille Hildebrandt, James Backhouse (eds.) (2005) FIDIS Deliverable D7.2: Descriptive analysis and inventory of profiling practices, <http://www.fidis.net/resources/fidis-deliverables/profiling/#c1764>
- [Hübner2004] Uwe Hübner, Föderiertes Identitätsmanagement, TU Chemnitz, <http://monarch.qucosa.de/fileadmin/data/qucosa/documents/4802/data/index.htm>
- [ISO/IEC 24760-1:2019] Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts; <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>
- [PRIME2006] PRIME: General Public Tutorial; <https://www.prime-project.eu/tutorials/gpto/>
- [Rannenber2004] Kai Rannenber: Identity management in mobile cellular networks and related applications; Information Security Technical Report; Vol. 9, No. 1; 2004; pp. 77-85; ISSN 1363-4127
- [SchKoß2006] Erich Schütz, Detlev Koßmann, SWR: Wer hat meine Daten - Wie wir täglich ausgespäht werden, Südwestrundfunk, 2006-03-20, available via e.g. Youtube
- [Sun2012] Sun, S. T., Hawkey, K., & Beznosov, K. (2012). Systematically breaking and fixing OpenID security: Formal analysis, semi-automated empirical evaluation, and practical countermeasures. Computers & Security, 31(4), 465-483.