

Privacy vs. Data: Business Models in the digital, mobile Economy

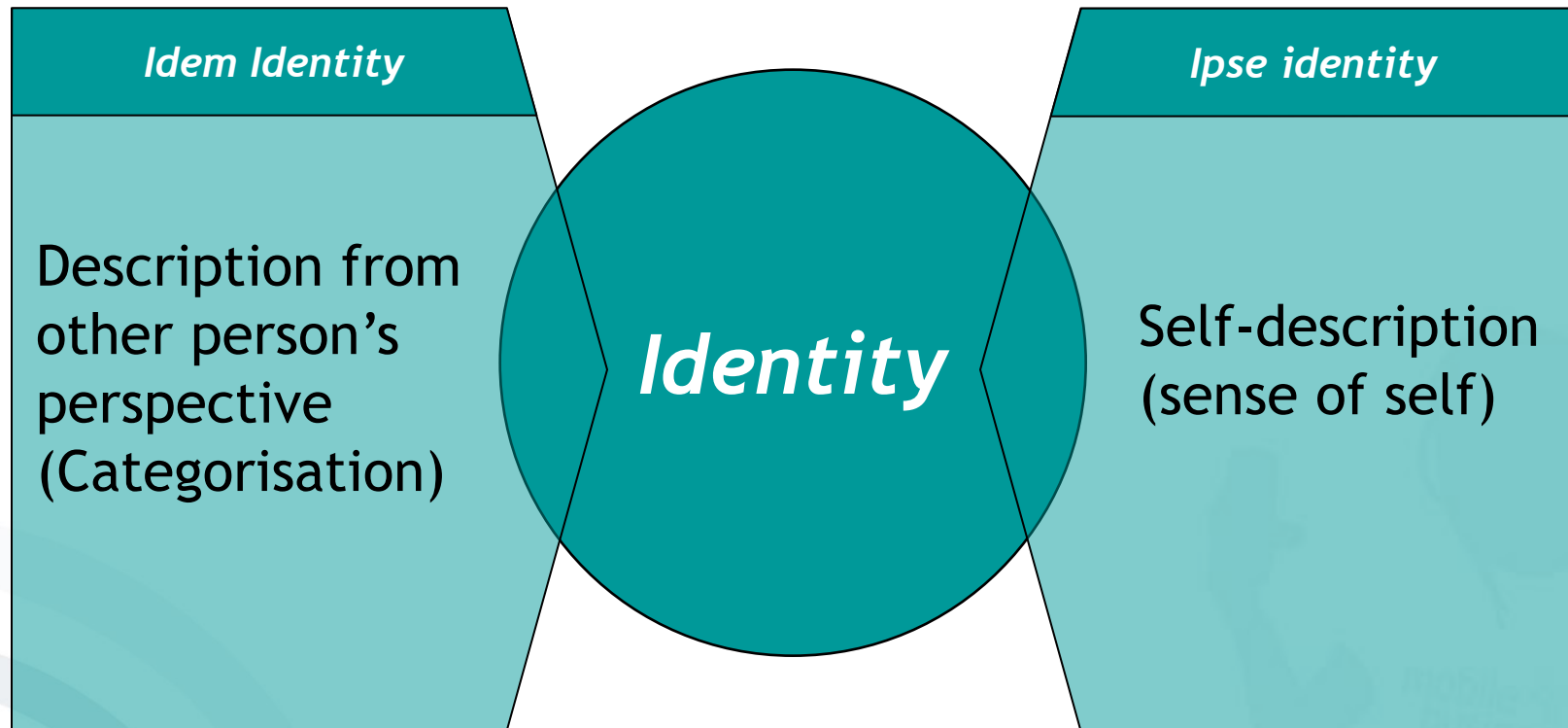
Lecture 11 (Mobile) Identity Management

WS 2011/2012

Dr. Andreas Albers
www.m-chair.net



- The Identity Concept
- Digital Identities
- Identity Management and Identity Management Systems
- Mobile Devices as Digital Identities
- Identity Threats



- **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.”

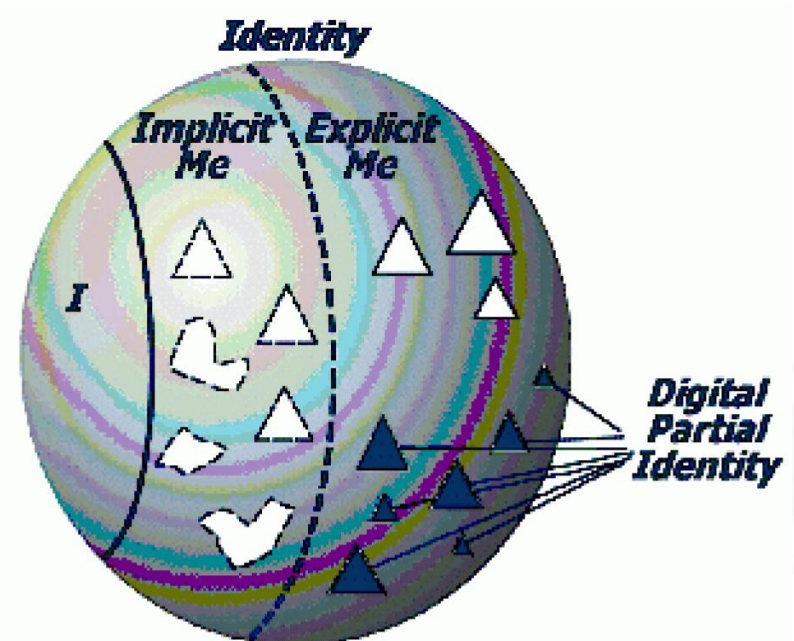
Source: Bogdanowicz and Beslay (2001)

- **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.

Source: Bogdanowicz and Beslay (2001)

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

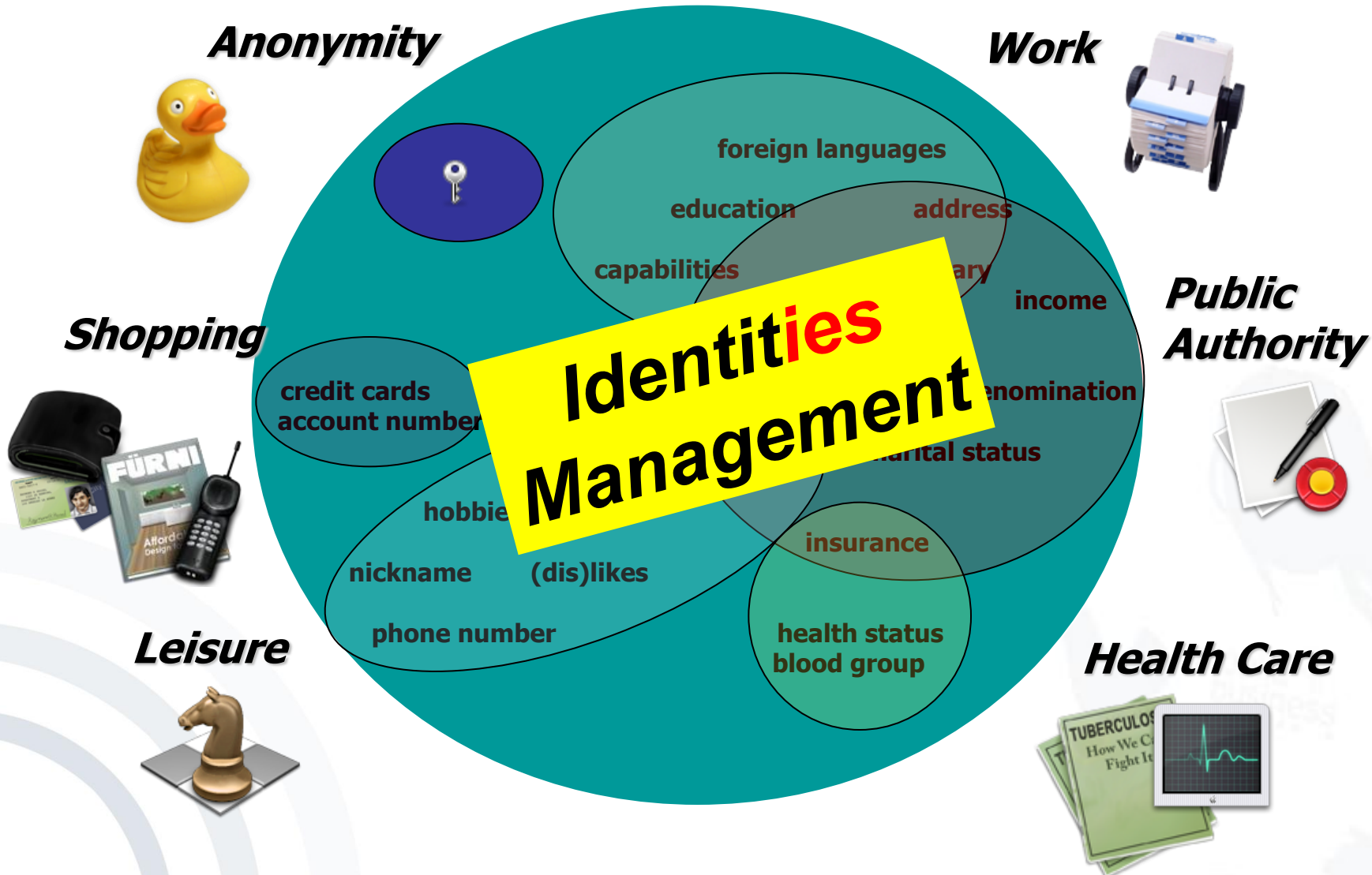


- ***Identity:***
The characteristics (attributes) representing an acting entity
- ***Partial identity:***
A subset of the characteristics of an identity

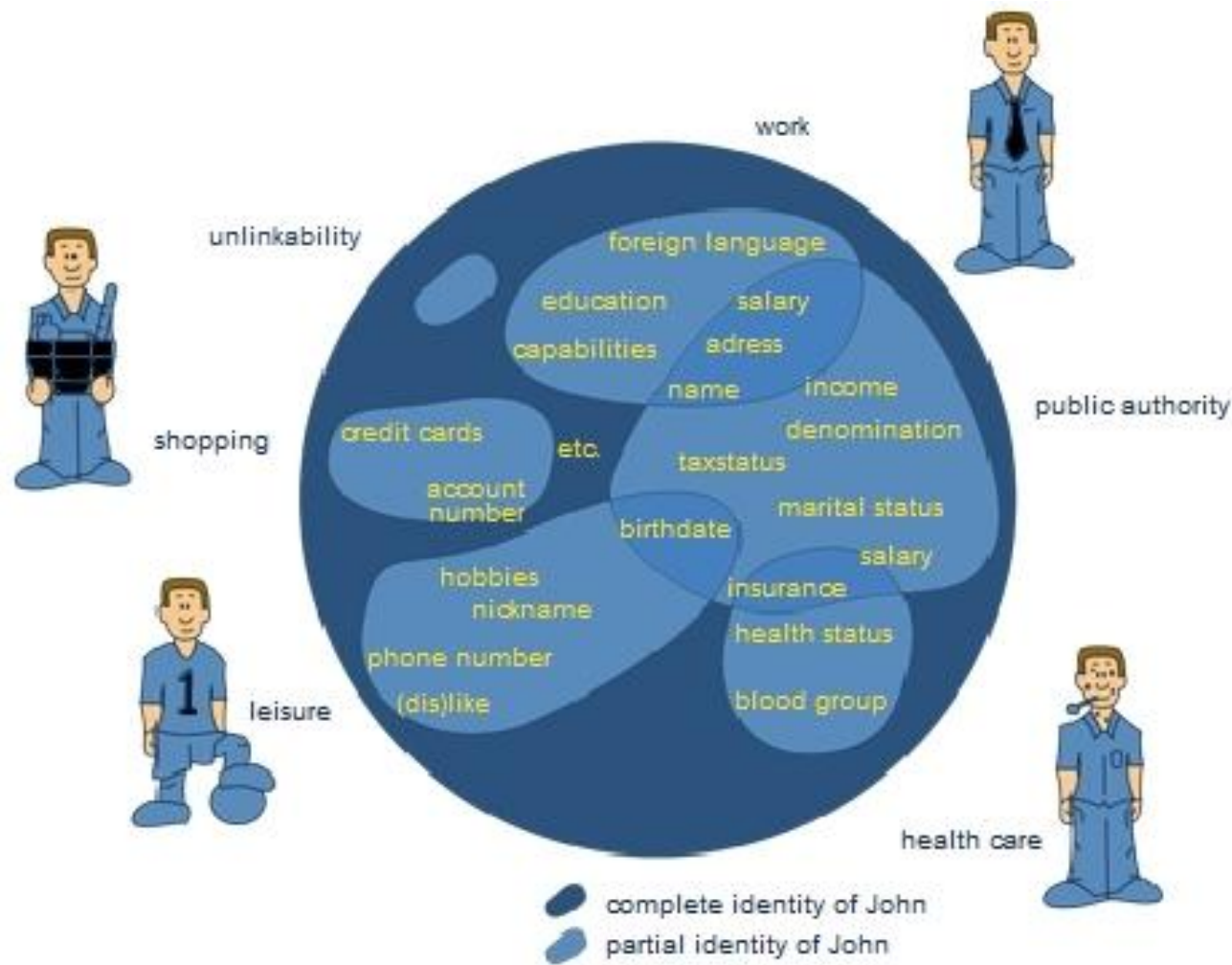
Why are partial identities important ?

- 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.

Source: Bauer and Meints (2005)



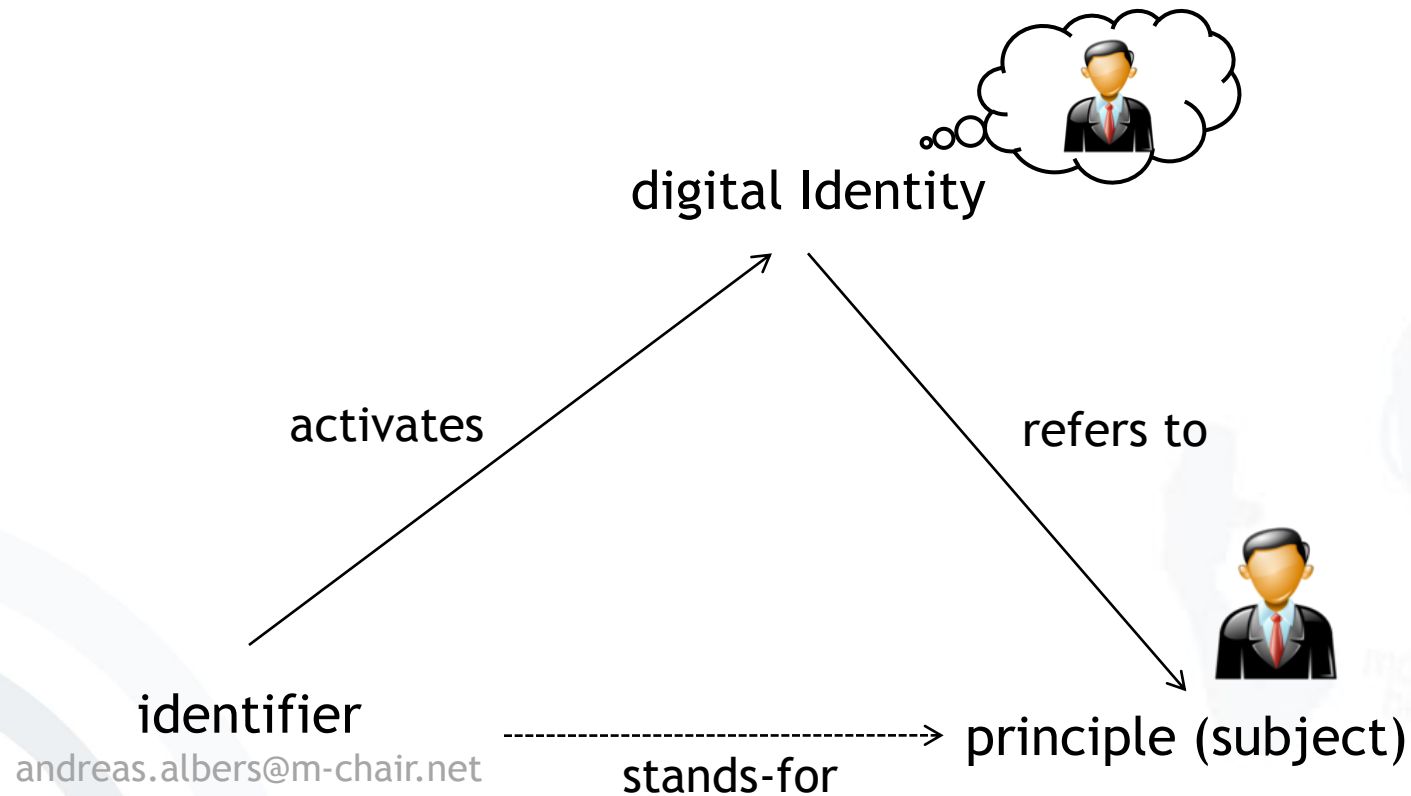
Identity Concepts: Partial Identities Illustrated (2)



Source: PRIME – General Public Tutorial

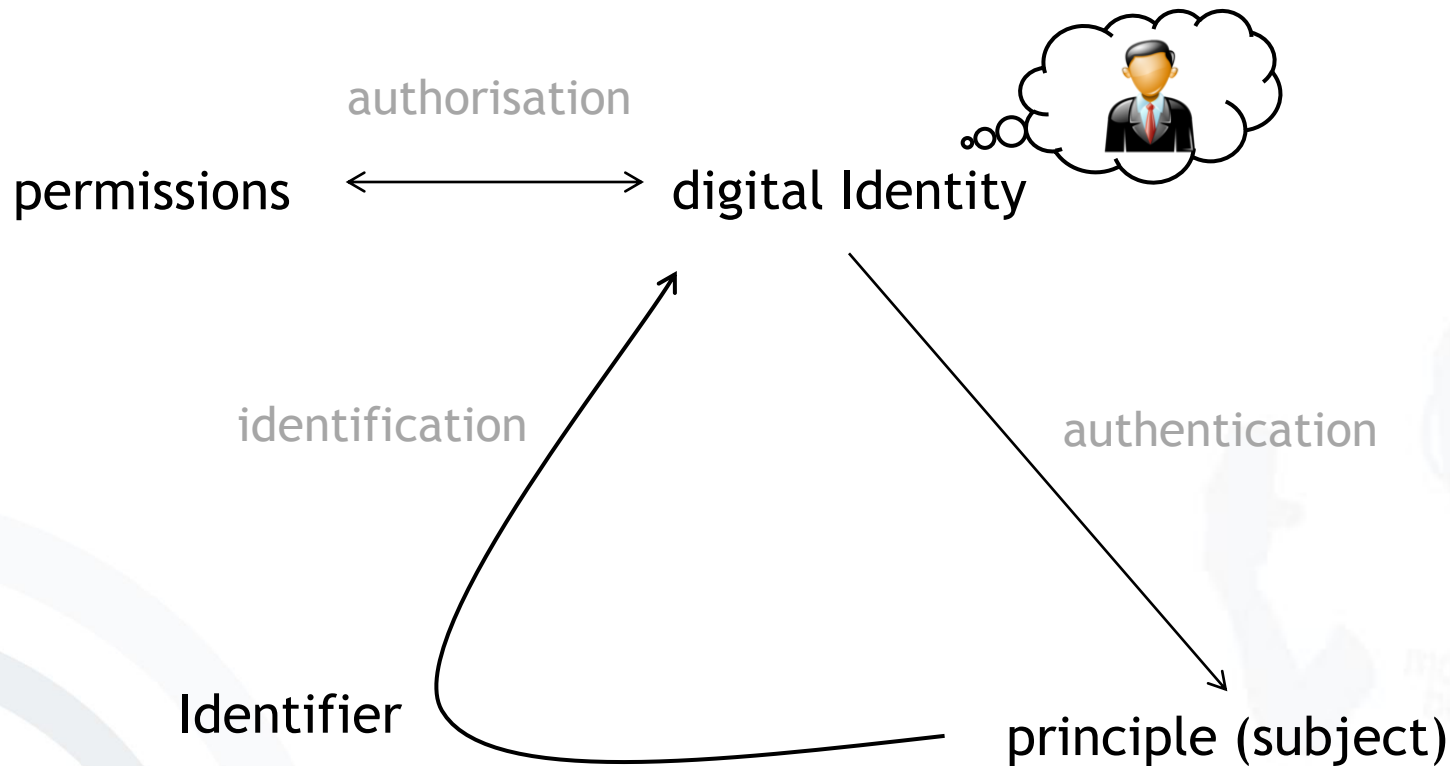
- The Identity Concept
- Digital Identities
- Identity Management and Identity Management Systems
- Mobile Devices as Digital Identities
- Identity Threats

▪ Digital Identity Triangle



Source: GINI (2011)

- Identification, Authentication, Authorization



Source: GINI (2011)

- Identification
 - The association between a personal characteristic and a subject representing various attributes (e.g. “Andreas Albers” identifies the person “Andreas Albers”)
- Authentication
 - The process of verifying a subject’s identity or other claim, e.g. one or more attributes.
- Authorisation
 - Through authorisation, rights are assigned to a digital identity.
- Identification without Authentication
 - E.g. subject is processing data that is linked to a different individual than the subject (e.g. a physician processing a patient’s identity data)
- Authentication without Identification
 - Anonymous credentials (e.g. verifying to be at least 18 years old without disclosing other attributes such as name and address).

Source: GINI (2011)

- The Identity Concept
- Digital Identities
- Identity Management and Identity Management Systems
- Mobile Devices as Digital Identities
- Identity Threats

Identity Management (IdM) is often used as a *buzz word* that can have many meanings such as:

- The management of accounts for employees, customers or citizens. These accounts contain those parts of an identity relevant for an organization (attributes, access rights, roles, ...) → Trend towards federations between organisations
- 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 → To build a ‘healthy’ virtual socio-psychological identity.

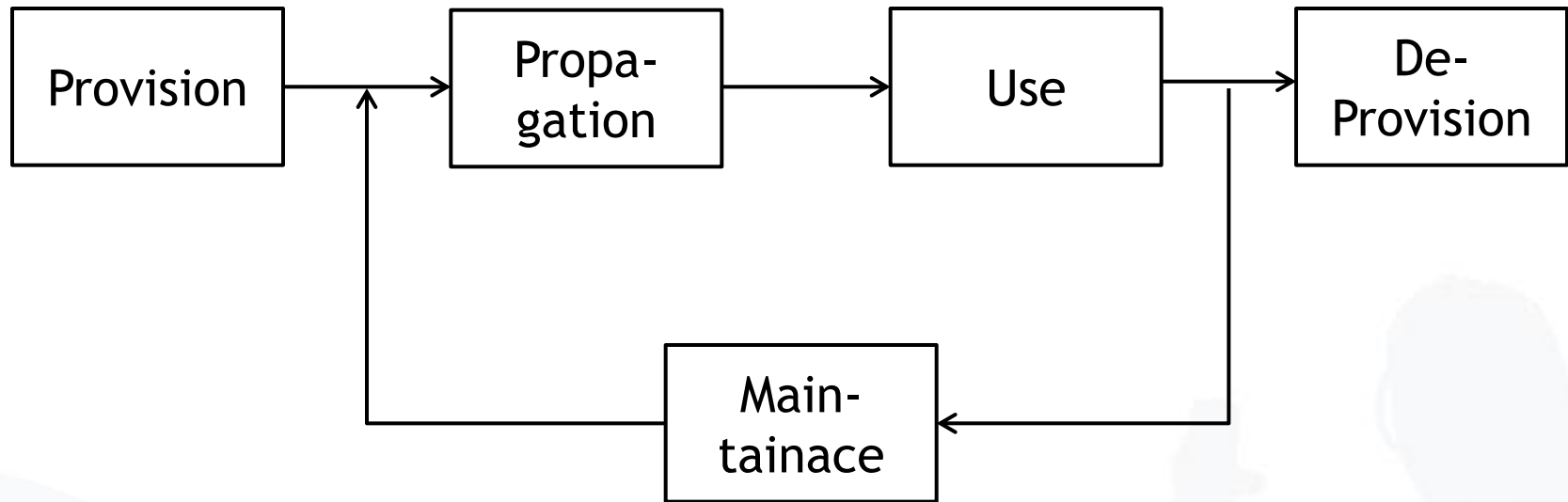
- Identity Management Systems (IdMS) are tools that support Identity Management activities.
- We distinguish
 1. Pure IMS main objective is the support of identity management functionality, e.g. MS Live, Liberty, Shibboleth, OpenID, password managers, form fillers
 2. Systems/applications with another 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

Source: Bauer and Meints (2005)

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



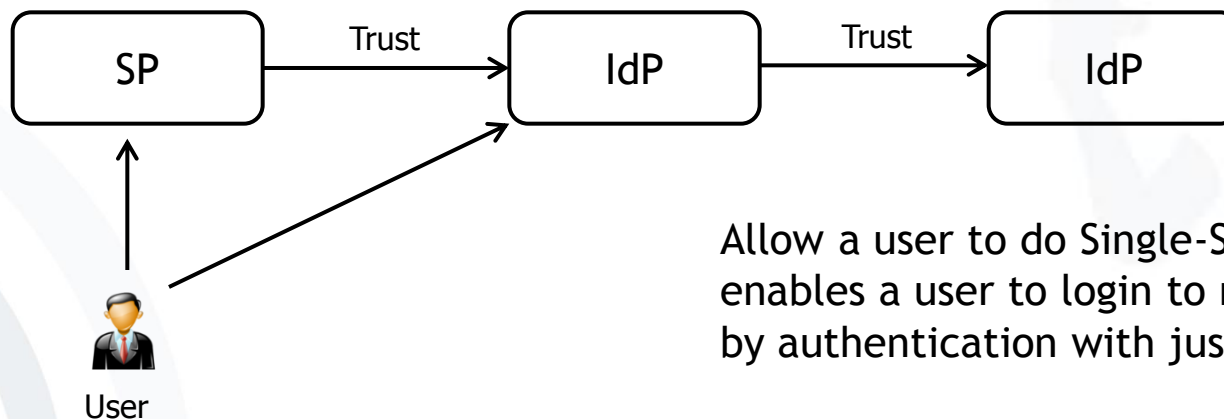
Identity Management LifeCycle





- **Partial Identities**
 - Part of the attributes of an identity of a subject or person
 - Note: Complete identities are typically not used in real-life since an application only requires certain but not all attributes of a person
- **Pseudonymous Identities**
 - Pseudonymisation decouples a digital identity from its real-world identity but linking is possible
- **Anonymous Identities**
 - Digital identity can not be linked in any way to its real-world identity

- Local
 - Local identity in a closed environment (e.g. Windows PC)
- Global
 - Global identity serves to identify entities in a broader context (e.g. passport of an individual)
- Federated
 - Identity federation is based on the conceptual separation between service providers (SP) and identity providers (IdP).

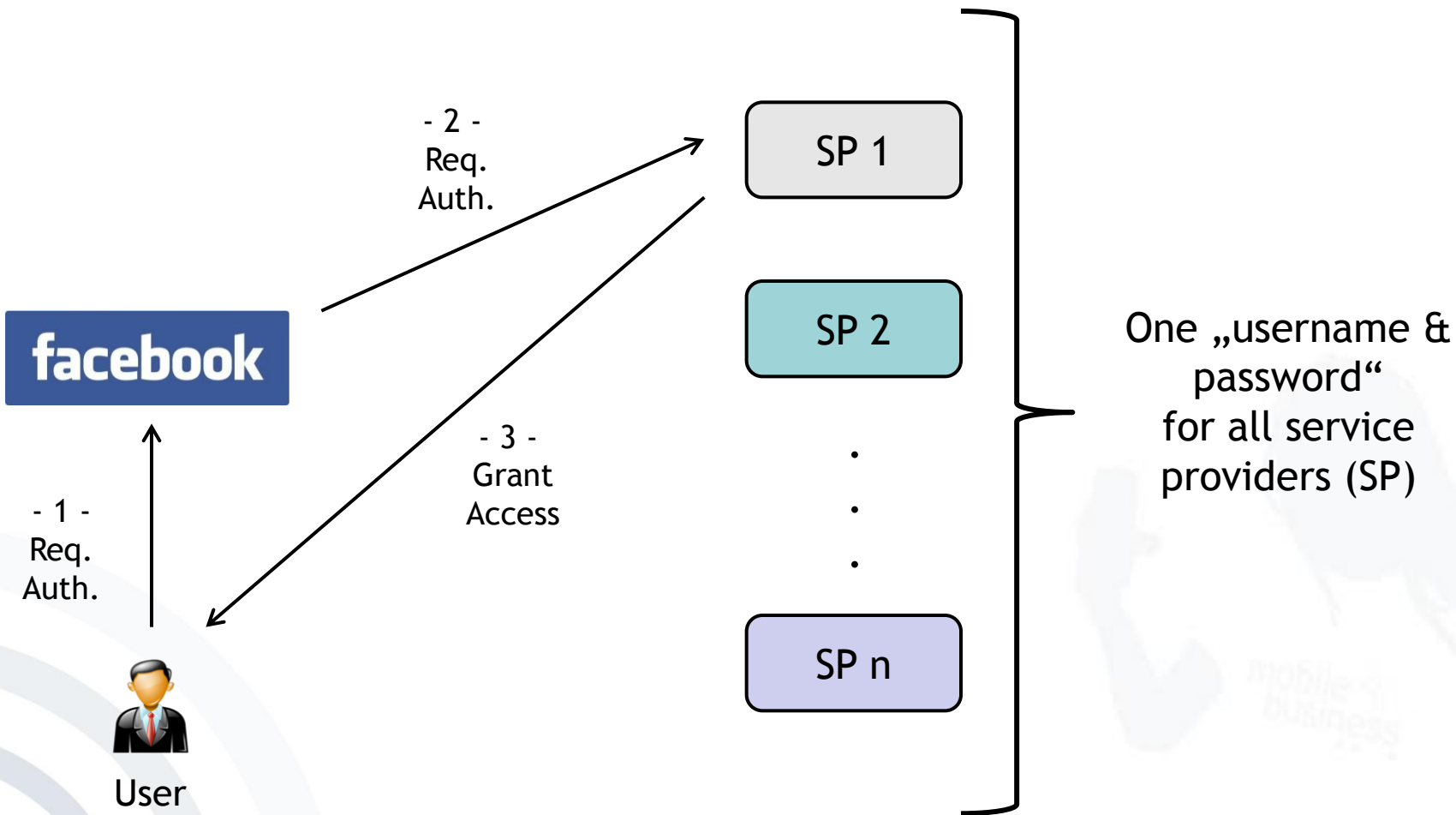


Allow a user to do Single-Sign-On. It enables a user to login to multiple SPs by authentication with just one IdP.

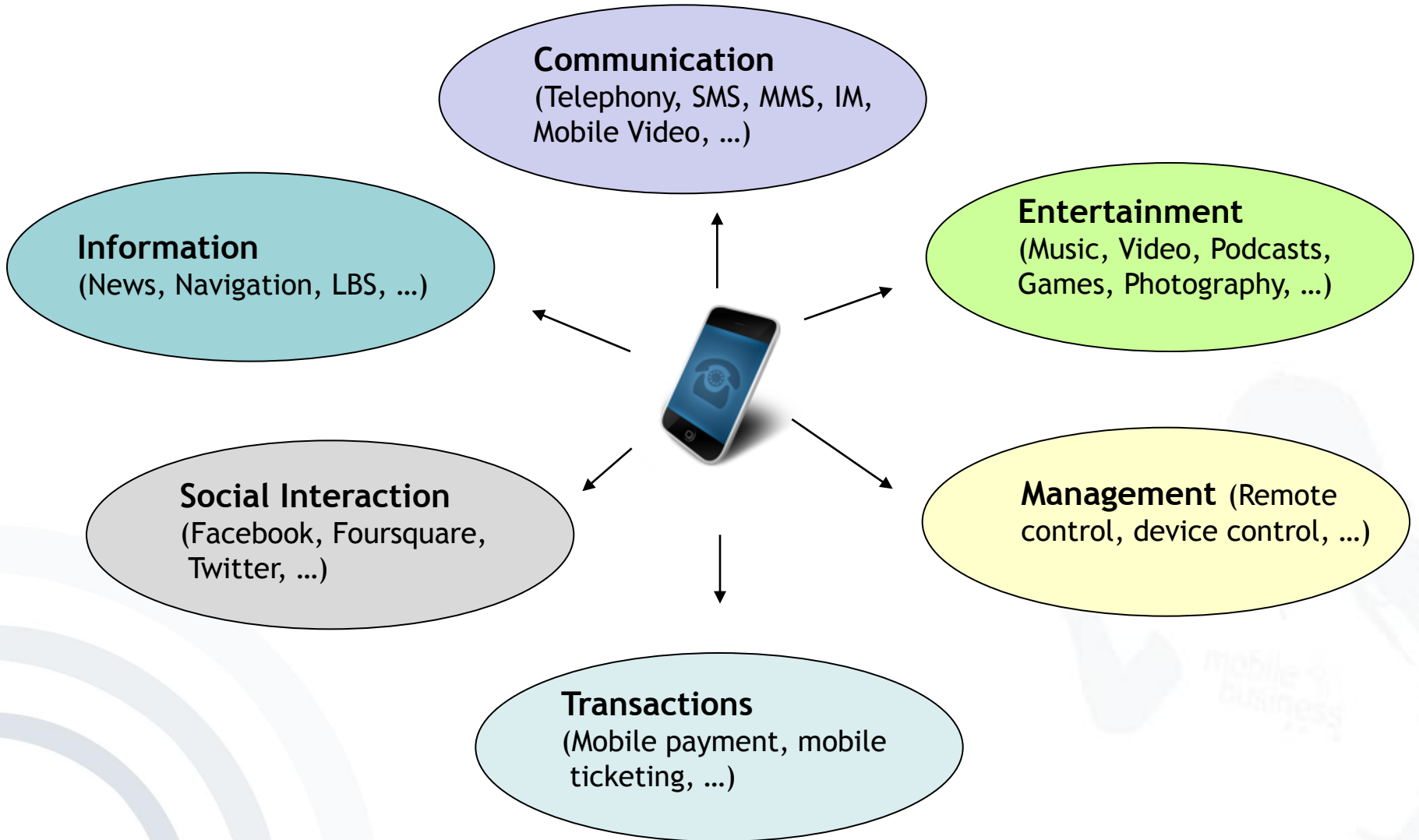
- User Centric Model
 - User is in control of his identity (e.g. identity information is stored on the mobile phone)
- Service Provider Model
 - Identity service provider controls a user's identity on his behalf (e.g. Microsoft LiveID)



Single Sign-On at the Example of Facebook Connect



- The Identity Concept
- Digital Identities
- Identity Management and Identity Management Systems
- Mobile Devices as Digital Identities
- Identity Threats



- Mobile phones ...

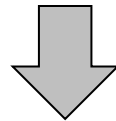
- are always carried with (besides wallet and keys)
- on average turned on 14 hours per day
- usually belong only to a single person
- are usually not lend to other persons
- allow a 1:1 communication
- can be used time or location independent
- are instant-on



- Mobile phones...
 - store, manage and process sensitive, personal data of their users
 - Contacts, photos, videos, text messages, mails, account credentials, etc.
 - provide context information about the current usage situation of their users
 - GPS data, time of usage, unique user ID, noise- and light information, ...
 - receive high attention and interaction from their owners
 - Text messages, push-mails, IM messages, ...



- Mobile phones ...
 - are personal devices
 - manage personal data and
 - enable the access to mobile services



- Mobile phone represent the **digital identities** of their users in everyday life



- The Identity Concept
- Digital Identities
- Identity Management and Identity Management Systems
- Mobile Devices as Digital Identities
- Identity Threats

- Security of identities and surveillance
- Persistence of identities over time
- Incapacitated data controllers
- Over-sharing of personal information
- Impairment of rights by digital services

Source: GINI (2011)



- Bogdanowicz, M. and Beslay, L.: Cyber-Security and the Future of Identity, IPTS Report 57, 2001, www.jrc.es/home/report/english/articles/vol57/ICT4E576.htm, accessed 2008-04-08.
- Bauer, M. and Meints, M. (eds.) (2005) Deliverable D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems, <http://www.fidis.net/resources/deliverables/hightechid/#c1787>, accessed 2008-04-08.
- Global Identity Networking of Individuals - A User-centric Framework of Identity Management Services, Deliverable 1.1, June 2011