

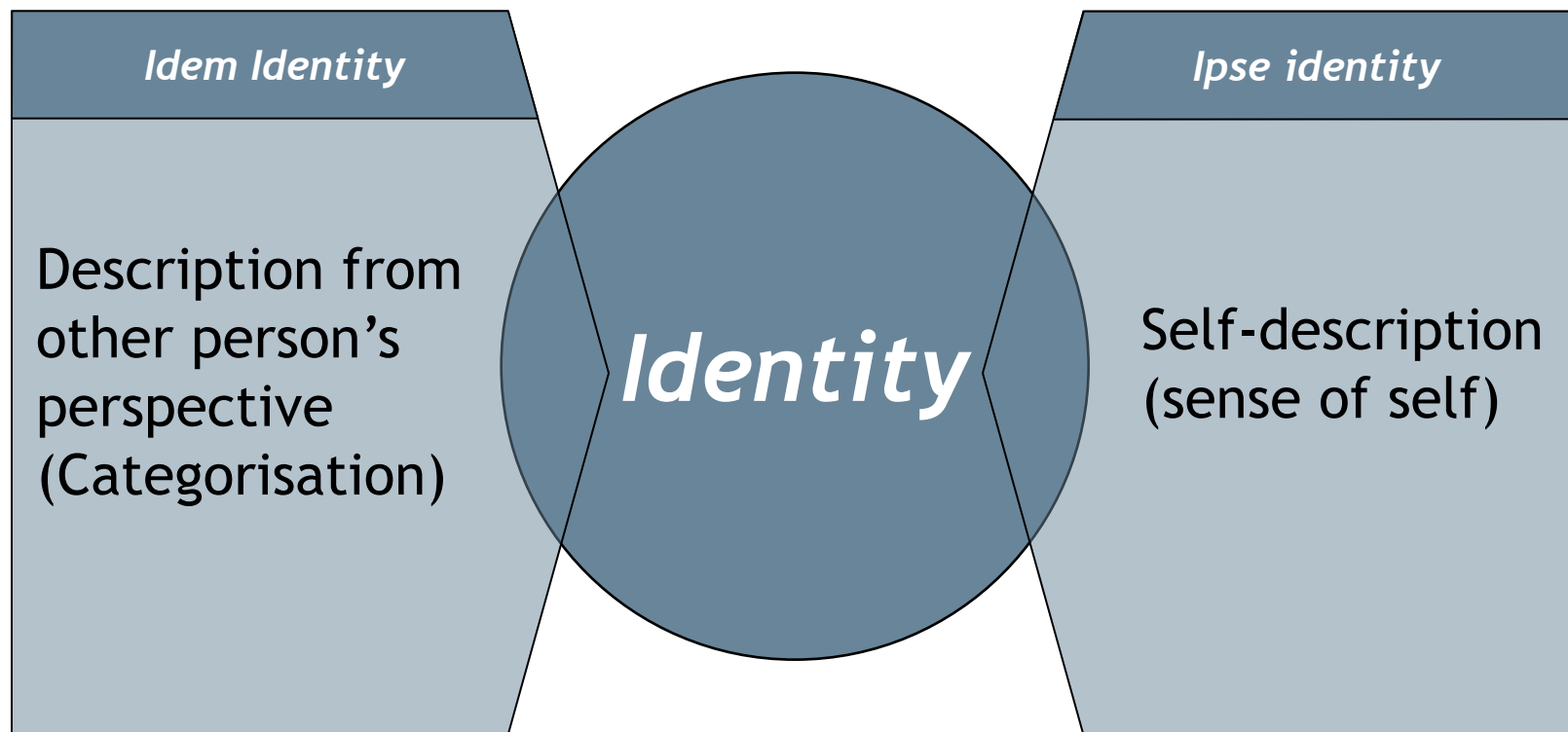
Information & Communication Security (SS 15)

Identity Management

Dr. Jetzabel Serna-Olvera
@sernaolverajm

Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

- Identity
 - Different Views of Identity
 - Working Definitions
- Digital Identities
- Identity Management
 - Account Management
 - Profiling
 - Personal Identity Management



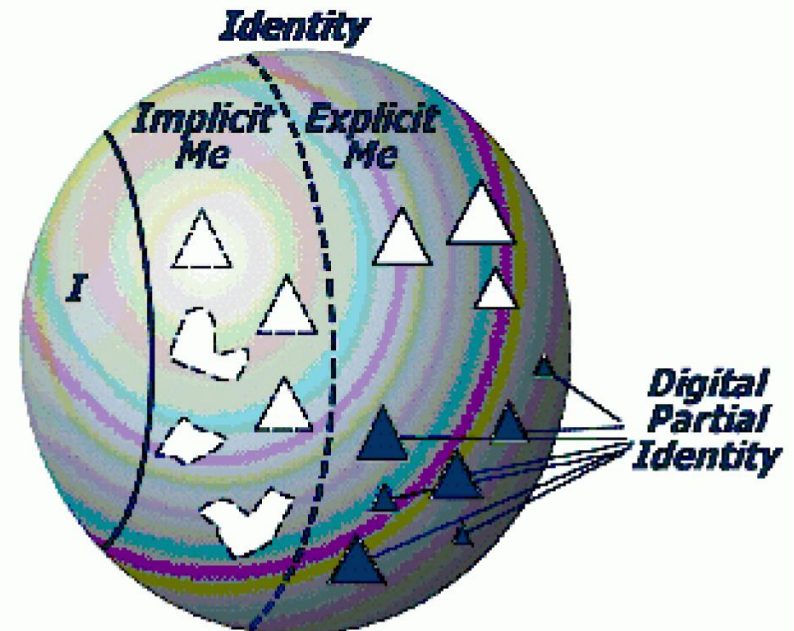
- **Mental identity** (ipse, I)
 - Researched by social/psychological sciences
 - Dynamically changing configuration reflecting, and shaped by, interactions between an individual and its environment
 - Private and endless task to go deeply in ones' own description:
 - “Only I can be responsible for acts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

- *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.*

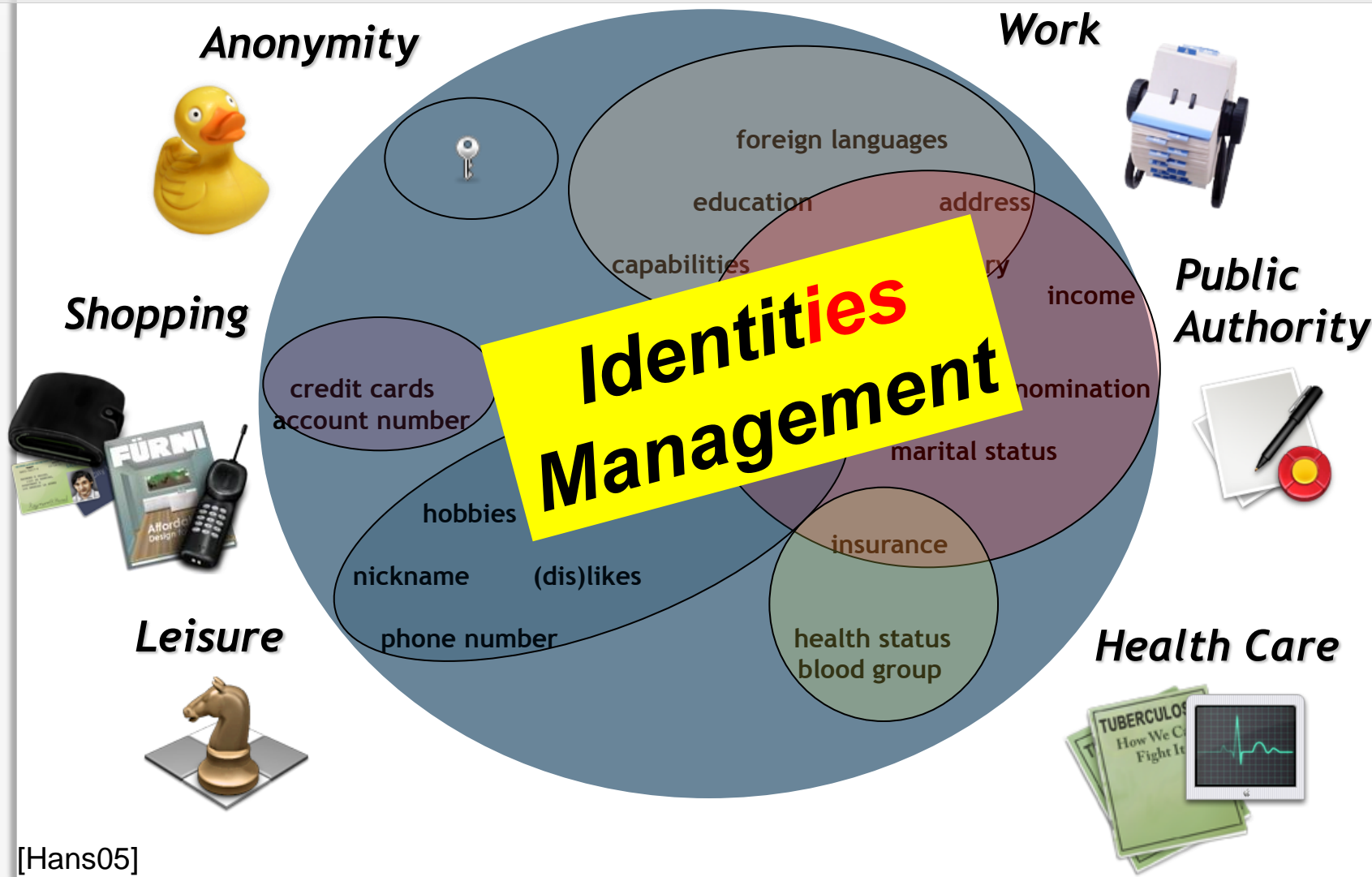
- A Tier 2 (assigned - ‘Our’) identity refers to our digital identities that are assigned to us by corporations (e.g. our ‘customer accounts’).
 - *Our* job title (assigned to us by our employer)
 - *Our* cell phone number (assigned to us by our mobile phone operator)
 - *Our* United Mileage Plus number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

- 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.

- ***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**

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 | 2



- Identity
 - Different Views of Identity
 - Working Definitions
- Digital Identities
- Identity Management
 - Account Management
 - Profiling
 - Personal Identity Management



- Types
 - **Partial Identities** : set of attributes of an identity of a subject or person
 - **Pseudonymous Identities**: separates a digital identity from its real-world identity but linking is possible
 - **Anonymous Identities**: cannot be linked in any way to its real-world identity
- Domains
 - Local (e.g. windows user)
 - Global (e.g. passport)
 - *Federated: links user credentials across multiple systems and services*

- Identity
 - Different Views of Identity
 - Working Definitions
- Digital Identities
- Identity Management
 - 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.

- **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, 2ndLife 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

- **Identity Federation:** allows the end users **to use the same set of credentials** to obtain access to multiple resources.
- **Single Sign On (SSO):** allow a **single user authentication process** across multiple applications, IT systems or even organizations. Users **provide their credentials once** and obtain access to multiple resources.

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

- 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

[Fidis2005, Rannenber 2004]

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

[BaMe05]

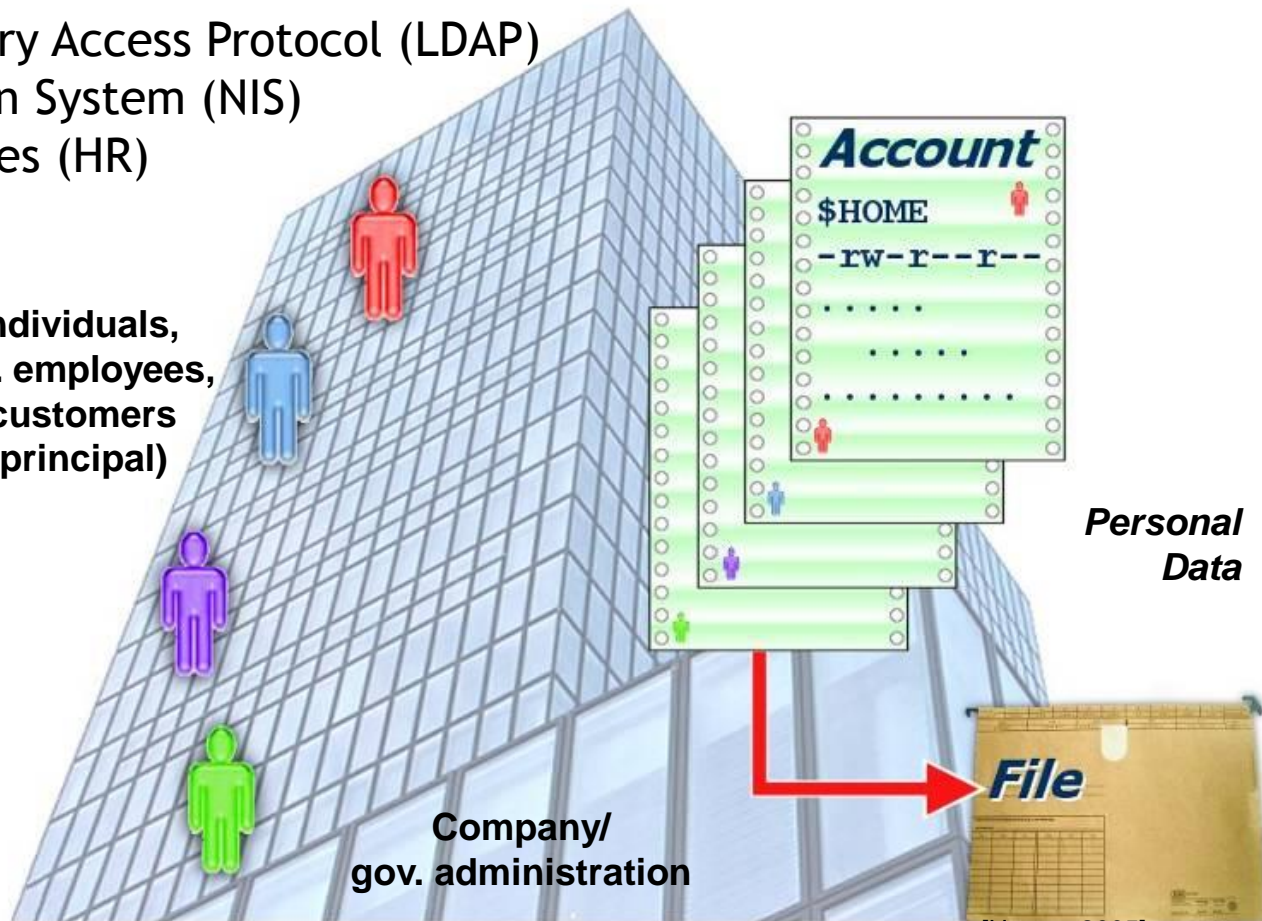
Type 1: "Account Management"

- 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);

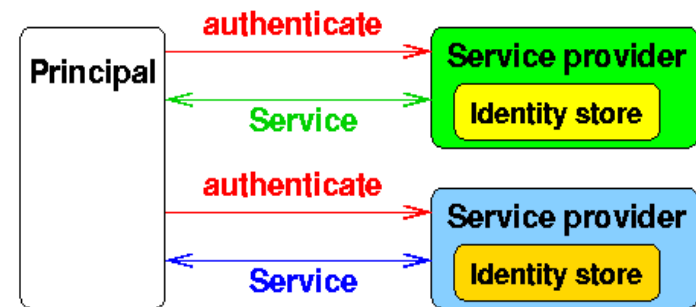
Means:
e.g. directory
services

Individuals,
e.g. employees,
customers
(principal)



[Hansen2005]

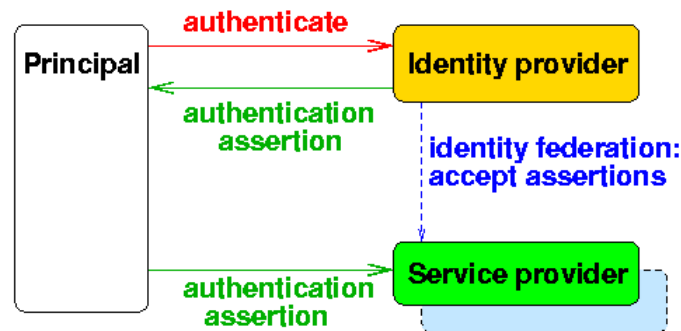
- Account provisioning
- Role & Policy Management
- Access Management
- Internal Single-Sign-On



→ Authentication, Access Control

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

- 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).



- Mobile Network Operators already manage “identities”:
 - SIM = **Subscriber Identity Module**
 - **7 billion SIM** subscribers (2014-04)
 - More countries with SIM infrastructure (ca. 220, 2014) than McDonalds (118, 2014) and UN-members (193, 2014-11)
- **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

Real World Examples II

Recent (Un)popular Approaches

- **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)
- **eBay (since 1995-09)**
 - > 150 million active buyers (3Q 2014)
 - 25 million active sellers (3Q 2014)
 - Identity Change Management
- **Facebook (since 2004-02)**
 - 1.23 billion users (2014-02)
- **Google (since 2004)**
 - 425 million Gmail users (2012-06)
 - Started supporting OpenID in 2009-02
- **Apple (since 2001)**
 - iTunes: 800 million accounts (2014-04)
 - Supported by iPhone spread

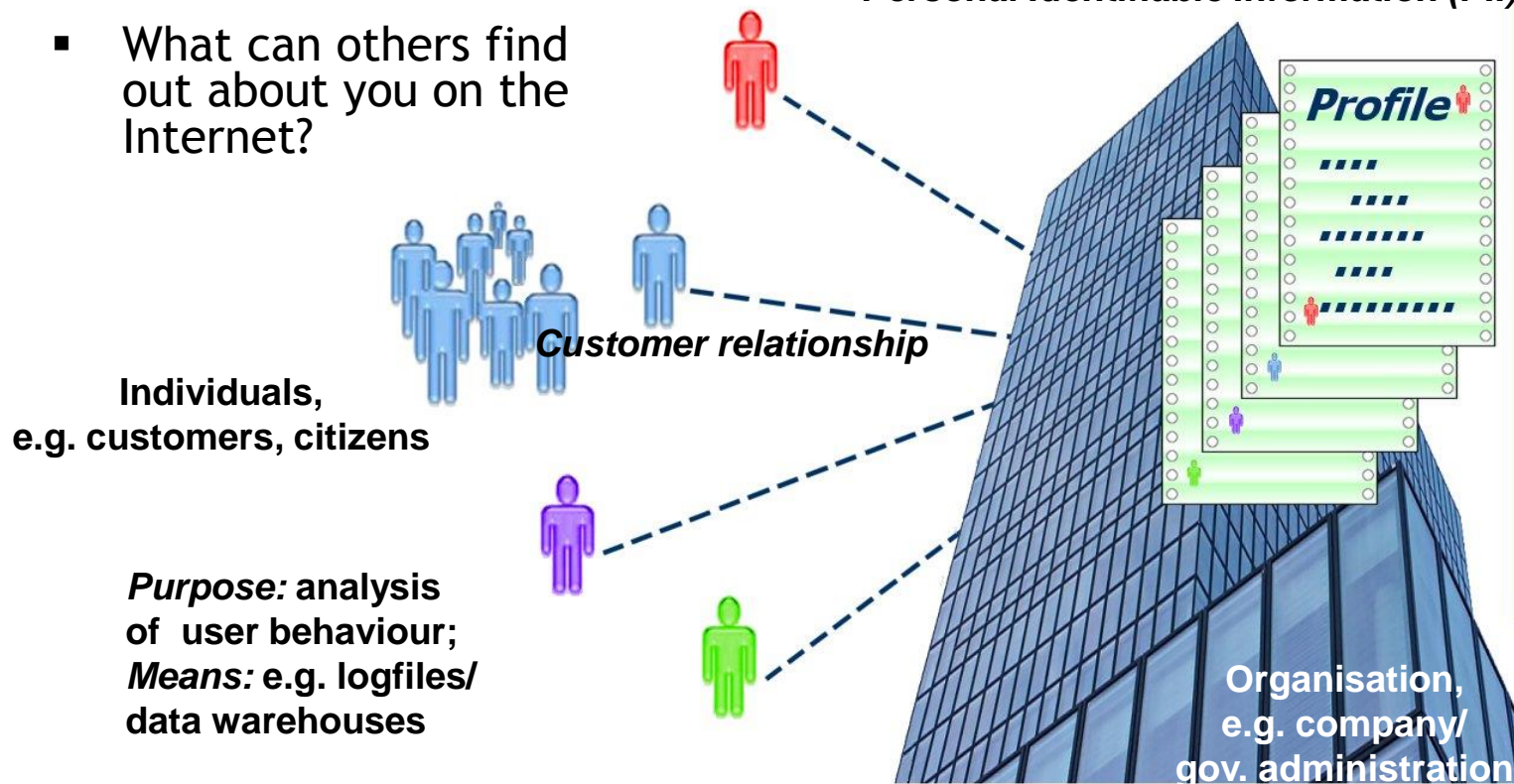


- Identity
 - Different Views of Identity
 - Working Definitions
- Digital Identities
- Identity Management
 - Account Management
 - Profiling
 - Personal Identity Management

Type 2: "Profiling"

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

Personal Identifiable Information (PII)



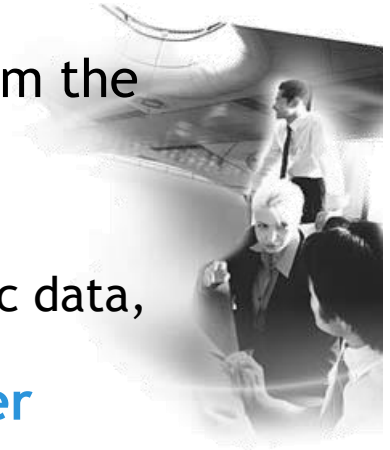
- A Profile is a type of knowledge consisting of patterns of correlated data and it is often built on data collected over a period of time.
- *Knowledge Discovery in Databases (KDD) can be applied to identity information*
 - **Step 1:** data collection; first level: physical
 - **Step 2:** data preparation;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

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

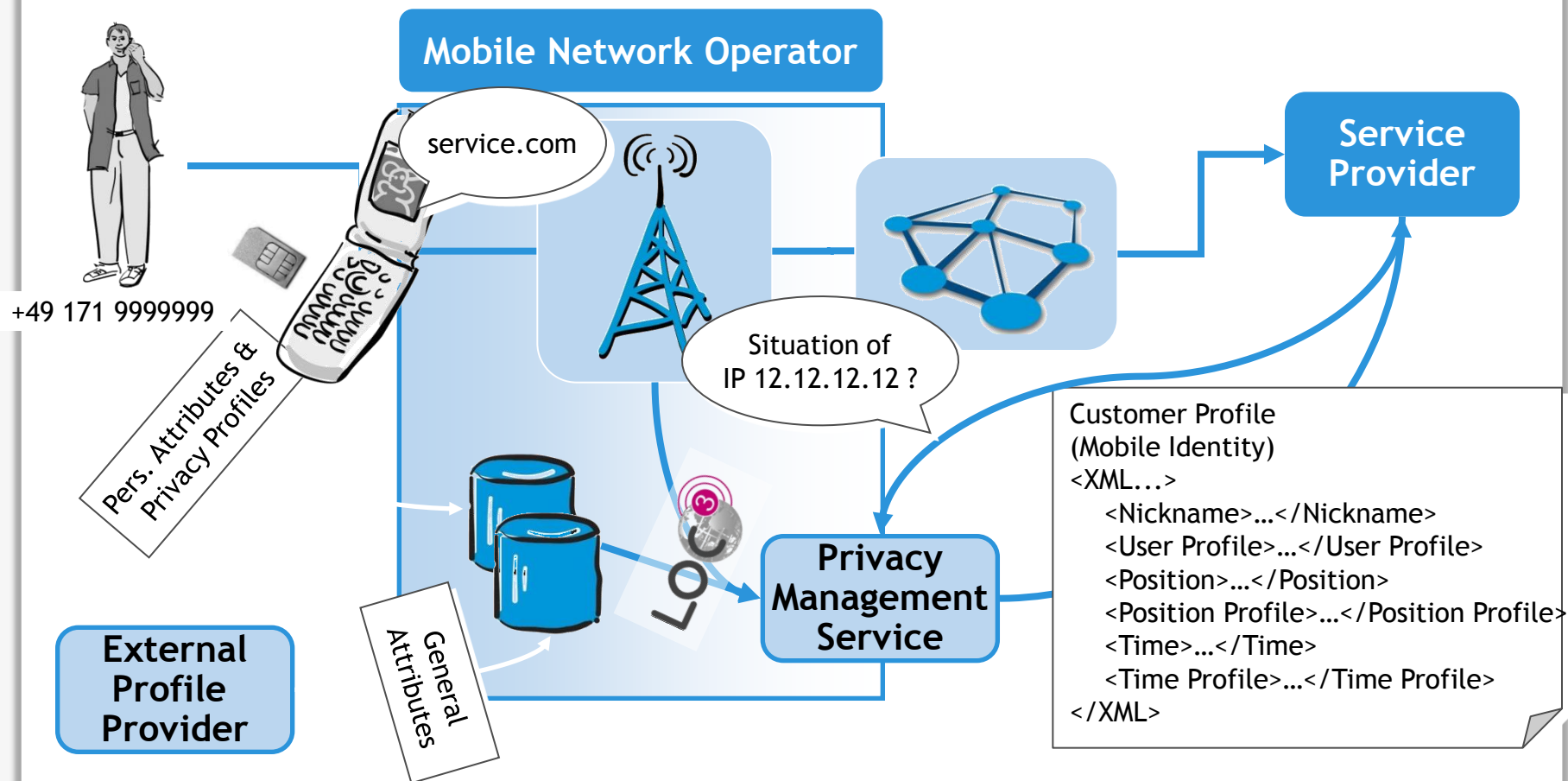
all this is a **type of risk- or opportunity-assessment.**

Example 1: 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: 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](#) »

ZoomInfo - Mozilla Firefox

Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe

http://www.zoominfo.com/ Go

Kostenlose Hotmail Links anpassen Martin Hartmann Studienplan für das ... Windows Media Windows

 **zoominfo**
people information summarized

Find People Summaries:

[Find!](#) [Advanced Search](#)
[My Web Summary](#)

Example: "Mike Souza" or "Lisa Joseph at Adobe"

Business Solutions: [Recruiting](#) | [Sales Intelligence](#) | [Other Markets](#) | [About ZoomInfo](#) | [Customer Login](#)

©2005 Zoom Information Inc. - 25,591,428 summaries of people on the Web

Fertig

XING 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

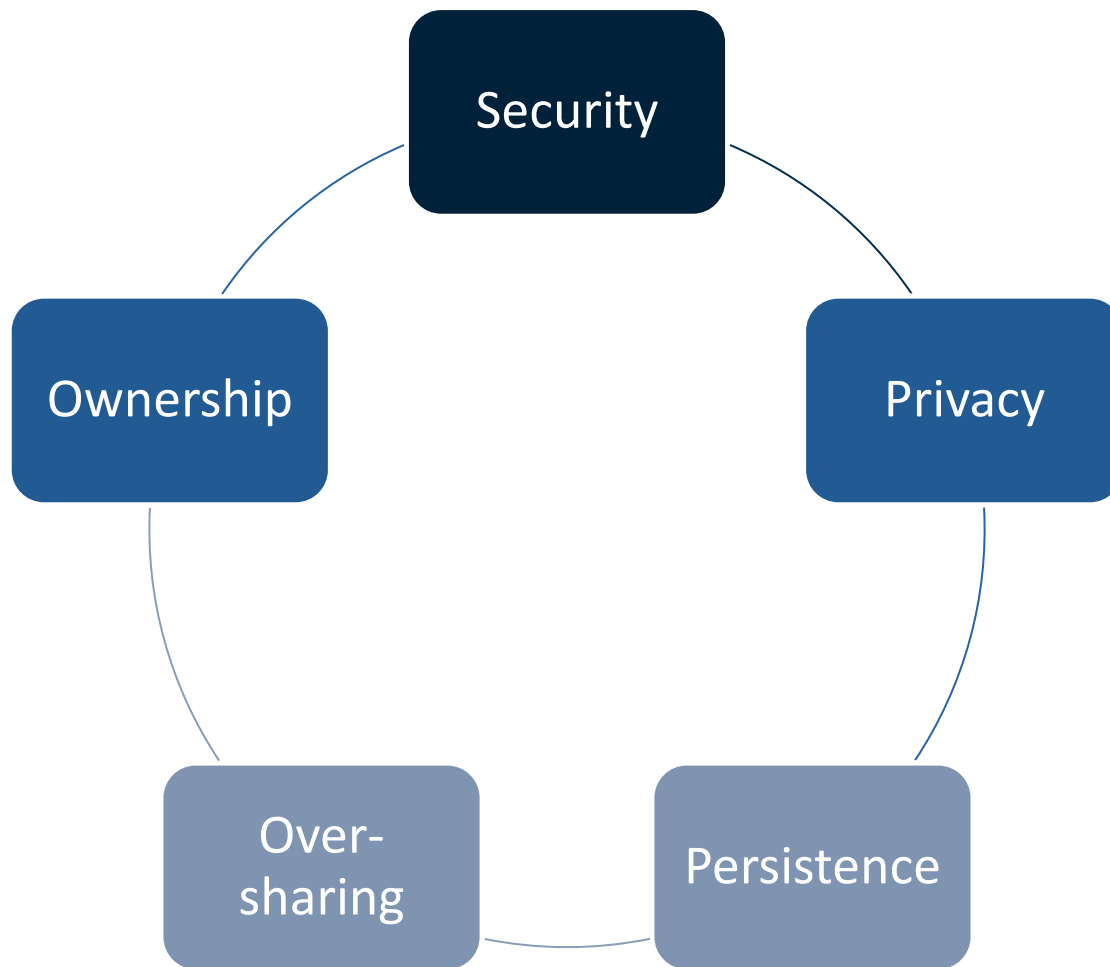
<http://www.m-chair.net>

> 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



- [BogLau2001] Cyber-Security and the Future of Identity, IPTS Report 57,
<http://www.jrc.es/pages/iptsreport/vol57/english/ICT4E576.htm>
- [SchCor1996] Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM, 1996
- [HanPfi2004] Marit Hansen, Andreas Pfitzmann, Anonymity, Unobservability, Pseudonymity, and Identity Management - A Proposal for Terminology,
http://dud.inf.tu-dresden.de/Literatur_V1.shtml
- [Durand2003] Andre Durand, Three Phases of Identity Infrastructure Adoption,
[http://discuss.andredurand.com/stories/storyReader\\$343](http://discuss.andredurand.com/stories/storyReader$343)
- [Durand2004] Andre Durand, Federated Identity & PKI Collide,
<http://discuss.andredurand.com/2004/09/17#a430>
- [Fidis2005a] WP3, Structured Overview on Prototypes and Concepts of Identity Management Systems, <http://www.fidis.net/293.0.html>
- [Hansen2005] Marit Hansen, PRIME & FIDIS: European Projects on Identity and Identity Management, <http://www.digimagine.de/Hansen-ldmanage-20050308-print.ppt>
- [Hübner2004] Uwe Hübner, Föderiertes Identitätsmanagement, TU Chemnitz, <http://archiv.tu-chemnitz.de/pub/2004/0042/data/>
- [Fidis2005b] WP7, Inventory of actual profiling practices and techniques, to be published 2nd Qt. 2005
- [Clarke1994] Roger Clarke , The Digital Persona and its Application to Data Surveillance, Information Society 10(2), 1994,
<http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html>
- [SchKob2006] Erich Schütz, Koßmann Detlev, SWR, Wer hat meine Daten - Wie wir täglich ausgespäht werden, 2006, <http://www.swr.de/betrifft/2006/03/20/>



Deutsche Telekom Chair of Mobile Business & Multilateral Security

Dr. Jetzabel M. Serna-Olvera

Goethe University Frankfurt

E-Mail: Jetzabel.Serna-Olvera@m-chair.de

WWW: www.m-chair.de