Identity Management Systems – An Overview

IST Event 2004 / 15.11.2004

Marit Hansen / Henry Krasemann

Unabhängiges Landeszentrum für Datenschutz //
Independent Centre for Privacy Protection
Schleswig-Holstein, Germany

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Overview

- **Identity Management –**
  More than Single Sign-on??
- **Requirements to the Design and Different Ways of Implementation –**
  Different Properties of Solutions
- **Identity Management and Law**
- **Evaluation of Main IMS –**
  Operational Database
- **Recent Survey Among Experts**

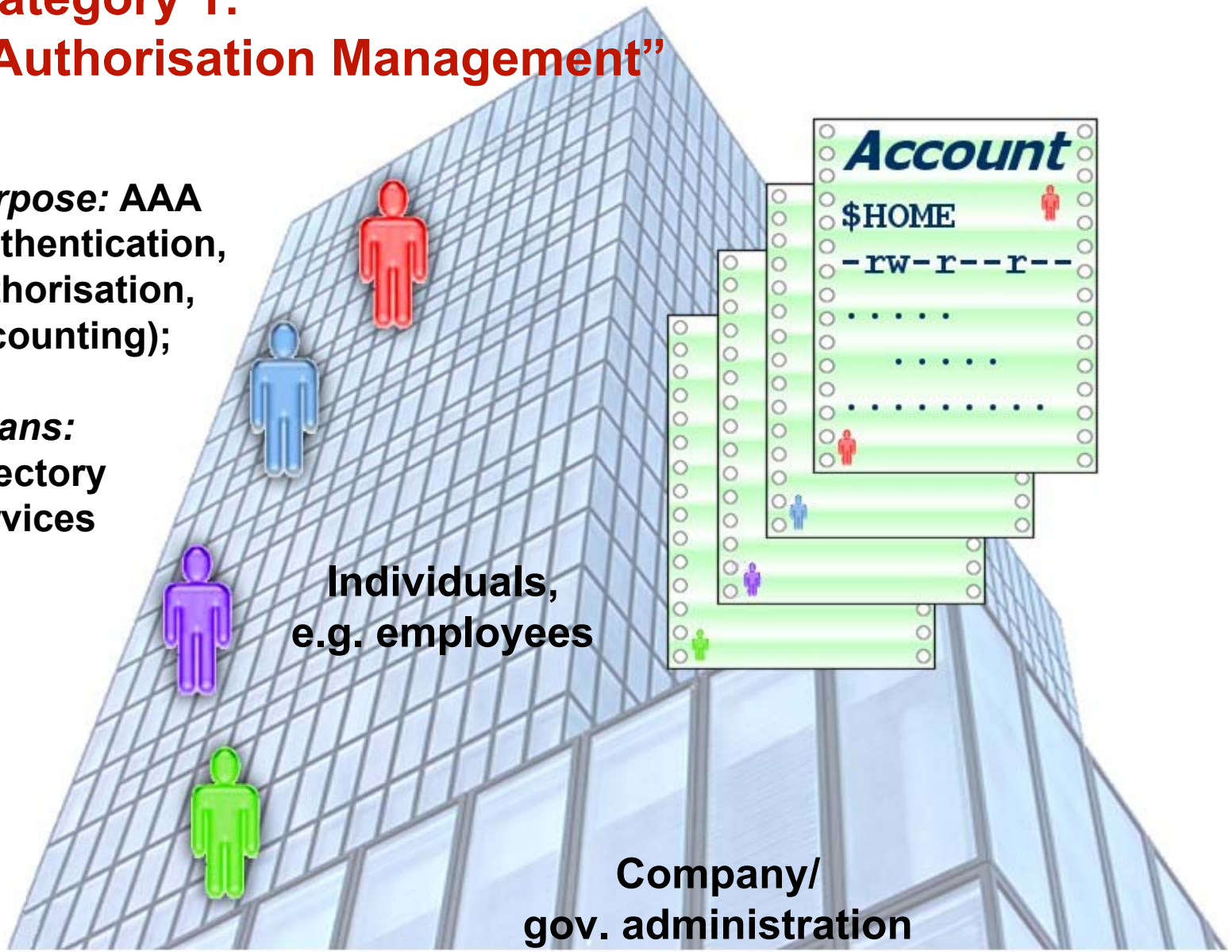
Identity Management:

Management of Identities or Identity Data

Category 1: "Authorisation Management"

Purpose: **AAA (authentication, authorisation, accounting);**

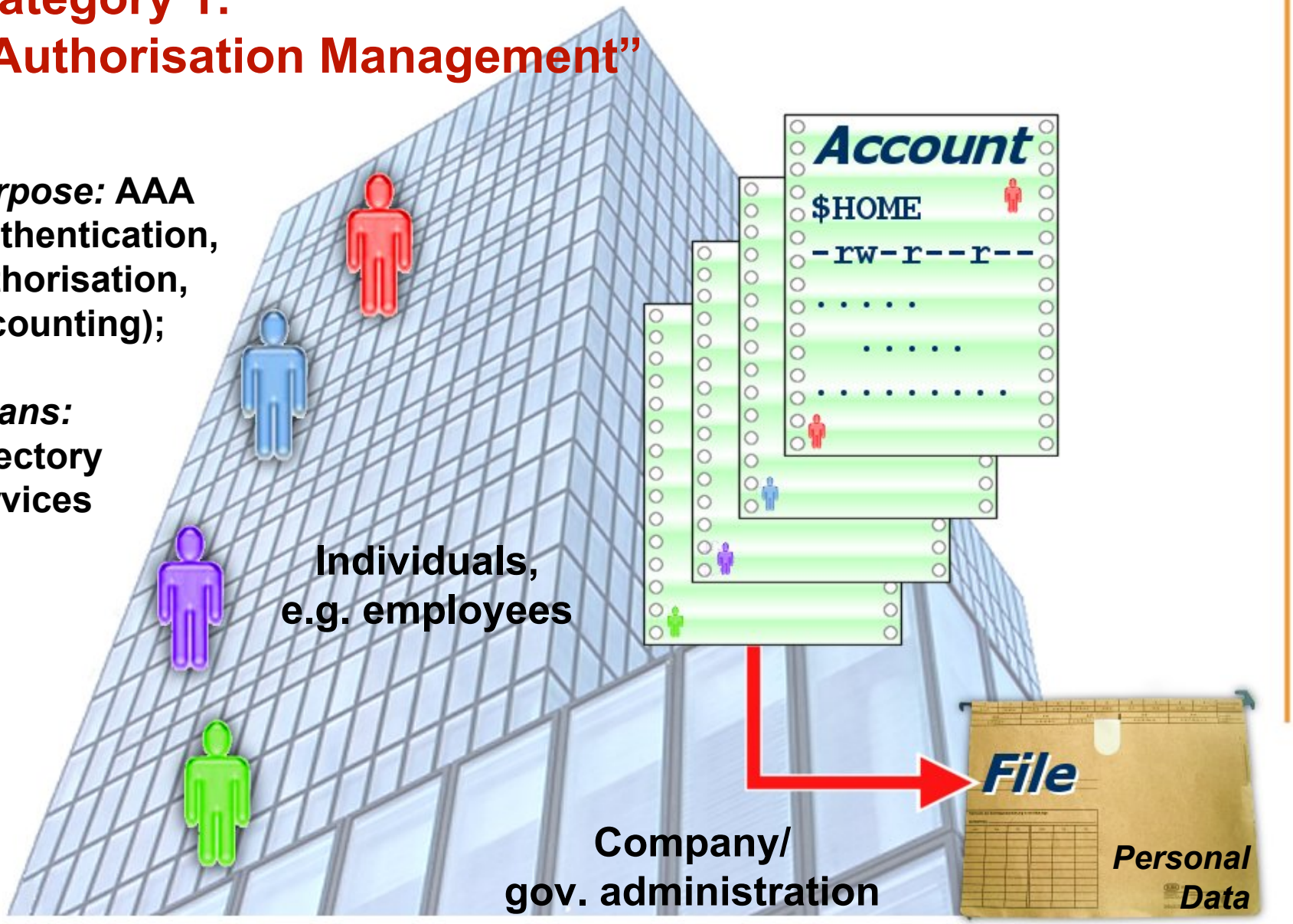
Means: **directory services**



Category 1: "Authorisation Management"

Purpose: **AAA (authentication, authorisation, accounting);**

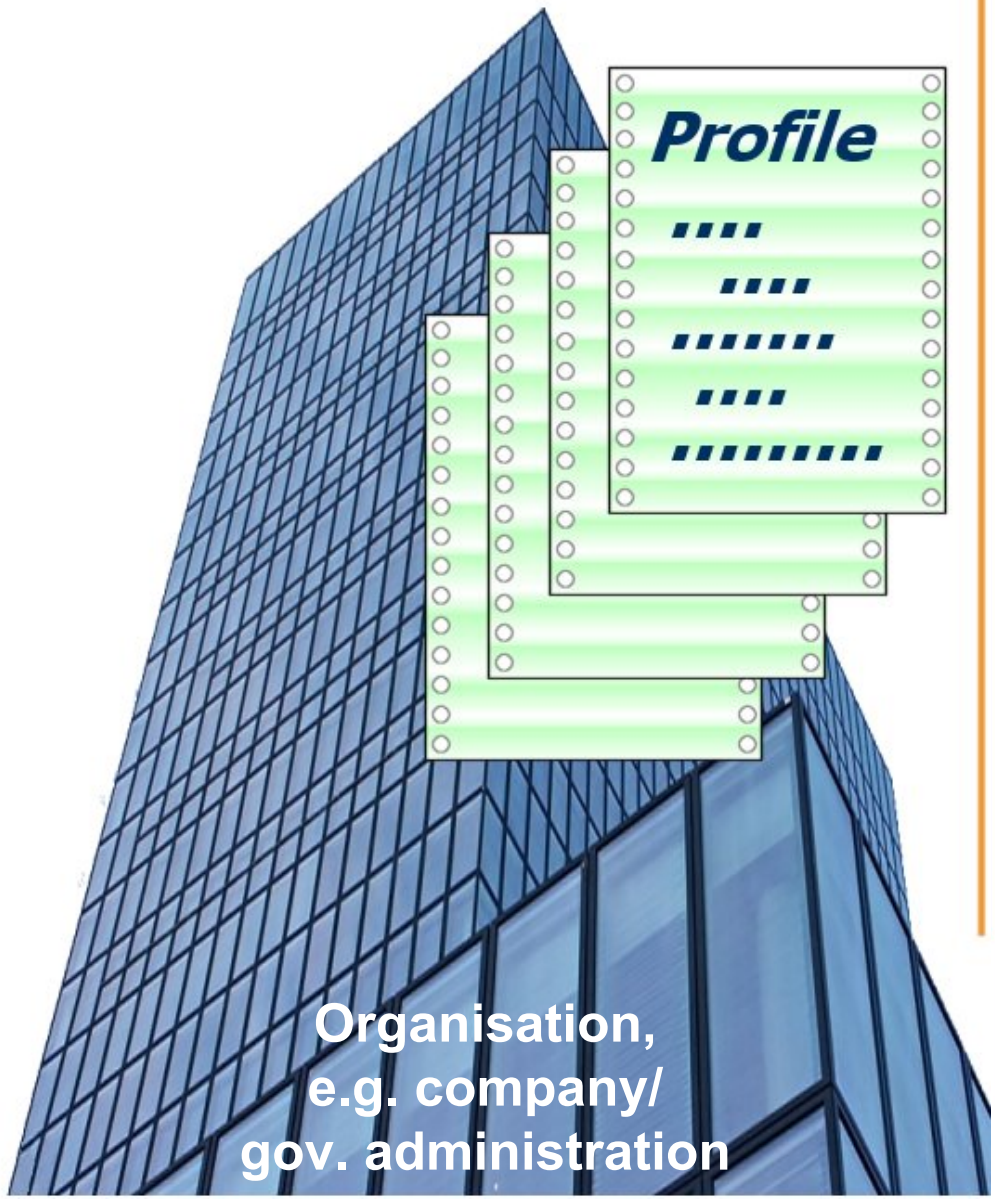
Means: **directory services**



Category 2: "Profiling"

Individuals, e.g. customers, citizens

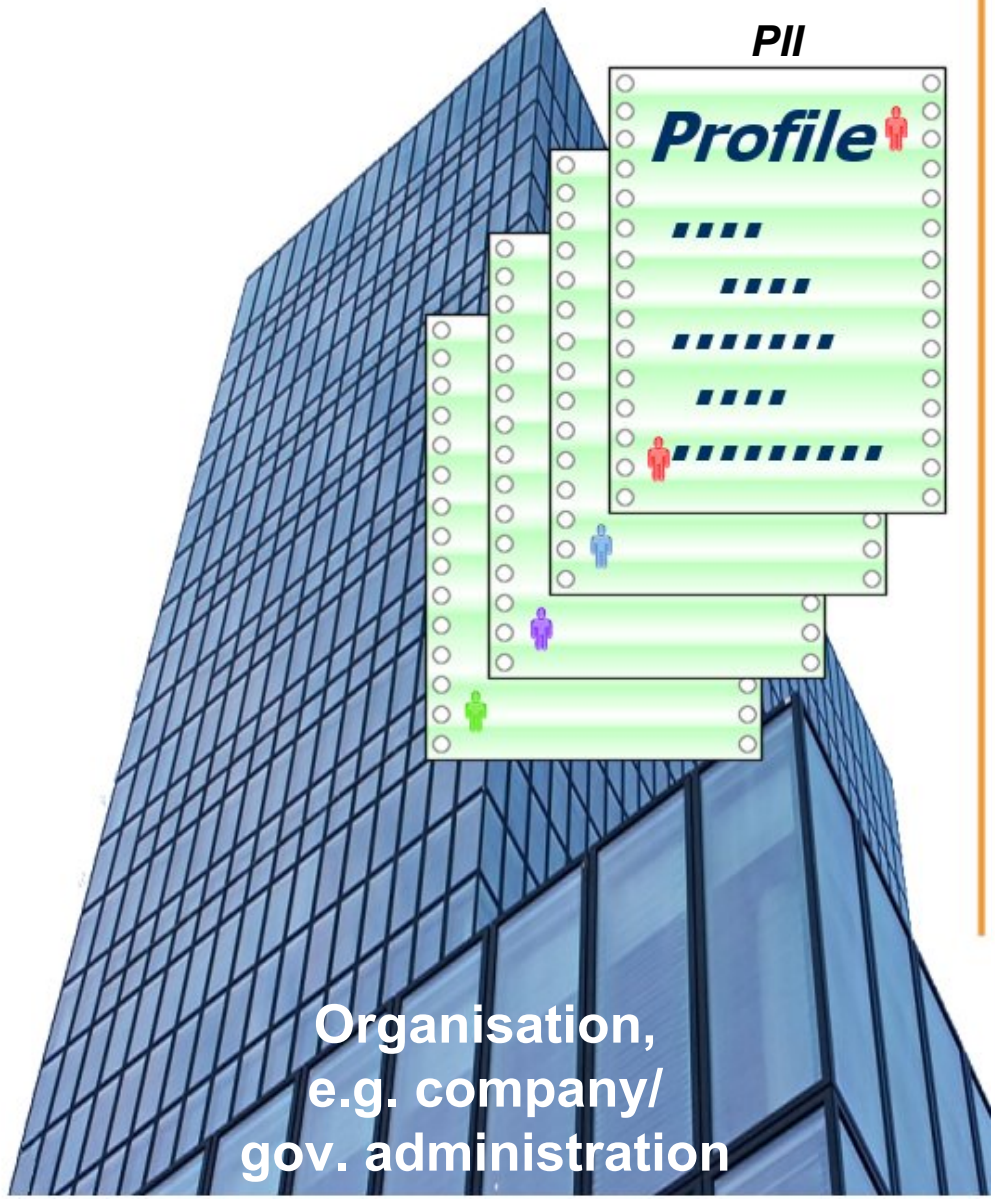
Purpose: **analysis of user behaviour;**
Means: **logfiles/ data warehouses**



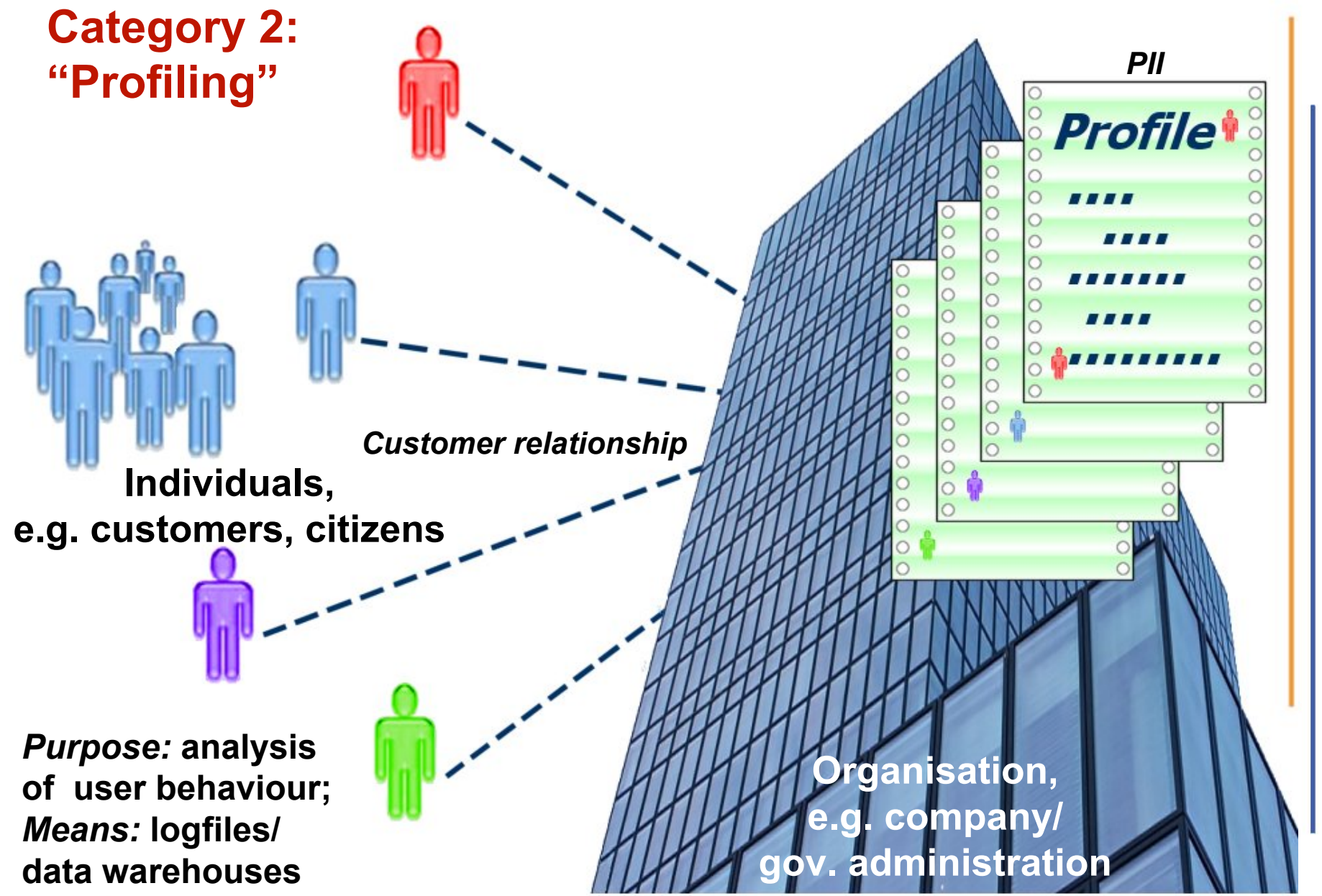
Category 2: "Profiling"

Individuals, e.g. customers, citizens

Purpose: **analysis of user behaviour;**
Means: **logfiles/ data warehouses**

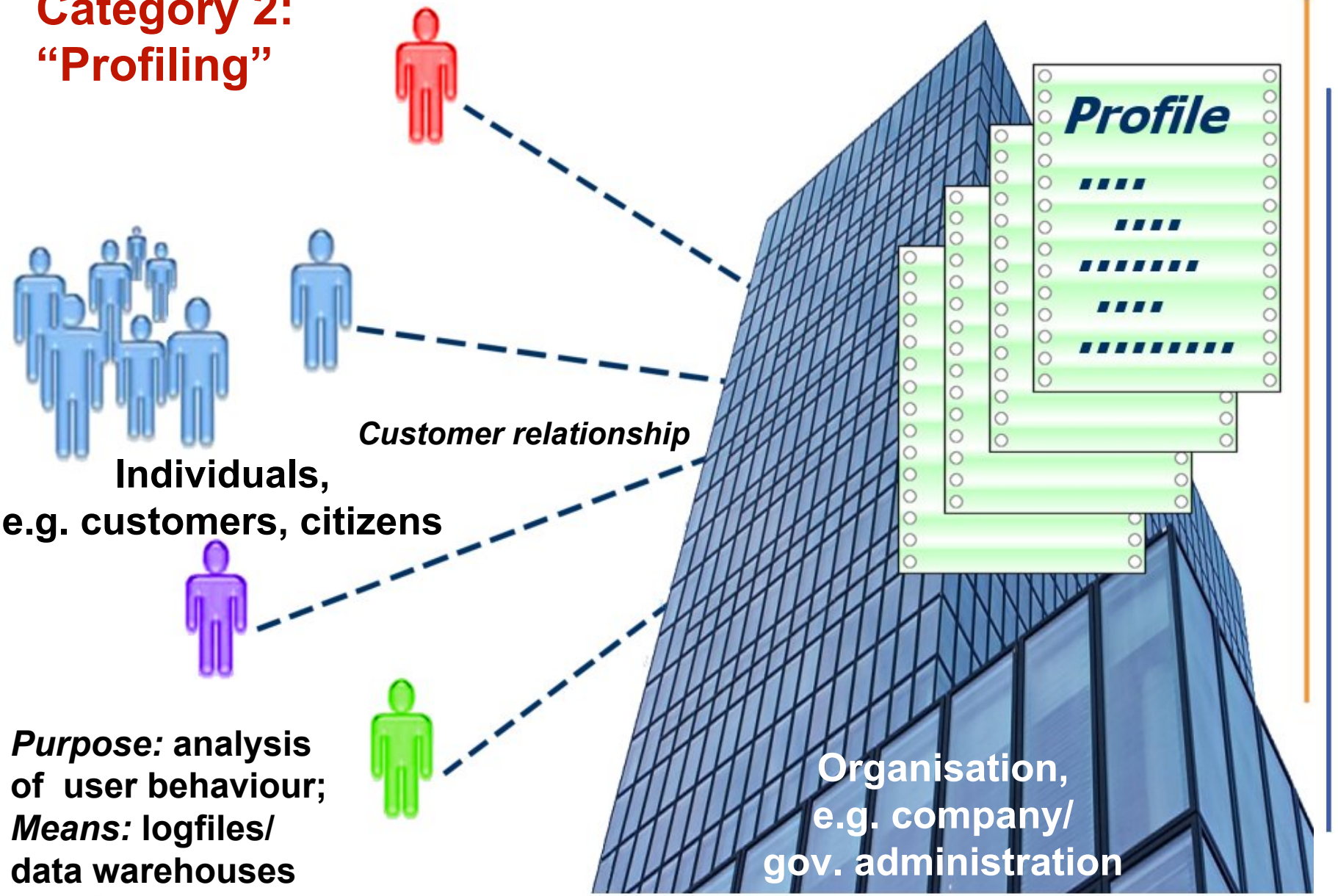


Category 2: "Profiling"

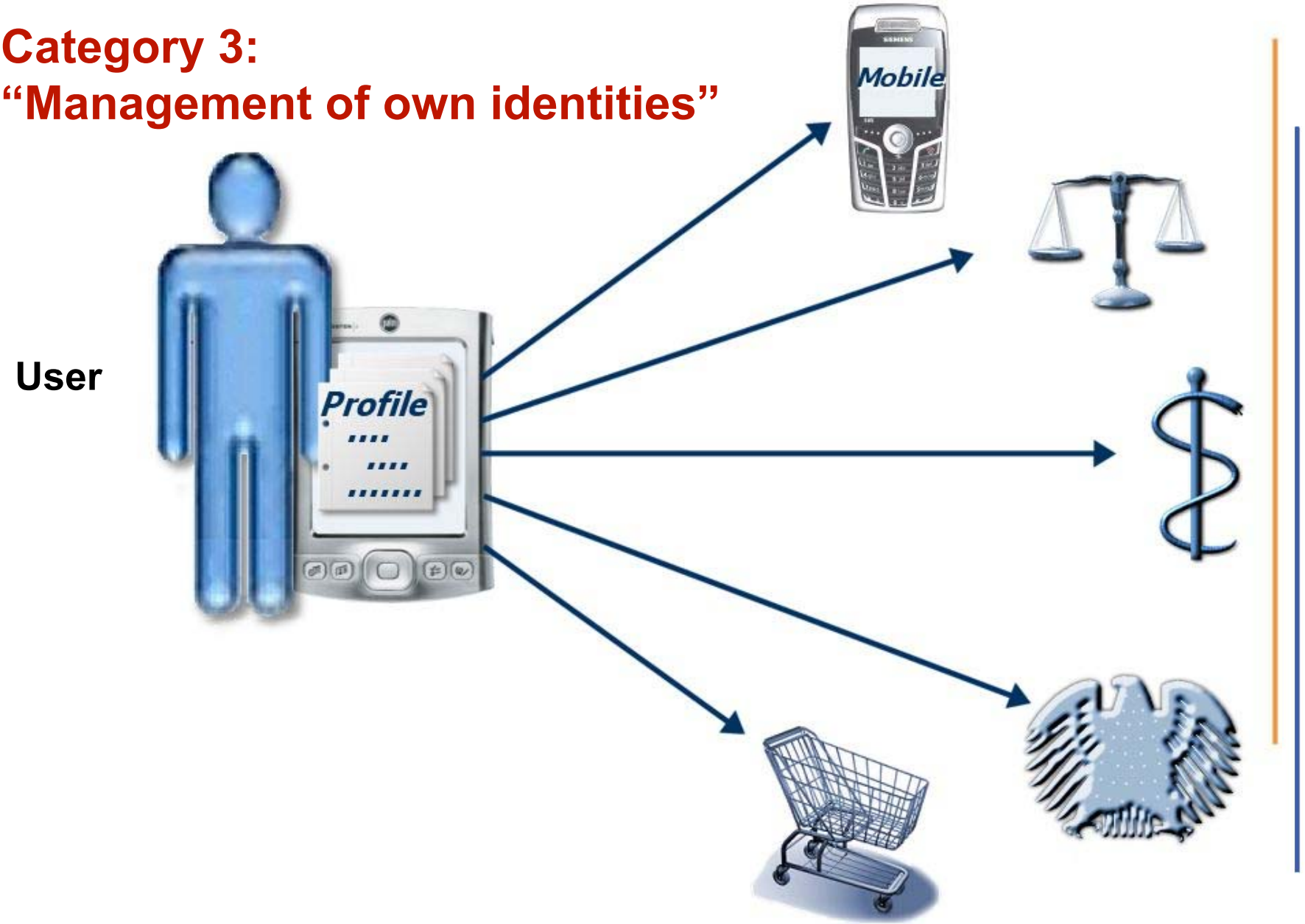


Purpose: **analysis of user behaviour;**
Means: **logfiles/ data warehouses**

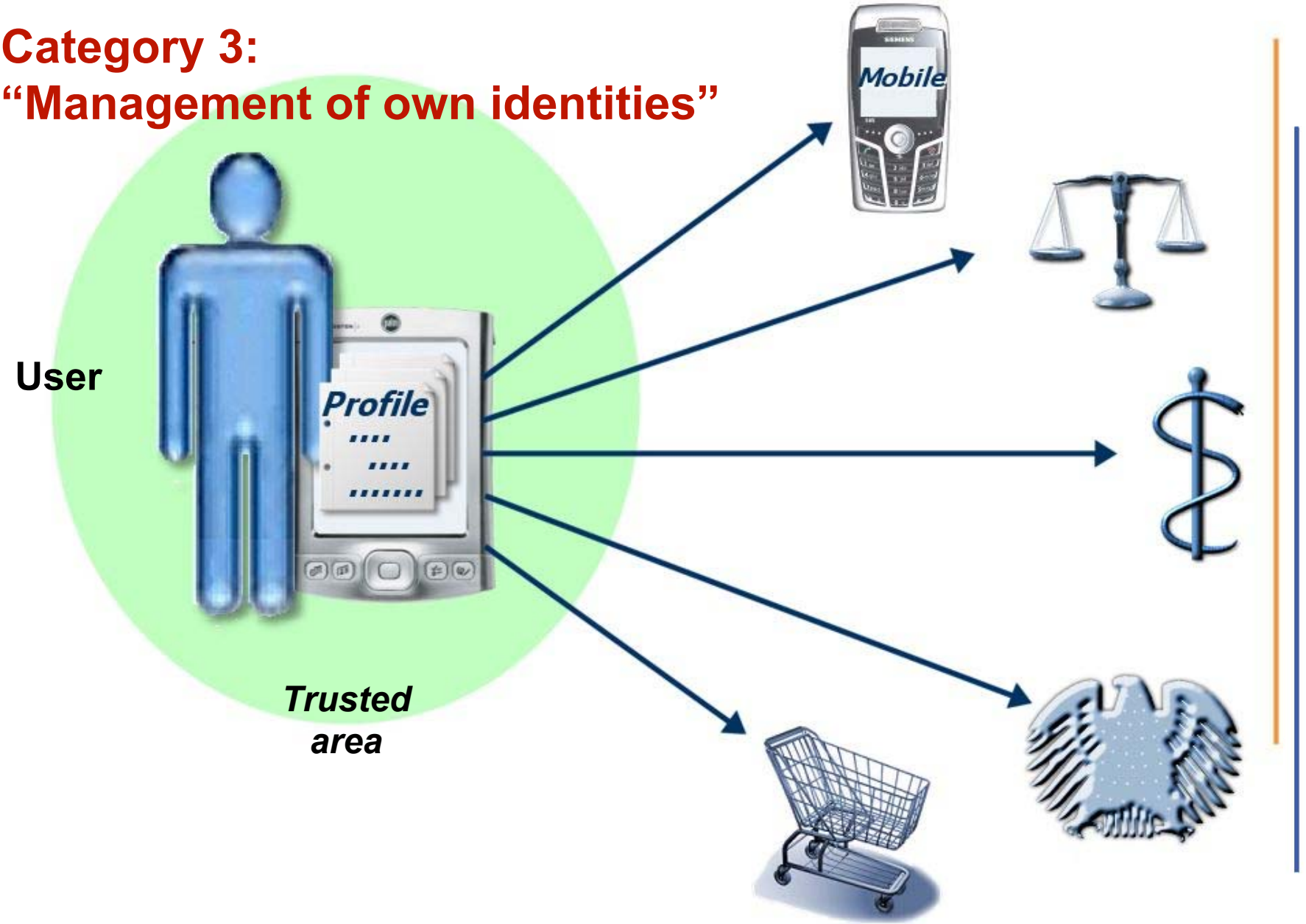
Category 2: "Profiling"



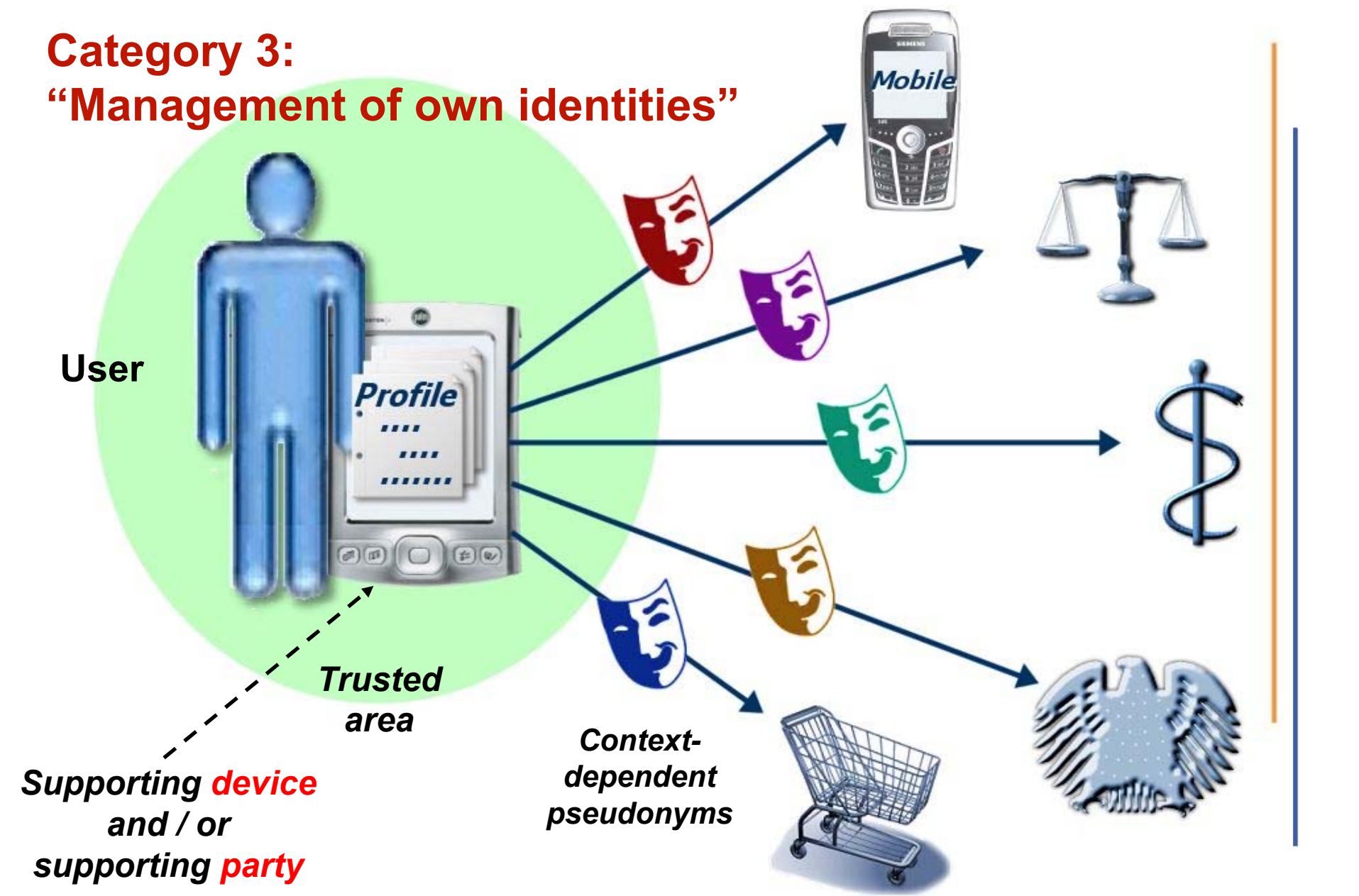
Category 3:
“Management of own identities”



Category 3:
“Management of own identities”



Category 3:
"Management of own identities"



Result: Privacy-Enhancing IMS?

Cat. 1		Authorisation Management: *assigned identity*	by organisation

Result: Privacy-Enhancing IMS?

Cat. 1		Authorisation Management: *assigned identity*	by organisation
Cat. 2		Profiling: *derived identity*	by organisation

Result: Privacy-Enhancing IMS?

~~Cat. 1~~		Authorisation Management: *assigned identity*	by organisation
~~Cat. 2~~		Profiling: *derived identity*	by organisation
Cat. 3		Management of own identities: *chosen identity*	by user himself supported by service providers

Requirements to the Design and Different Ways of Implementation

Different Properties of Solutions

Motivation

Problem
Confusing and inconvenient handling of my different “identities”
Little knowledge of what others know about me
Little control about what I permit from the outside
Little legal liability; no protection against Identity Theft

Motivation

Problem	Solution Concept
Confusing and inconvenient handling of my different "identities"	Password Management / Single Sign-on; Form Filler
Little knowledge of what others know about me	
Little control about what I permit from the outside	
Little legal liability; no protection against Identity Theft	

Motivation

Problem	Solution Concept
Confusing and inconvenient handling of my different "identities"	Password Management / Single Sign-on; Form Filler
Little knowledge of what others know about me	Anonymity as basis, on top: Controllability of data flow and of privacy preferences; Reputation Management
Little control about what I permit from the outside	
Little legal liability; no protection against Identity Theft	

Motivation

Problem	Solution Concept
Confusing and inconvenient handling of my different "identities"	Password Management / Single Sign-on; Form Filler
Little knowledge of what others know about me	Anonymity as basis, on top: Controllability of data flow and of privacy preferences; Reputation Management
Little control about what I permit from the outside	Reachability Management
Little legal liability; no protection against Identity Theft	

Motivation

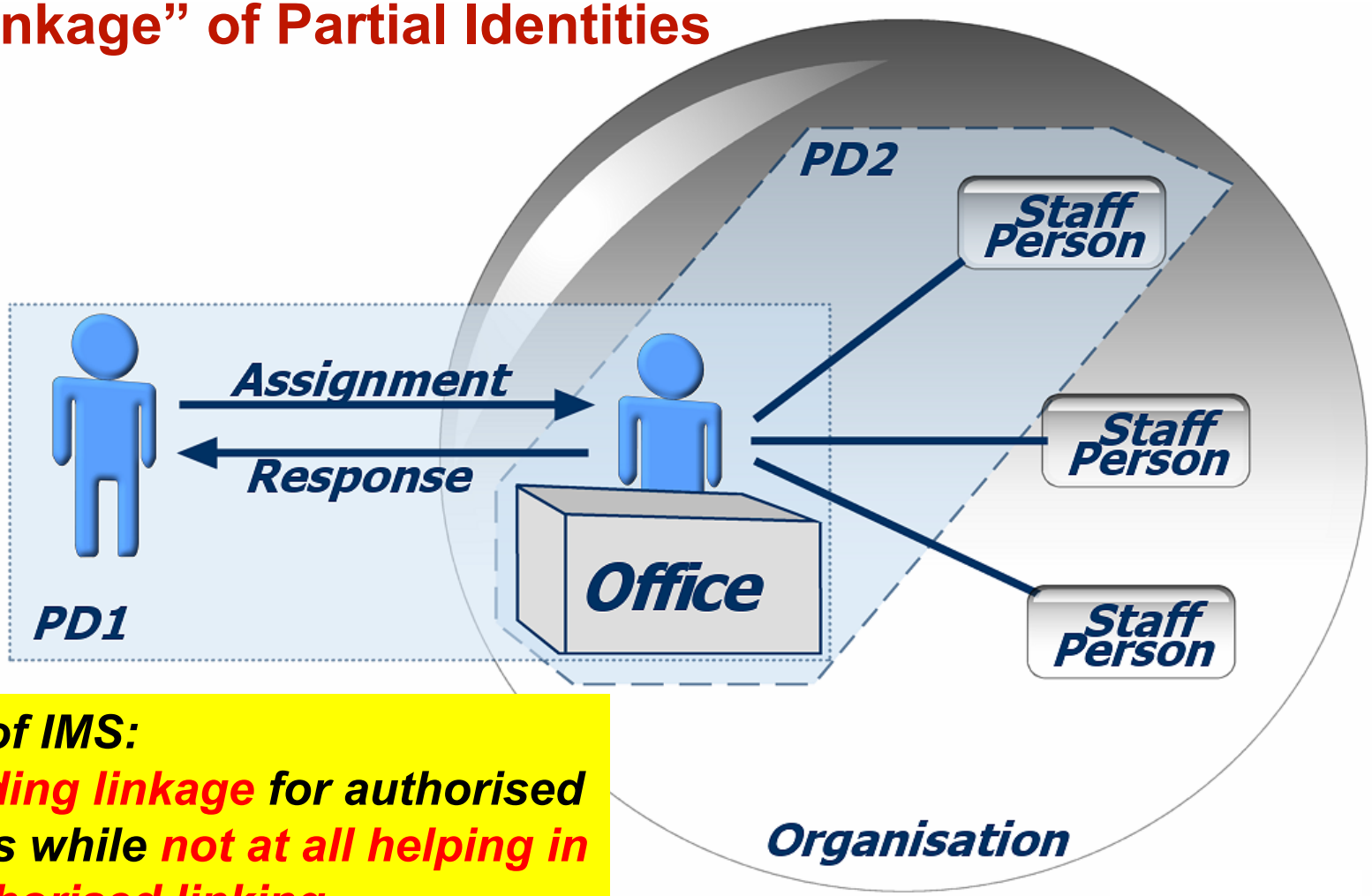
Problem	Solution Concept	State of the Art?
Confusing and inconvenient handling of my different "identities"	Password Management / Single Sign-on;	+
	Form Filler	+
Little knowledge of what others know about me	Anonymity as basis, on top:	-
	Controllability of data flow and of privacy preferences;	-
	Reputation Management	±
Little control about what I permit from the outside	Reachability Management	±
Little legal liability; no protection against Identity Theft	Authenticity supported by infrastructure	-

Key question:
Who is in control?

Identity Management

Identity Management is managing of own partial identities according to specific situations and contexts.

Workflow Design according to Pseudonym Domains (PD): “Unlinkage” of Partial Identities



Task of IMS:
Providing linkage for authorised parties while not at all helping in unauthorised linking

Identity Management and Law

Identity (Management) and Law

- **Identity – Elements for identification**
  - **Name, sex, birthday, place of birth, number of birth certificate, identity of parents, nationality, domicile, job, etc.**
  - **Biometrics (fingerprints etc.)**

  = personal data

- **Personal rights (bonded to person)**
  - **Constitutions, human rights**
  - **Right to the free development of one's personality**
    - **Change of name, sex, appearance, domicile, etc.**

Management of Parts of Identity

- **Name**
  - Possibility of choice of name (pseudonym / stage name)
  - Change of name (cf. Germany § 3 Abs. 1 NÄG), adoption, marriage (also child), divorce, transsexuality (first name), etc.
- **Gender**
  - Sex reserval (cf. Germany § 8 ff. Transsexuellengesetz)
- **Appearance (Germany Art. 2 Abs. 1 GG)**
- **Domicile**
  - Freedom of movement throughout the EU (Art. 39 EC Contract)
  - Freedom of establishment (Art. 43 EC Contract)
- **Nationality**
  - Naturalization (e.g. Germany §§ 85 ff. AuslG)
  - Double citizenship

Management of Parts of Identity

- One-man company / single-member company
  - Cf. e.g. Germany “GmbH” since 1.1.1981 (§ 1 GmbHG)
  - Europe: Twelfth Council Company Law Directive 89/667/EEC of 21 December 1989
  - Private limited - liability companies

- Domain name / email address
  - Right to bear a name

No General Obligation to Disclose Identity

- Freedom to decide when to disclose own identity

- Obligation to prove one's identity
  - Some countries have no identity papers
  - Others: obligation only in front of special persons (e.g. police)
    - No obligation to carry it always with oneself

- Possibility to "lie" (cf. e.g. Germany Art. 2 par. 1 GG)
  - E.g. apply for job / flat
  - Limitations: law, rights of third parties (and manners)

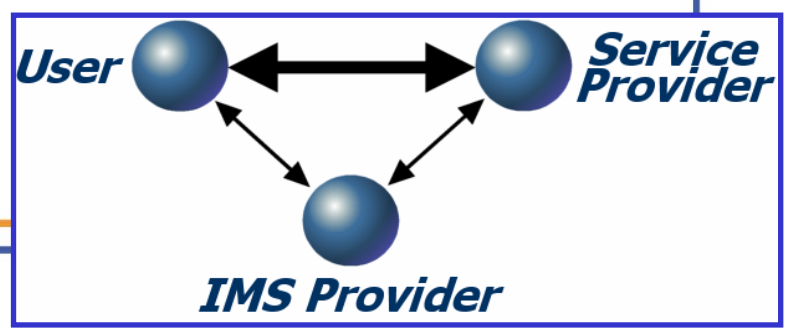
Using Different Name(s)

- Germany: “Handeln unter fremdem Namen”
- Possibility of dealing on one’s own behalf using a different name / identity / pseudonym
  - If identity is irrelevant or negligible for the business partner
    - E.g. purchase at a bakery

    ⇒ Possibility to use a pseudonym
  - Otherwise: regulations about representation

Identity Management and Third Party Support 1/2

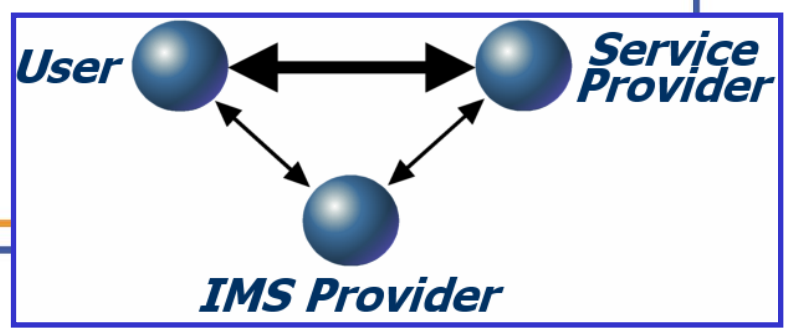
- Infrastructure security and resilience
- Certification services:
  - Possibly supporting various degrees of data minimisation, e.g., by allowing pseudonymous but accountable authentication (incl. convertible credentials).
- Mediator services, e.g.:
  - Identity brokers reveal the identity of a pseudonym holder under specific circumstances.
  - Liability services clear a debt or settle a claim on behalf of the pseudonym holder.
  - A value broker may perform the exchange of goods without revealing additional personal data.



Identity Management and Third Party Support 2/2

- **Separation of knowledge:**
  - **E.g., unlinkability of the "who (buys)" and the "what (is bought)" may be achieved by applying separation of knowledge between payment and delivery services.**

- **Reference information:**
  - **A privacy information service can give input on privacy information data such as security and privacy risks with respect to the IMS deployed, which may influence the behaviour of the system.**
  - **The privacy information service could also be offered in a peer-to-peer manner.**



Evaluation of Main IMS

Operational Database

IMS Study 2003: First Evaluation of IMS


Identity Management Systems (IMS): Identification and Comparison Study

Independent Centre for Privacy Protection (ICPP) / Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein

and

Studio Notarile Genghini (SNG)

2003-09-07

Contract N°19960-2002-10 F1ED SEV DE.

- Approx. 100 IMS identified
- Detailed evaluation for 7 IMS:
  - Single Sign-On:
    - Microsoft Passport
    - Liberty Alliance (in spec. process, > 150 companies involved)
    - Yodlee
  - Form Filler:
    - Mozilla Navigator
    - DigitalMe
    - CookieCooker
  - E-Mail Client: Outlook Express
- Usage:

  Big user numbers only when integrated such as Microsoft Passport (200 million accounts, 3.5 billion authentications per month, 91 websites supported)

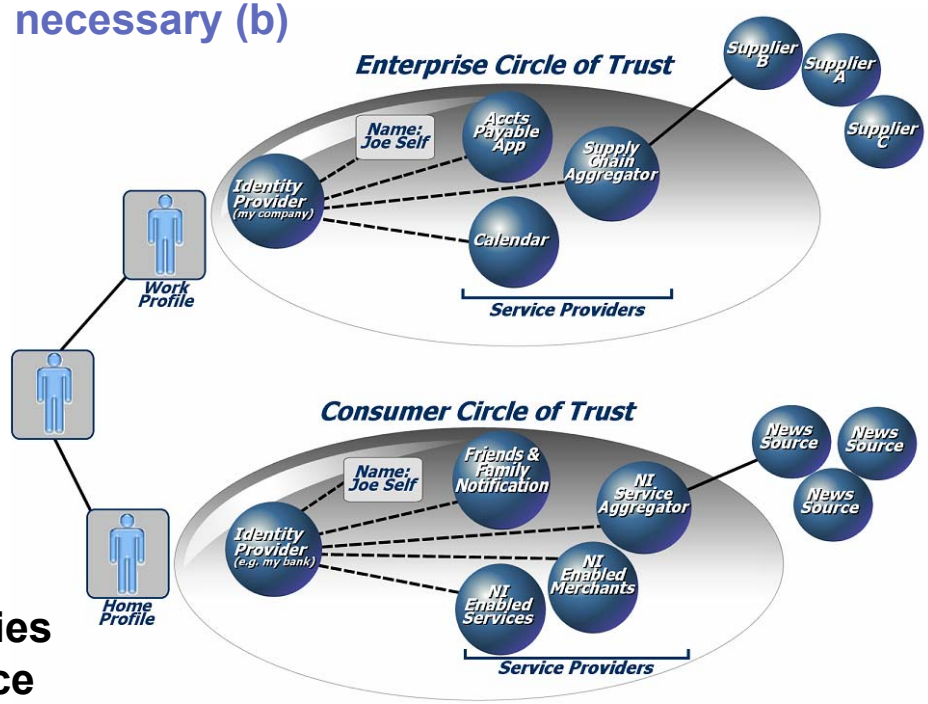
Centralised vs. Federated Identity

Centralised Identity:
Single IMS provider

- \+ Easier to **maintain**
- \+ **Less effort** in user support
- \+ **Cheaper**
- – **Concentrate** personal data of people (content and data trails)
- – Put big **responsibilities** on the providers
- – Are **attractive targets** for attackers
- – May act as **convenient data bases** of other interested parties

Federated Identity
a) user-side identity administration
b) multiple IMS providers

- \+ **User** can be in control (a)
- \+ **No concentration** of personal data (b)
- \+ IM solution for **SME** (a,b)
- ± Put bigger **responsibilities** on the user (a)
- – **More effort** in user support (a)
- – **Standardisation** of protocols/interfaces necessary (b)



⇒ *Question of Trust*

Example:
Federated Identities
in Liberty Alliance

Evaluation of Selected IMS

Application	Main Functionality	Type of ID	Usefulness	Ease of Use	Malfunction Understanding	Security	Privacy	Digital Evidence	Trustworthiness	Cost for User	Business Model
Microsoft Passport	SSO	centralised	4	4	2	1.5	1.5	0	1	0	Paid by partner sites
Liberty Alliance	SSO	federated	4	2+X	X	1.5+X	1.5+X	0	2+X	0	Paid by partner sites
Yodlee	SSO	centralised	4	3.5	4	3.5	2	0	1	0	Presentation / Promotion
Mozilla Navigator	Form Filler	federated (client)	4	4.5	4	2	3	0	3	0	Open Source
Digitalme	Form Filler	centralised	4	3.5	2	2.5	3	1	1	0	Presentation / Promotion
CookieCooker	Form Filler	federated (client)	4.5	2	3	2	3.5	1	2	15 €	Paid by user
Outlook Express	Mail Identities	federated (client)	3.5	4.5	5	1.5	3	1	3	0	Part of MS Windows

Until end of 2003 Microsoft Passport will have integrated major changes according to requirements of the Working Document on on-line authentication services by the Article 29 Data Protection Working Party.

First List of IMS

Name	Closed / Open System	Client / Server (Storage of Identity Data)	Access Management	Form Filling	Automatic Choice of Identity	Pseudonym Management	Reachability Management	Specific Functionality / Component
AccountCourier	Open	C/S	Y	N	N	(Y)	(Y)	Automated account provisioning and user ID management (mainly for organisations)
Anonymizer Privacy Manager	Open	Client	N	N	N	(Y)	(Y)	Allows user to customise an individual privacy and security level for each site
AssureAccess	Open	C/S	Y	N	N	(Y)	(Y)	Access management software for Java/J2EE-based web, portals, and web services (for application developers)
ATUS	Open	Client	N	N	Y	Y	N	Choice between different partial identities
Certification Authorities / PKI	Open	C/S	N	N	N	Y	(Y)	E.g., Telesec.de, Verisign.com etc.
ClearTrust	Open	C/S	Y	N	N	N	N	Web access management
Cookie Pal	Open	Client	N	N	(Y)	N	N	Cookie manager
CookieCooker	Open	Client	(Y)	Y	(Y)	Y	N	Exchange of cookies, management of different identities, and form filling
DASIT	Open	C/S	N	N	N	Y	(Y)	Privacy control functionality for e-Commerce
Digital Handshake	Open	Client	(Y)	(Y)	N	(Y)	N	US standards-based electronic signature solution
Digital Identity	Open	Server	Y	N	N	(Y)	Y	Implements SOAP and supports relevant standards such as SAML
Digital Signature Certification	Open	C/S	(Y)	N	N	(Y)	N	Various PKI providers
DigitalMe	Open	Server	Y	Y	N	Y	N	Control of personal information presented to the public or single persons (meCard)
Dotomi	Closed	C/S	(Y)	N	N	(Y)	(Y)	Users can specify the vendors from whom they wish to receive communication in advertising space on the web
DRIM	Open	Client	(Y)	N	(Y)	Y	(Y)	Comprehensive concept based on IDMAN, SSONET etc.
eBay	Closed	Server	N	N	N	(Y)	(Y)	Auction community in the web with own reputation system
Erreichbarkeitsmanager	Closed	Client	N	N	(Y)	Y	Y	Implementation of reachability management on Newton MessagePads
eTrust	Closed	C/S	Y	N	N	(Y)	N	Modular suit for user provisioning, single sign-on and authentication for business
Every.one.name	Open	Server	N	N	N	(Y)	(Y)	Provides e-mail addresses to customers for use by themselves from a pool of second level domains
eWallet	Open	Client	Y	Y	N	N	N	Form filling and password management
FINEID	Open	C/S	(Y)	N	N	N	N	Identification card with digital signature
Flirtmaschine.de	Closed	Server	N	N	N	(Y)	(Y)	Dating agency working with pseudonyms
Freedom	Open	Client	N	N	N	N	(Y)	Services include spam blocking, cookie management, anonymous surfing, and Internet content filtering service
Freever	Closed	Server	N	N	N	(Y)	(Y)	Mobile community management (chat) over SMS, MMS, WAP, and voice
GetAccess	Open	Server	Y	N	N	(Y)	(Y)	Provides organisations with single sign-on to web portal applications
Hushmail	Open	C/S	N	N	N	(Y)	(Y)	Web-based e-mail and document storage system with block lists, auto-responders, different e-mail domains, and digital signature verification
ID2	Open	C/S	(Y)	N	N	N	N	Digital identification solutions on the Internet based on PKI and smart card technology
idemix	Open	Client	(Y)	N	(Y)	Y	N	Anonymous credential system
IDMAN	Open	Client	N	N	(Y)	Y	(Y)	Component of DRIM for management of identities resp. pseudonyms
iPrivacy	Open	C/S	N	N	N	(Y)	Y	Enables consumers to surf and purchase online anonymously, use different unique e-mail addresses and receive products without revealing names, addresses, or credit card information to the merchant
It's My Profile	Open	Server	N	N	N	(Y)	(Y)	Site allows the user to control information about own activities and preferences, e.g., to authorise e-mail contacts from advertisers in relation to these activities
Keon	Open	C/S	(Y)	N	N	(Y)	N	Enterprises can issue and manage their own web server SSL certificates, relying on a third party
Kerberos tickets	Open	C/S	Y	N	N	N	N	A unique key (a so-called ticket) is assigned to each person that authenticates to the network
KeyNote Trust management	Open	C/S	Y	N	N	(Y)	N	Provides a single, unified language for both local policies and credentials
LibertyAlliance	Open	C/S	Y	N	N	-	-	Developing open standards for network identity
Lotus Notes	Open	C/S	Y	N	N	N	(Y)	Management of communication and administration of information flow
ManageID Suit	Open	Server	Y	N	N	(Y)	N	User life cycle management and automation solution for organisations
Match	Closed	Server	N	N	N	(Y)	(Y)	Dating agency working with pseudonyms
Meetup	Open	Server	(Y)	N	N	(Y)	(Y)	Organises local interest groups
Micircles	Closed	Server	(Y)	N	N	N	Y	Phone / SMS equivalent of using mailing lists
Midentity	Open	Server	(Y)	N	?	?	?	Manage how to share digital information & content with other people
Mozilla 1.4	Open	Client	Y	Y	(Y)	(Y)	(Y)	Browser with e-mail client
Netidentity	Open	C/S	N	N	N	(Y)	(Y)	Providing different e-mail addresses with different domain names to users
NetKey	Open	Client	(Y)	N	N	Y	N	Possibility to manage different digital signatures
NetPoint	Open	C/S	Y	N	N	N	N	Unites enterprise identity management and web access control
OpenPrivacy	Open	C/S	Y	N	N	Y	N	Collection of software frameworks, protocols, and services providing a cryptographically secure and distributed platform for creating, maintaining, and selectively sharing user profile information
Orby Privacy Plus	Open	Client	N	Y	(Y)	N	N	P3P features
OTPW	Open	Client	(Y)	N	N	N	N	A one-time password login capability
Outlook Express 6 (Internet Explorer 6)	(Closed)	Client	Y	Y	N	(Y)	(Y)	Browser with e-mail client
P3P + APPEL	Open	C/S	N	N	(Y)	(Y)	N	Platform for Privacy Preferences (P3P) - standard for matching privacy policies / A P3P Preference Exchange Language (APPEL)
Parkinsonpas	Open	C/S	(Y)	N	N	N	N	Care and security card for Parkinson and chronic disease patients
Passport	Open	Server	Y	N	N	N	N	Single sign-on service
Persona	Open	C/S	(Y)	N	N	N	(Y)	Acts as a user-driven information broker between the consumer and a website; supports P3P and cookie management
PGP / GnuPG	Open	Client	N	N	N	Y	N	Cryptographic software for encryption, decryption, and managing different key pairs for different e-mail addresses
PingID	Open	C/S	Y	N	N	N	N	Independent and open system that interoperates with .Net Passport and Liberty Alliance
Playboy Privacy Pass	Closed	Server	Y	N	N	N	N	Single sign-on solution for websites with erotic content
Policy Manager	Open	Client	N	N	N	N	Y	Allows organisations to automatically control the distribution, confidentiality, and retention of e-mail and attachments
PRIMA DataManager / IJournal	Open	Client	N	N	(Y)	Y	N	Manages history of personal data that a user has transmitted to service providers
Privacy Companion	Open	Client	N	N	(Y)	N	N	Allows automated cookie decisions based on the site's P3P policy
Privacy Manager	Open	Server	N	N	(Y)	N	N	Helps organisations to build privacy policies and practices into their e-business applications and infrastructure (supports P3P)
Privacy Network	Open	?	N	N	(Y)	(Y)	N	Privacy tools for B2B with support of P3P and APPEL
Private Credentials	Open	C/S	(Y)	N	N	Y	N	Pseudonyms that contain no information that can be linked to the identity of their holder
Private Payments	Open	Server	Y	N	N	N	N	Using a random, unique number for each online payment
Roboform	Open	Client	Y	Y	N	(Y)	N	Password manager, form filler, password generator
SafeZone	Open	Server	N	N	N	(Y)	Y	Customers buy and receive products without revealing their names, addresses, or credit card information to the merchant
SAML	Open	C/S	(Y)	N	N	(Y)	N	Standard which defines user authentication, entitlements and attribute information in XML documents
Secretmaker	Open	Client	N	N	N	(Y)	N	Anonymiser that exchanges specific information of the computer with "phantoms" before it is released to the Internet
SelectAccess	Open	C/S	Y	N	N	N	(Y)	Web access control and authorisation management product for organisations
SiteMinder	Open	Server	Y	N	N	(Y)	(Y)	Authentication and authorization management and providing single sign-on for organisations
Shibboleth	Open	Client	Y	(Y)	(Y)	Y	N	Supports inter-institutional sharing and controlled access to web available services with privacy info monitor for the user
Spamex	Open	Client	N	N	N	Y	(Y)	Hides the user's e-mail address and uses disposable e-mail addresses
Speednames	Open	Server	N	N	N	Y	(Y)	Represents providers for domain name registration for building an Internet identity (cf. [Dyson 2002a])
Sun One / Network Identity	Open	Server	Y	N	N	(Y)	N	Account management and organisation identity management
The Sims Online	Closed	Server	N	N	N	Y	Y	Game / Virtual Residence simulation with chat function
There	Closed	Server	N	N	N	Y	Y	Game / Virtual Residence simulation with chat function
TrueSign	Open	C/S	(Y)	N	N	N	N	Secure verification of digitally signed electronic documents
TrustBridge	Open	C/S	Y	N	N	(Y)	N	Enable organisations to share user identities across business boundaries
Trusted Transaction Roaming Project	Open	C/S	(Y)	N	N	N	N	Aims to leverage the existing mobile telephony infrastructure to provide evidence of identity and payment capabilities

Results of IMS Comparison

State-of-the-Art of IMS:

- Main goal: usefulness
- Deficiencies concerning privacy and security functionality, and if realised: usability problems
- Digital evidence is not addressed (lack of liability / no non-repudiation), no support for law enforcement
- Identity theft is not prevented
- Little functionality, limited purposes
- No general solutions, no standards

- Trustworthy computer systems and infrastructure are still missing ⇒ no trustworthy and secure IMS possible

- Business models:
  Service and software mostly free for users

Today's IMS: Playground for users & service providers

Recent Survey Among Experts

IMS Survey

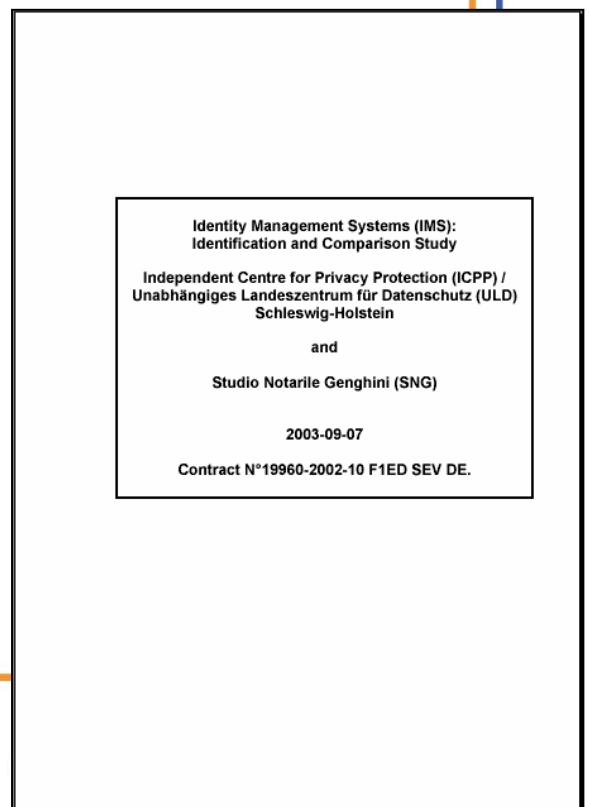
- **Survey: questionnaire sent to experts**
  - E-mail to 238 experts from Identity Management Community
  - Questionnaire filled in by 89 experts (37 %)
  - Topics: State-of-the-art & Vision

- **Background of experts who filled in questionnaire:**
  - Institution: research (33 %), privacy agencies (18 %), manufacturers of IMS (12 %)
  - Position: research (52 %), management (15 %), lawyer (8 %)
  - Culture: Europe (76 %, thereof 45 % Germany), Canada/USA (18 %, thereof 79 % USA), Japan (3 %)

- **General results of IMS survey:**
  - Most experts are dealing with IMS ca 4 years.
  - Only few experts are using an IMS by themselves.
  - State-of-the-art: Microsoft Passport

The Market of Identity Management Systems

Source:
Identity Management Systems (IMS): Identification and Comparison Study, September 2003


Identity Management Systems (IMS):
Identification and Comparison Study

Independent Centre for Privacy Protection (ICPP) /
Unabhängiges Landeszentrum für Datenschutz (ULD)
Schleswig-Holstein

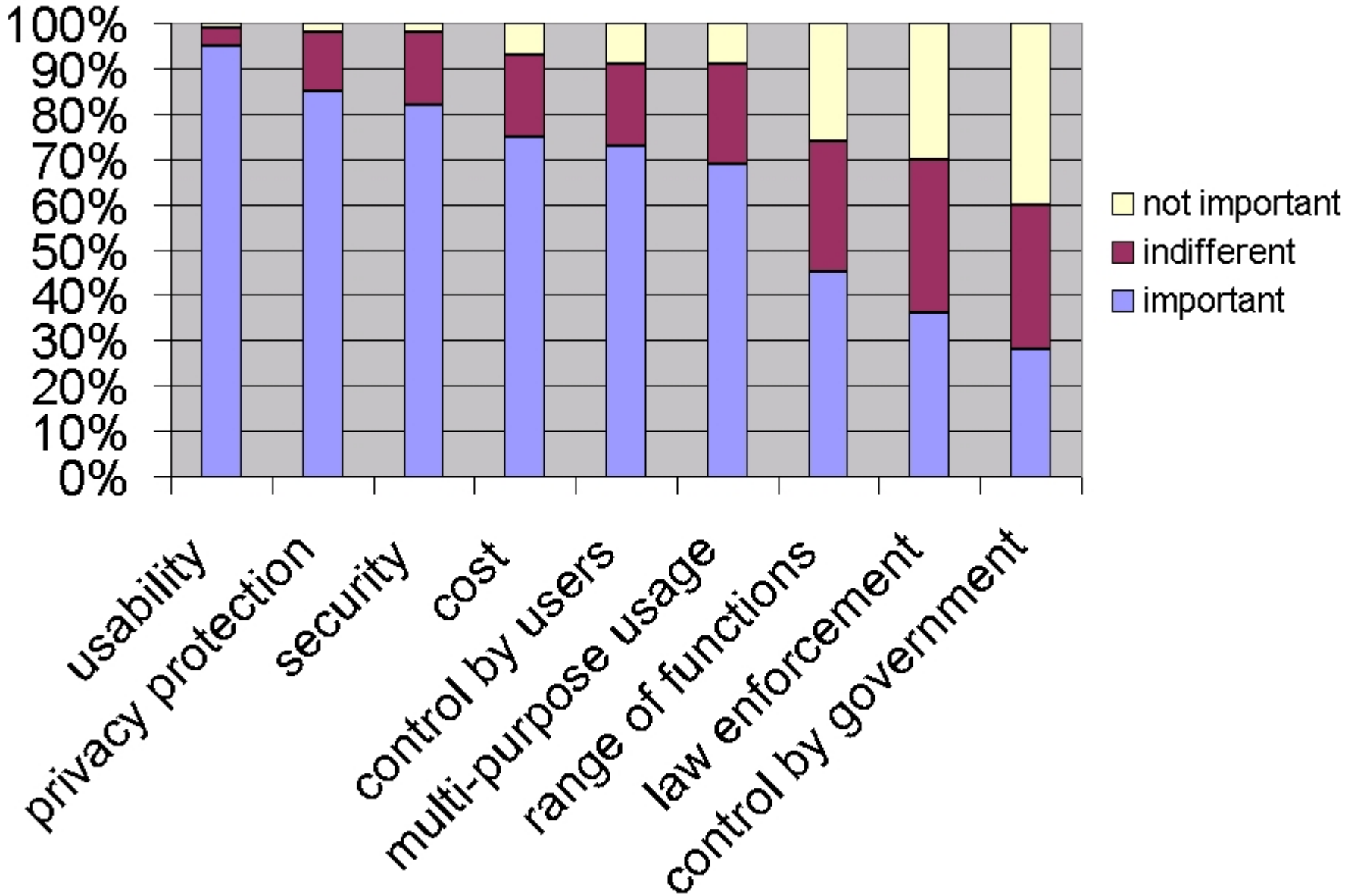
and

Studio Notarile Genghini (SNG)

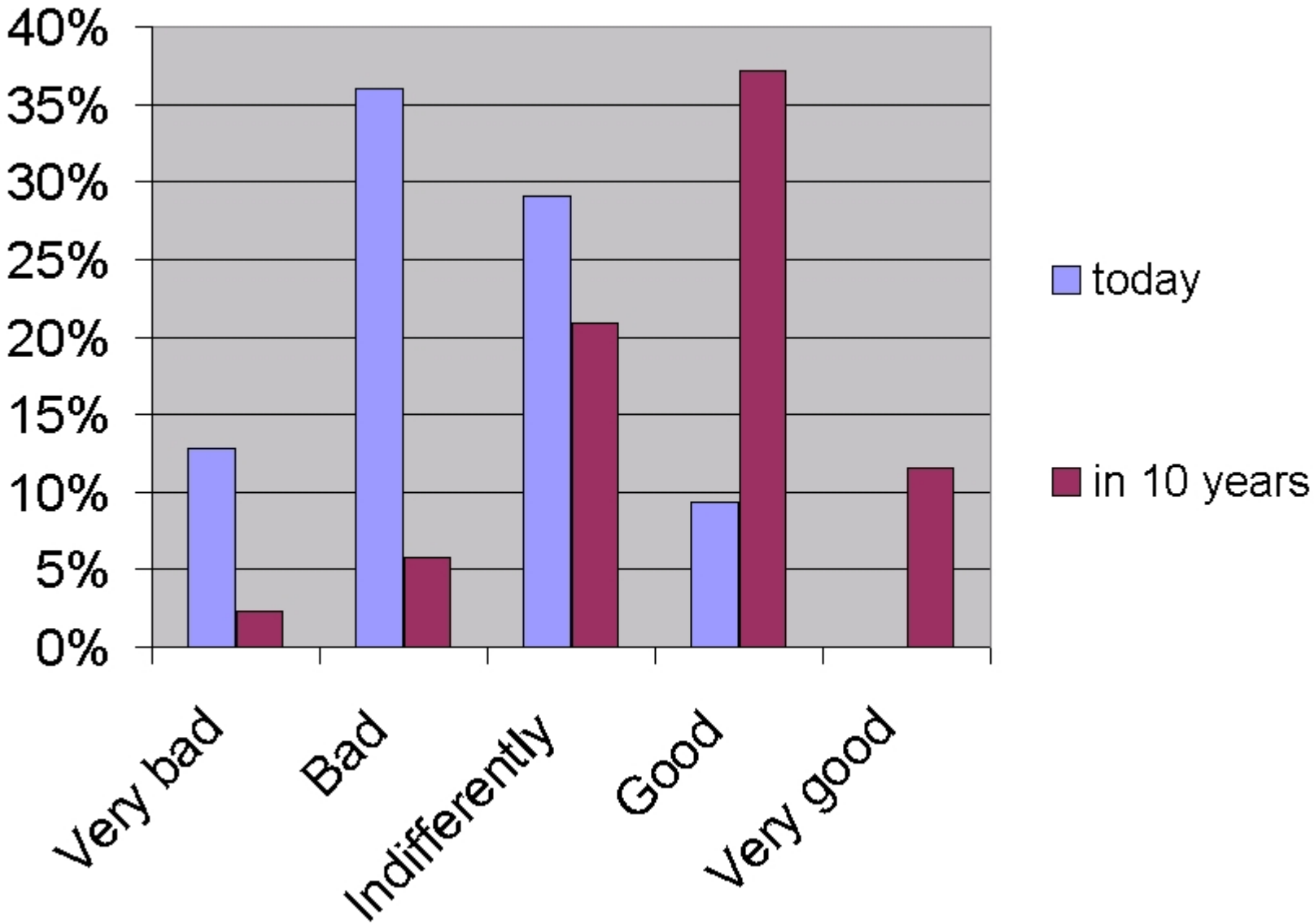
2003-09-07

Contract N°19960-2002-10 F1ED SEV DE.

Important Aspects of an IMS



Marketability Today vs. In 10 Years



Results of IMS Survey II

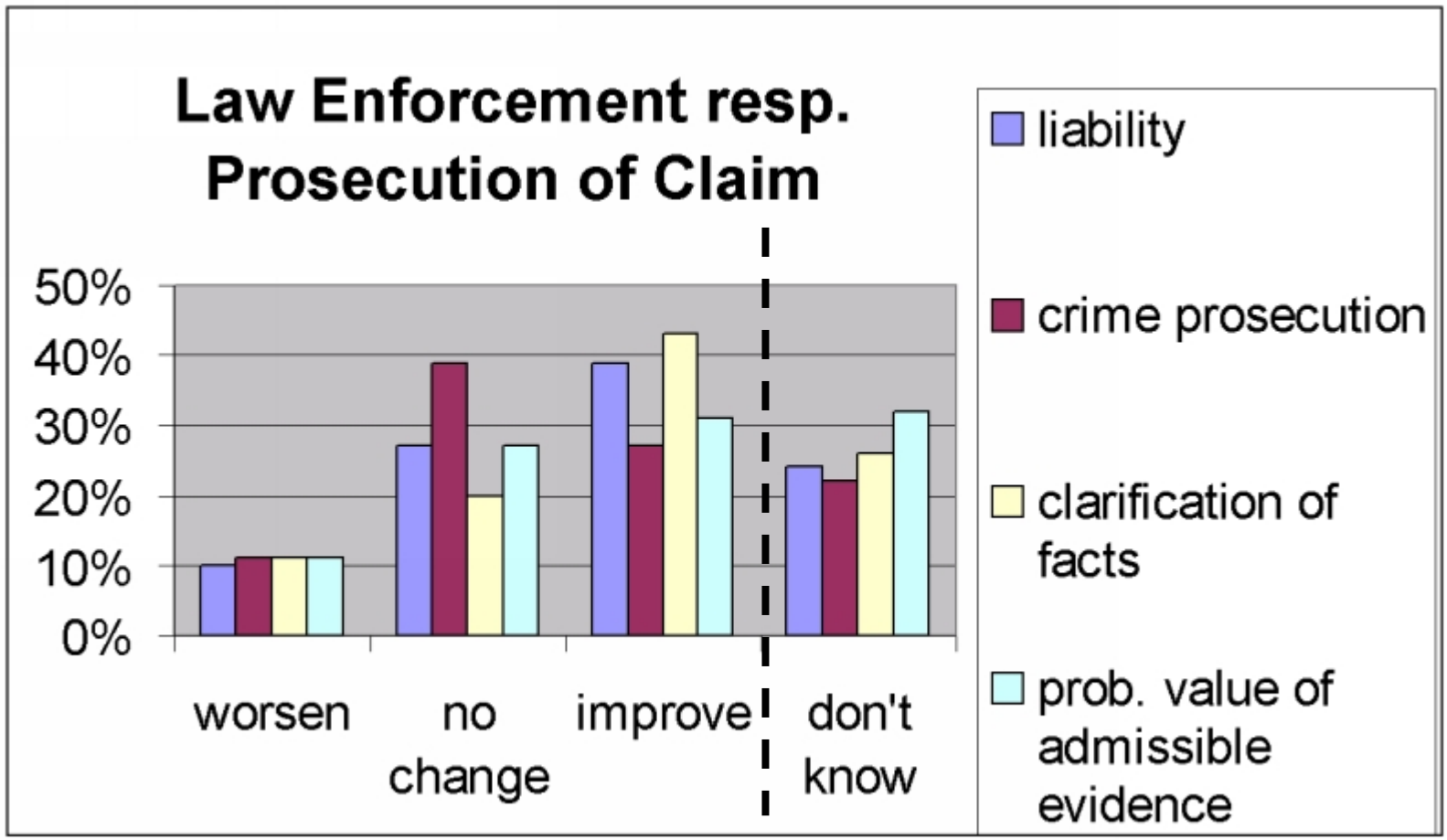
- "Society-wide implementation of a multi-purpose IMS for every day use": in **ca 11.5 years** in average

- Potential main bottlenecks:
  - **Bad usability (60 %)**
  - **Insufficient technological development (25 %)**
  - **Insufficient security (9 %)**

- State tasks:
  - **Standardisation**
  - **Deployment of infrastructure**
  - **Functionality for digital evidence**
  - **Incentives for development and use**

Influence of IMS on Liability ...

Will an IMS improve or worsen the following aspects of law enforcement and prosecution of claim?



Thank you for your attention!

Questions?