



# ★ IFIP - FIDIS ★ Summer School

---

★ Privacy-Friendly Identity Management in  
★ eGovernment

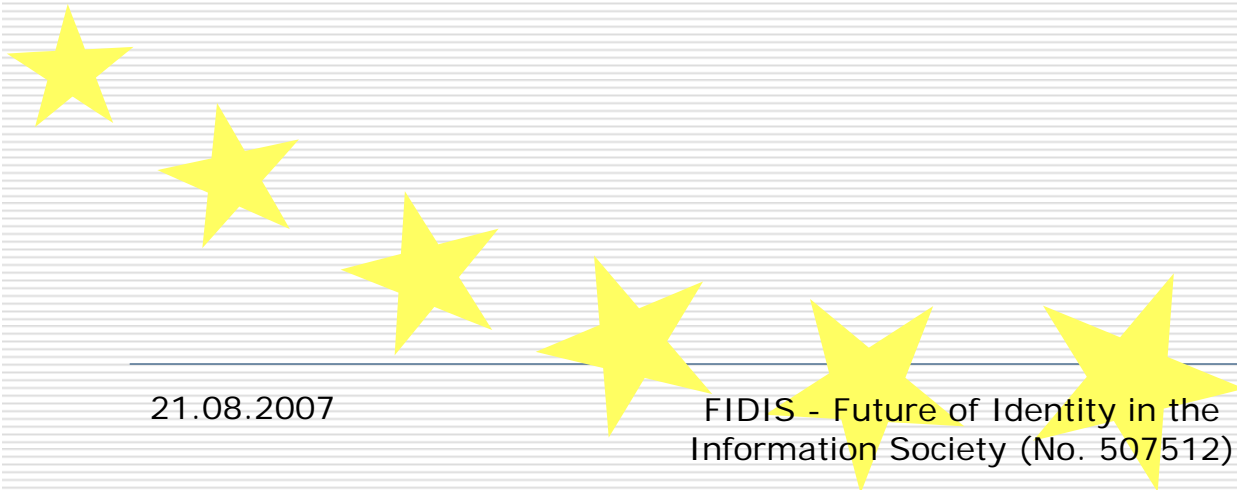
Xavier Huysmans  
K.U.Leuven ICRI



# Objective of this talk

---

- Explaining
  - legal drivers for
    - Privacy-Friendly
      - Identity Management
        - in eGovernment

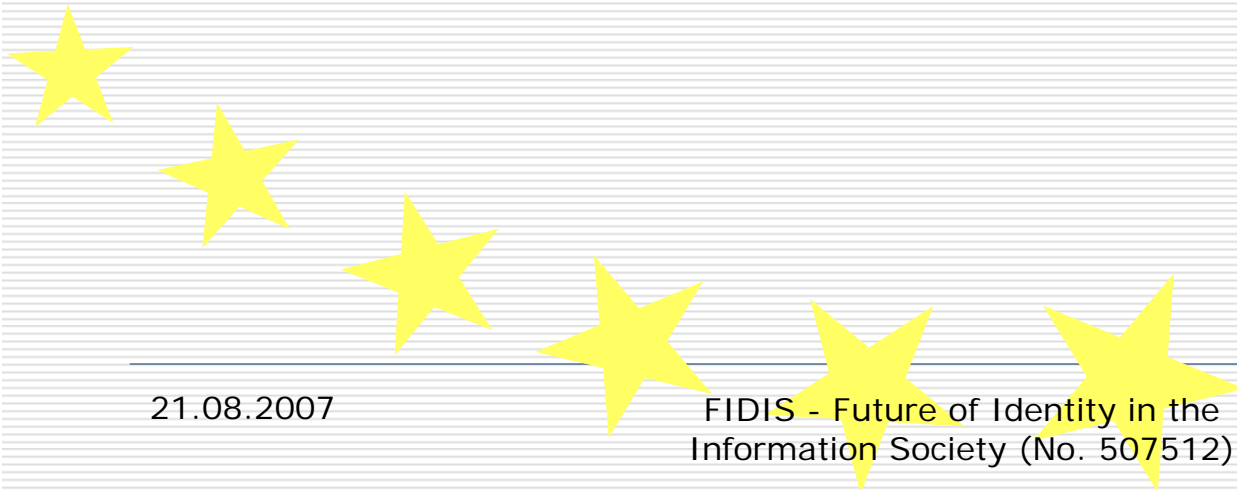




# Agenda

---

- What is eGovernment?
- What is organizational Identity Management?
- Limitation of current privacy research
- An alternative

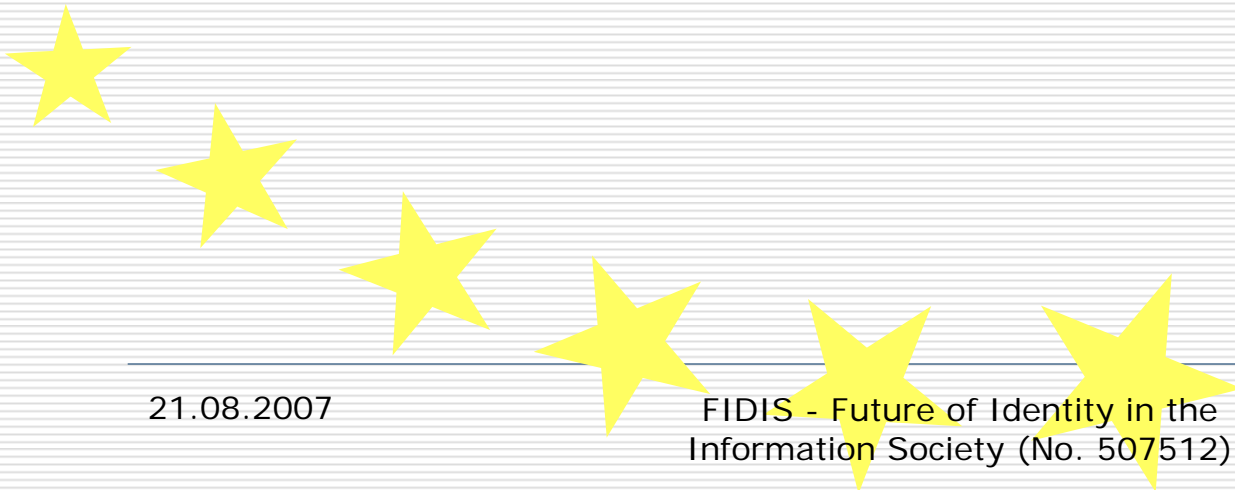


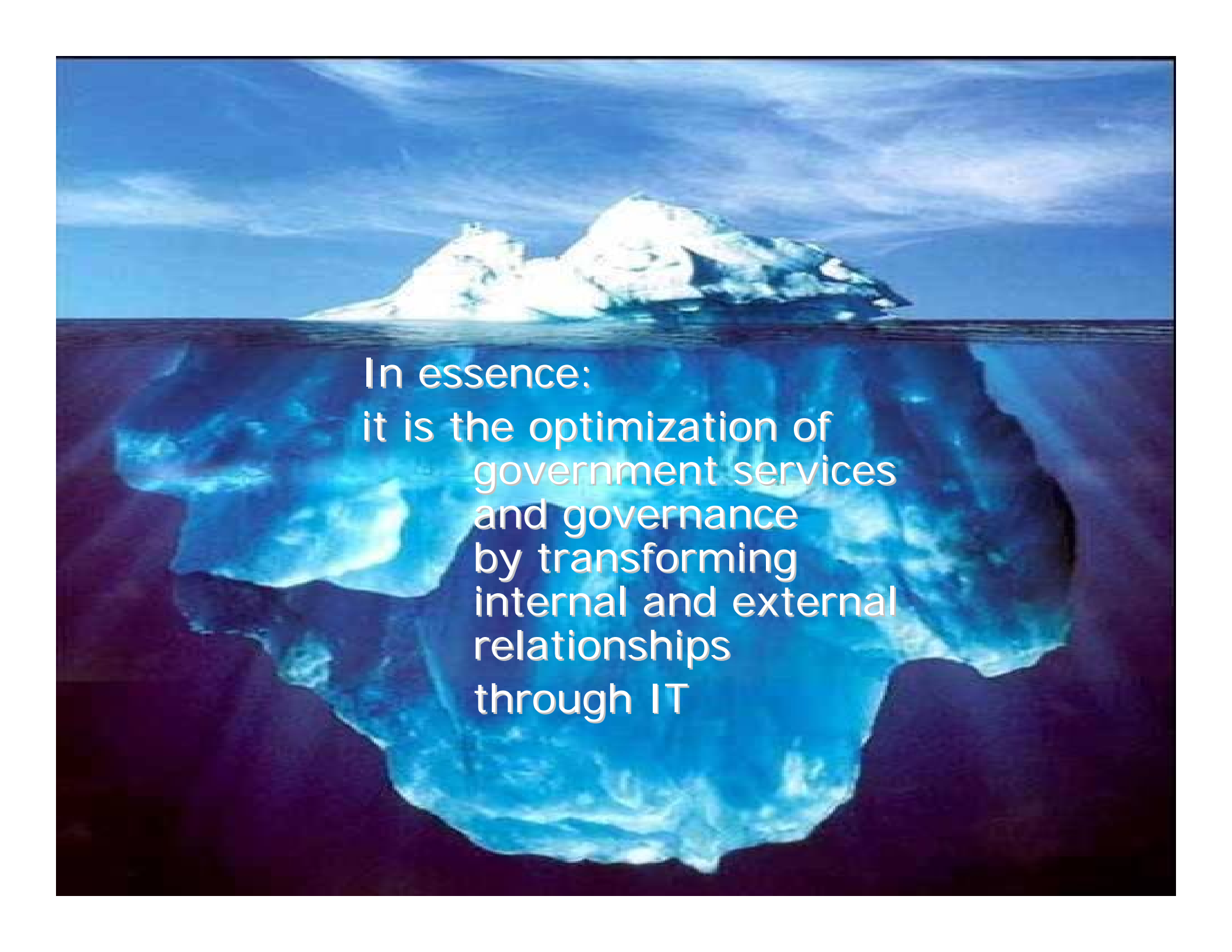


# Agenda

---

- What is eGovernment?



An iceberg floating in the ocean. The tip of the iceberg is visible above the water, while the much larger, submerged part is below the surface. The sky is blue with light clouds, and the water is a deep blue. The text is overlaid on the submerged part of the iceberg.

In essence:  
it is the optimization of  
government services  
and governance  
by transforming  
internal and external  
relationships  
through IT

In other words: not this



# But this:

cooperation with respect for each others  
competence: one virtual government

integration of back-offices

client centric reengineering  
of service delivery within  
and across government  
levels

semantic, functional,  
technical interoperability,  
common **identifiers**

**good information management**

think global, act local

measures to prevent  
a digital divide

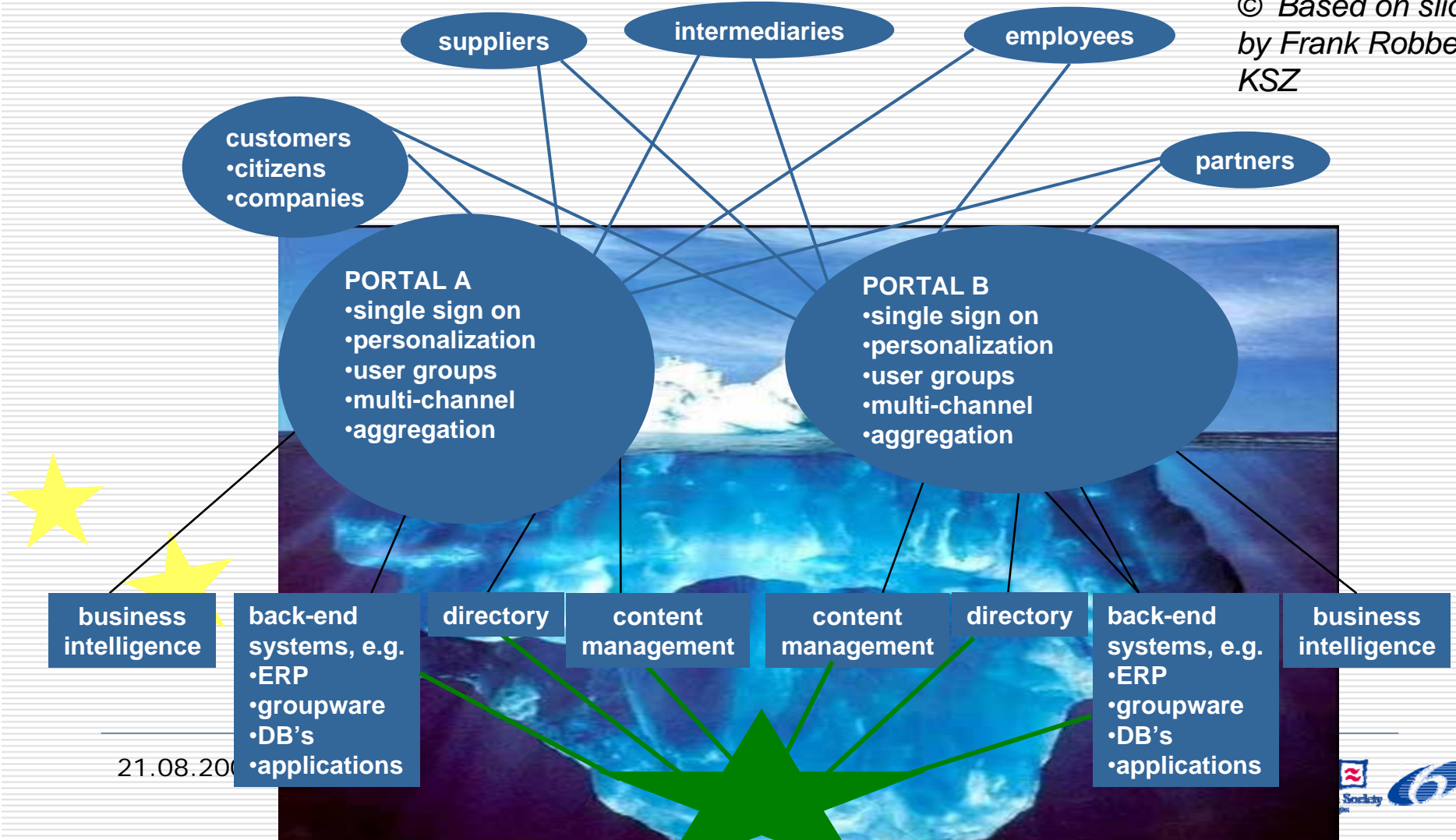
respect for the law,  
especially **data protection**  
**privacy** and IT regulation

security framework, **access control**  
**authentication mechanisms**



# One virtual government

© Based on slide by Frank Robben, KSZ

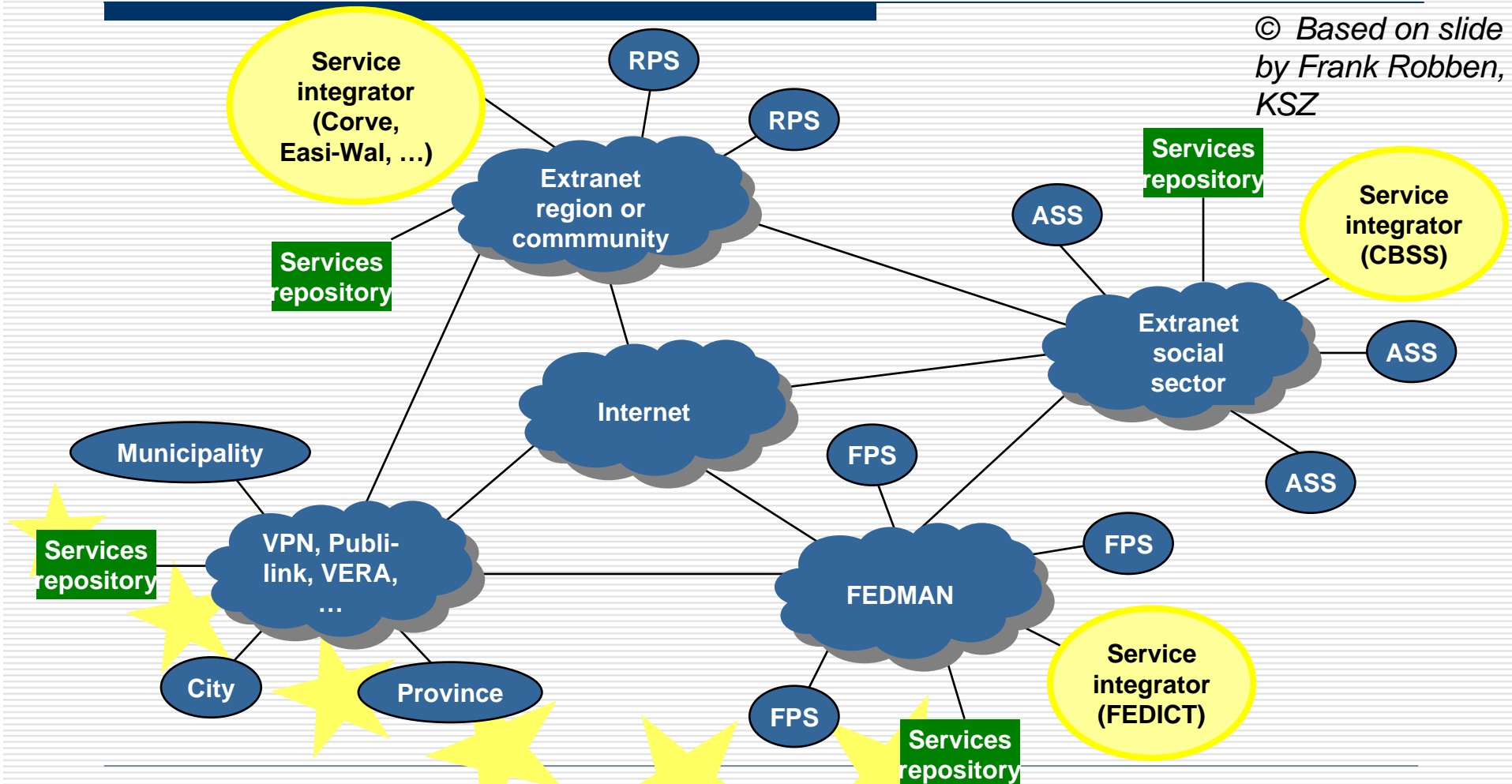






# Integration of back-offices

© Based on slide by Frank Robben, KSZ



21.08.2007

FIDIS - Future of Identity in the Information Society (No. 507512)

9

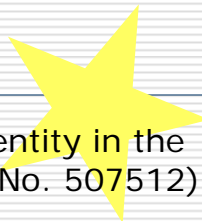
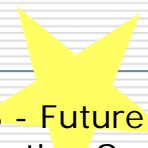




# Agenda

---

- What is eGovernment?
- What is organizational Identity Management?
- Limitations of current privacy research
- Alternatives

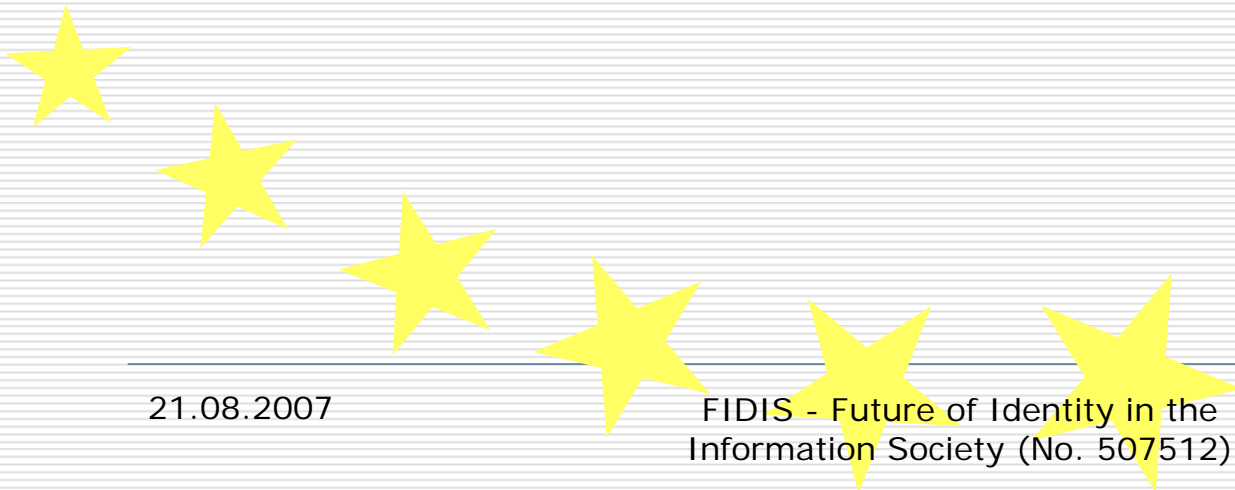




# Agenda

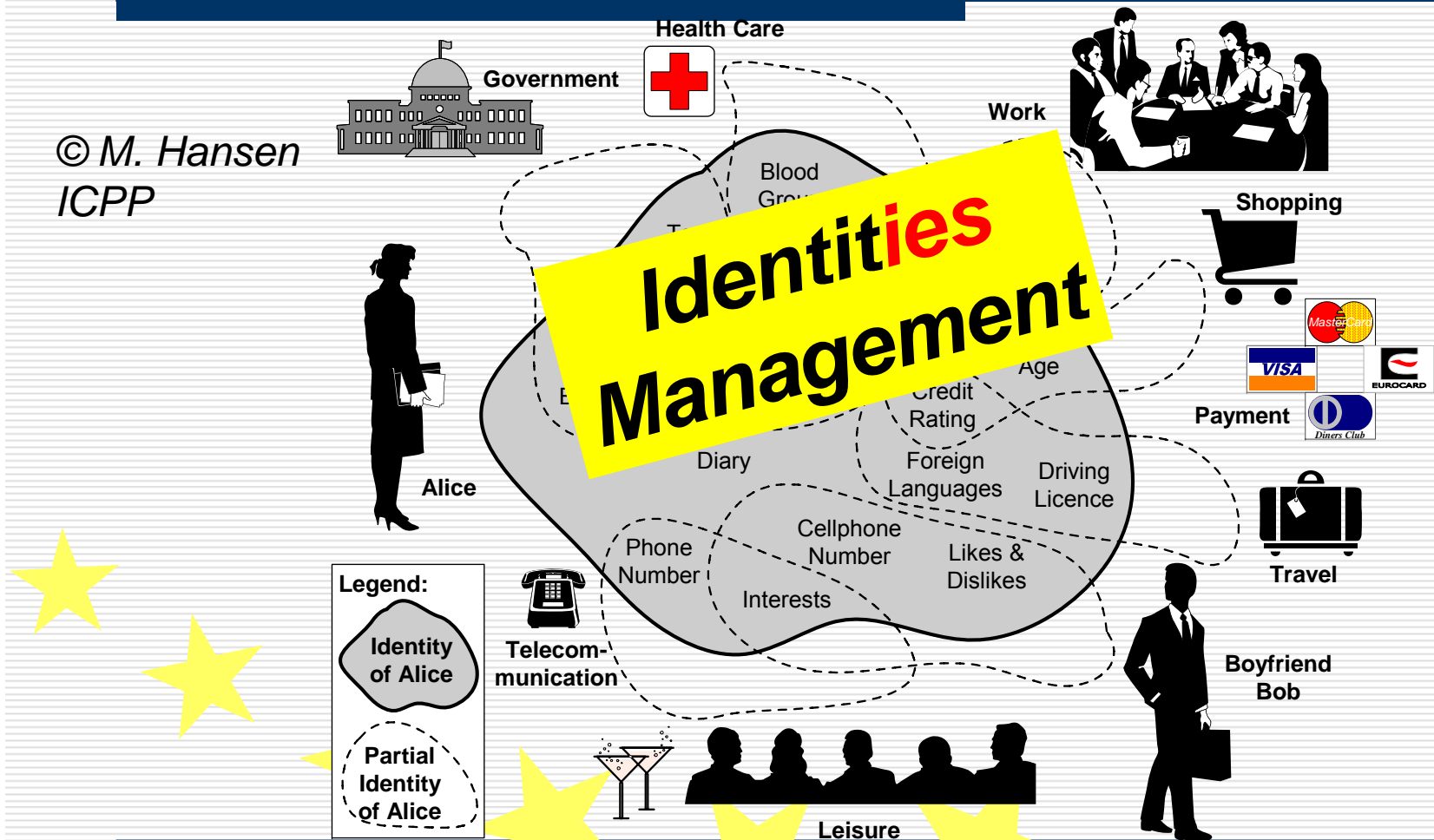
---

- What is eGovernment?
- What is organizational Identity Management?



# Organizational IDM

© M. Hansen  
ICPP



21.08.2007

FIDIS - Future of Identity in the  
Information Society (No. 507512)




23



# Organizational IDM

- IDM is:
  - the definition, designation and administration of identity attributes
  - as well as the administration of the choice of the partial identity to be (re-) used in a specific context,
  - to manage the access to and the usage of online applications, services and resources.
- It includes:
  - the management of identity attributes
  - by:
    - their owners (user-side IDM) and/or
    - those parties with whom the owners interact (services-side IDM).

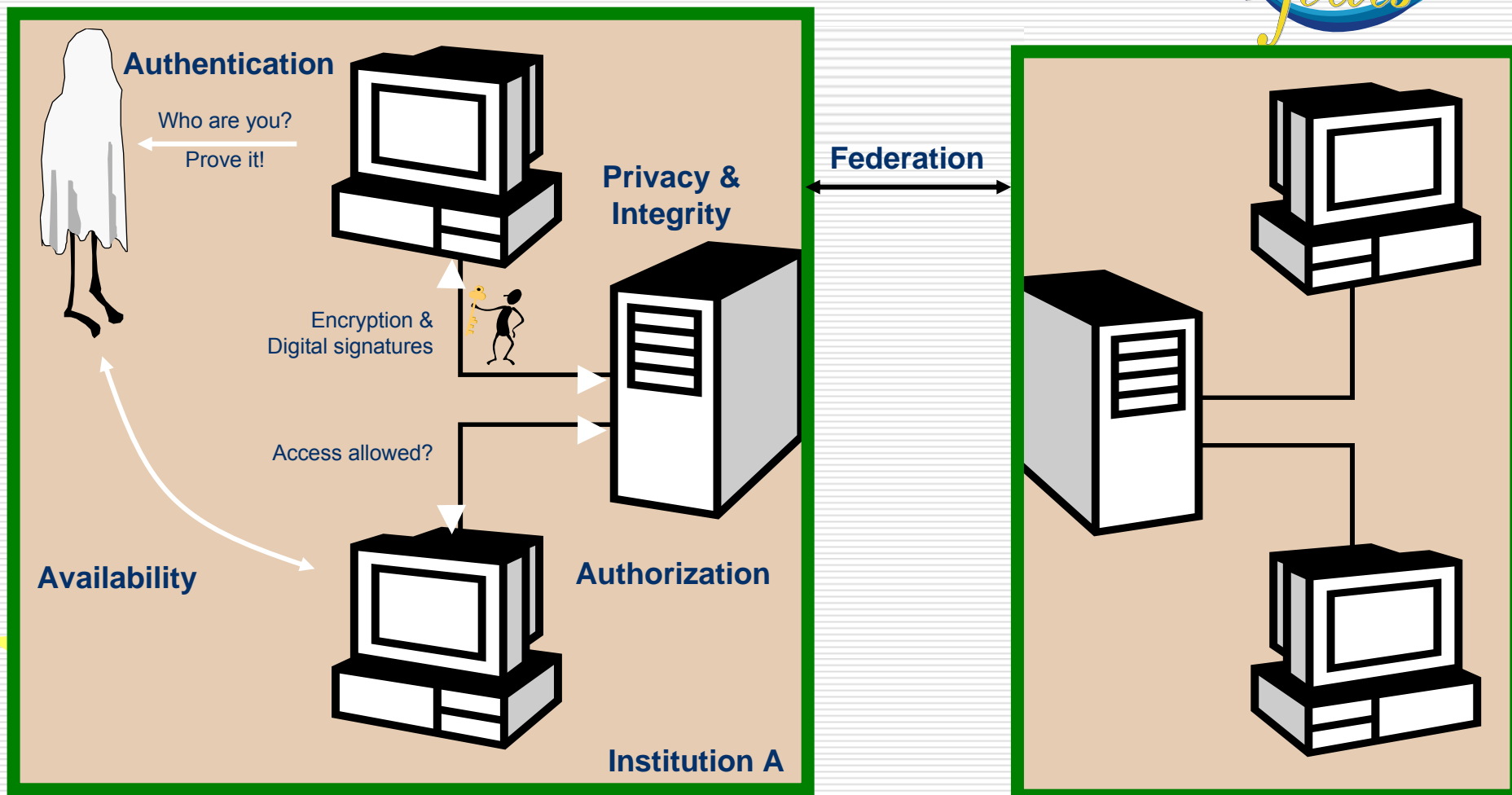
# Organizational IDM

<b>Type 1</b>		Account Management: <i>assigned identity</i>	by organisation
<b>Type 2</b>		Profiling: <i>derived identity</i>	by organisation
<b>Type 3</b>		Management of <i>own identities:</i> <i>chosen identity</i>	<i>by user himself</i> supported by service providers

© FIDIS D2.3, D3.1

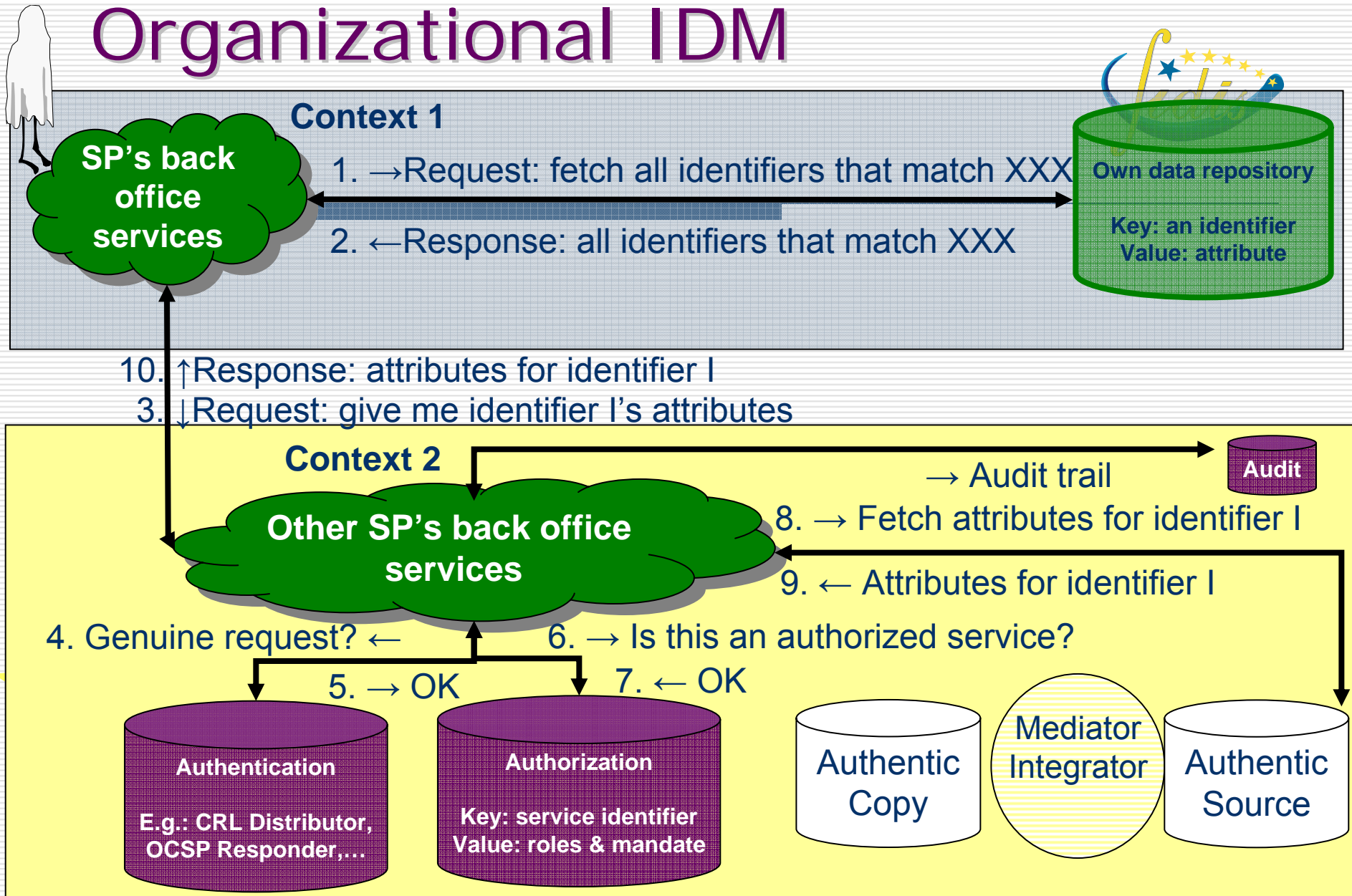
There are hybrid systems.

# Organizational IDM



© Based on slide from Witheridge & Vullings, MAMS project

# Organizational IDM

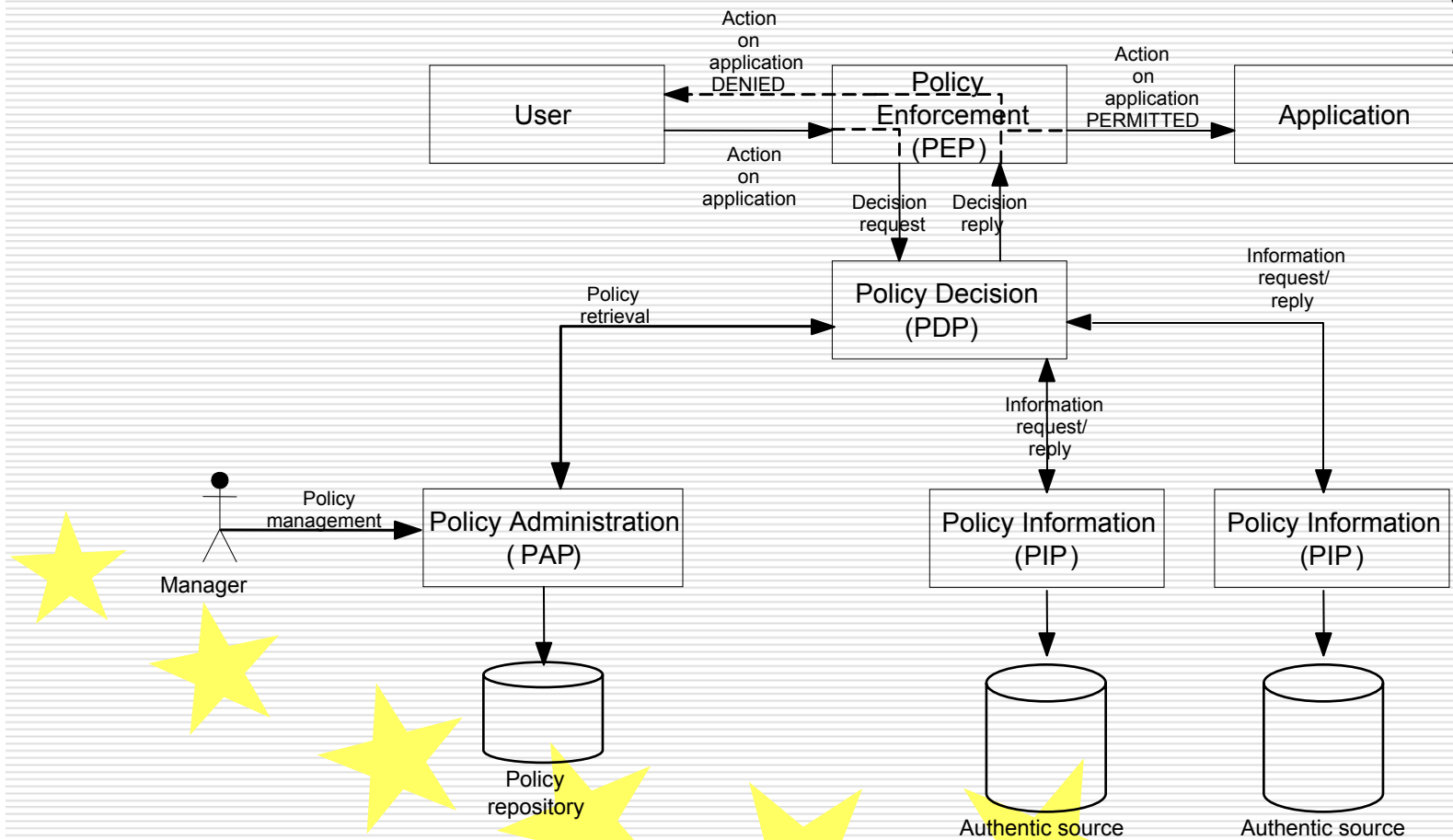


21.08.2007



# Organizational IDM

© Figure by Frank Robben, KSZ

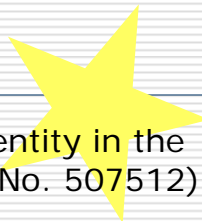




# Agenda

---

- What is eGovernment?
- What is organizational Identity Management?
- Limitations of current privacy research
- Alternatives

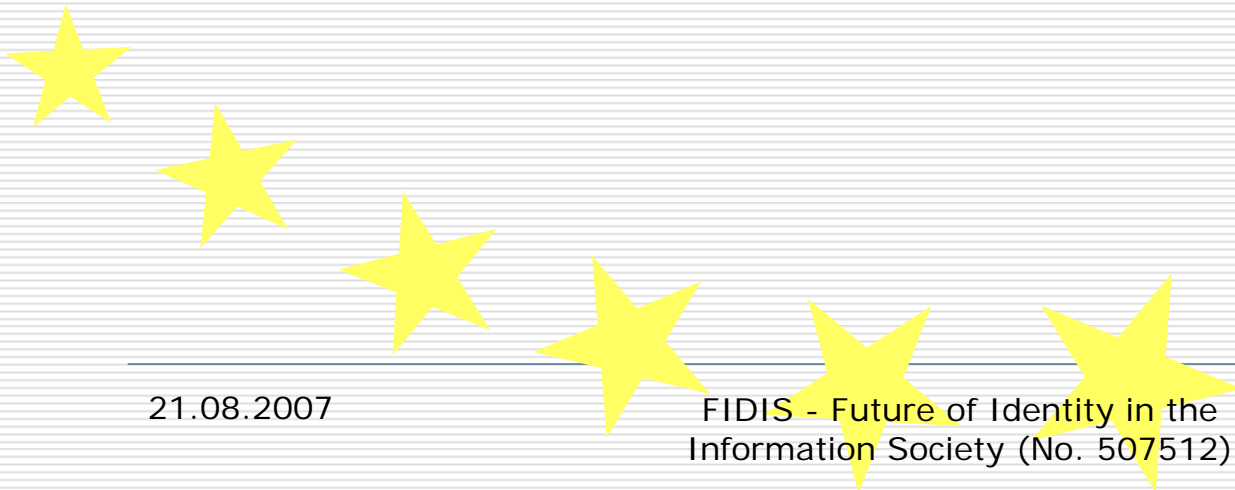




# Agenda

---

- What is eGovernment?
- What is organizational Identity Management?
- Limitations of current privacy research**



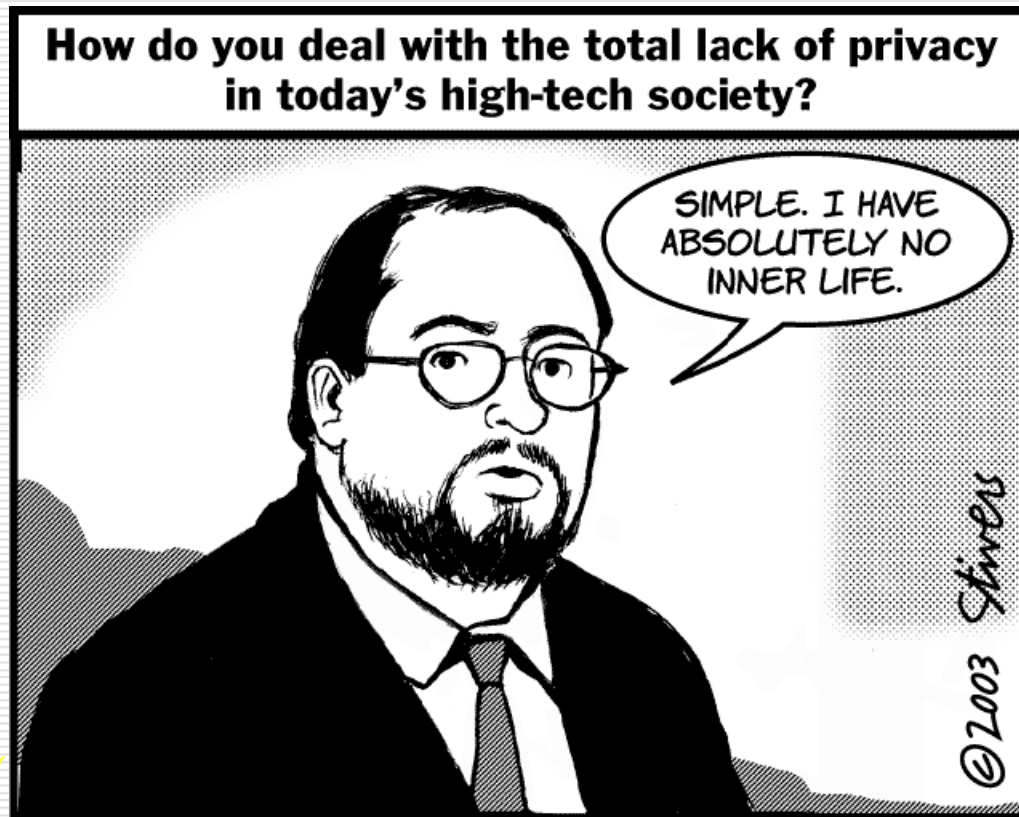
# Privacy and IDM

## □ Drivers for **privacy by design**

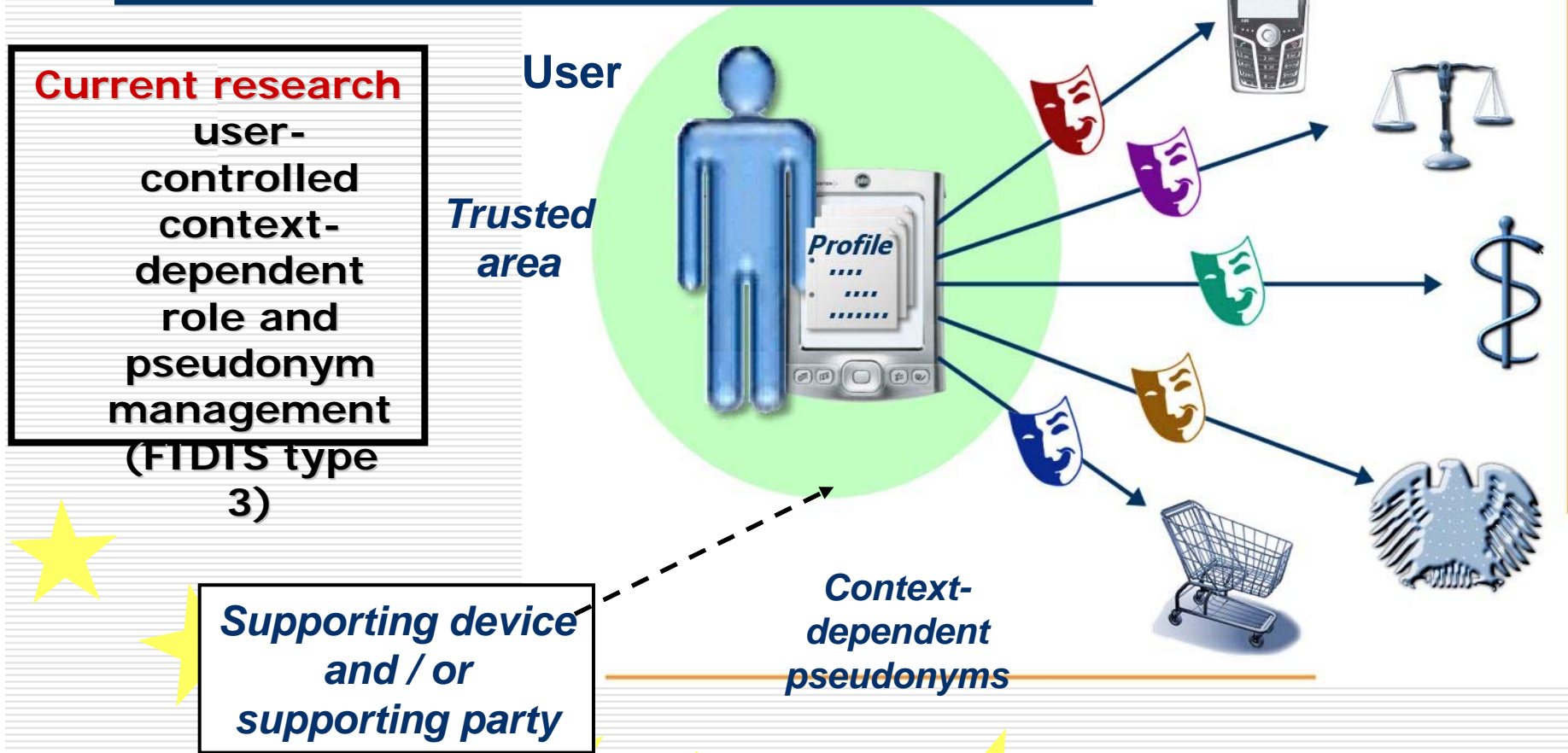
- “Natural people should be helped to protect themselves from **undesired identification and profiling**, and, generally, to enforce their privacy and data protection rights”.
- “When identification is always required, it is possible that even though a number of data interconnections are not authorized, or illegal, they will take place anyway” → **risk**
- “Trust relationships have to do with much more than identification, and identification is certainly not always necessary” → **data minimization**
- “The access to services is not granted on the basis of identification, but on the basis of a capacity or competence” → **authorization**

# Privacy and IDM

- Drivers for **privacy by design**



# Privacy and IDM



© Marit Hansen, ICPP

FIDIS - Future of Identity in the Information Society (No. 507512)



# Privacy and IDM

- An application is designed in a (perfectly) **privacy-enhancing (PE) identity management** enabling way if,
  - in addition of being compliant with data protection regulation,
  - neither the pattern of sending/receiving messages
  - nor the attributes given to entities (i.e., natural and legal persons, computers)
  - imply more linkability
  - than is strictly necessary to achieve the purposes of the application.

# Privacy and IDM

## □ But... is PE IDM a requirement?

- Privacy is a relative human right – other important rights limit the right to privacy, e.g., the public interest (especially in eGovernment)
- Complying to data protection does not necessarily require anonymity, nor pseudonymity and certainly not user-centricity.
- We could theoretically cope with the liability and other risks by other measures, without privacy by design (e.g., insurances)
- Anonymous/pseudonymous online transactions require a complex and thus costly, well functioning privacy enhanced identity management infrastructure
  - < cost-reduction, < effectiveness, < user experience etc.
- Is PE-IDM an obligation for the data controller?

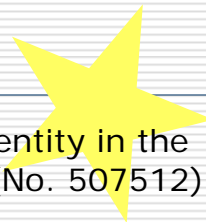




# Agenda

---

- What is eGovernment?
- What is organizational Identity Management?
- Limitations of current privacy research
- Alternatives

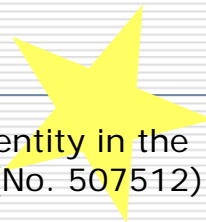




# Agenda

---

- What is eGovernment?
- What is organizational Identity Management?
- Limitations of current privacy research
- Alternatives**





# Privacy and IDM in eGov

- In eGovernment, the answer seems to be "no"
  - no obligation for PE IDM as the default position for all government data exchange in eGovernment
- Why?
  - why imposing more limitations than strictly necessary? (> privacy = < efficiency?)
  - only user-control where really necessary
  - only different identifiers where really necessary
- Result
  - **no privacy by design** in eGovernment?
  - Is there an alternative to PE IDM?



# Privacy and IDM in eGov

- A privacy friendly IDM system
  - addresses the interest of the individual in controlling, or at least significantly influencing the processing of data about him/her-self and
  - complies with the applicable privacy and data protection regulation
  
- It is thus:
  - not necessarily user-centric
  - not necessarily focused on pseudonym management



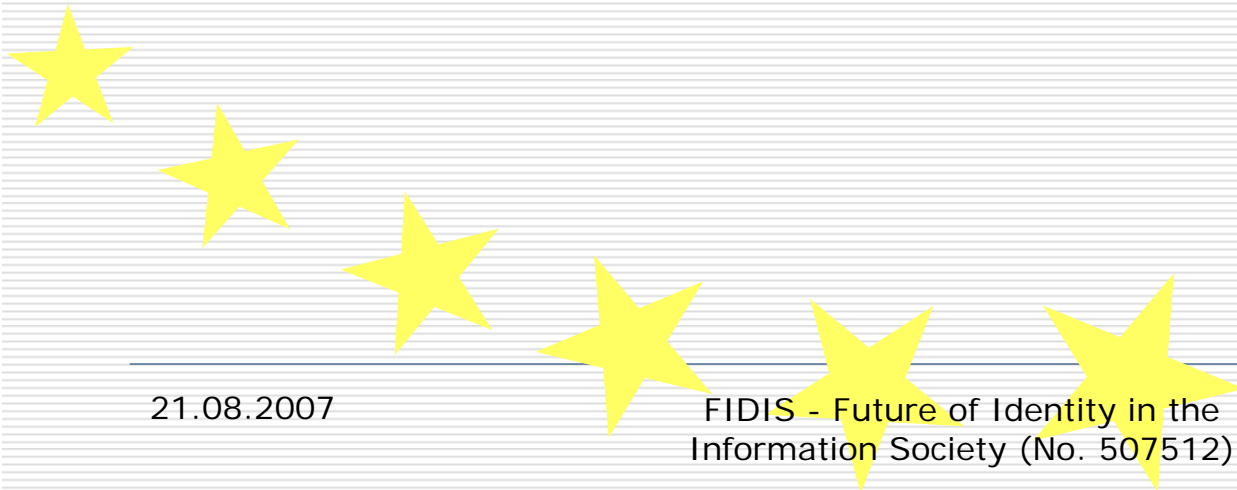
# Privacy and IDM in eGov

- Example where it can be **non-user-centric**:
  - The Belgian Crossroads Bank for Social Security:
    - **organizational IDM** (FIDIS type 1), used inter alia for account and resource provisioning, access control etc.
    - data is only accessible and exchangeable with thereto authorized entities, **upon submission of an authorization** by (a subcommittee of the Belgian privacy commission).



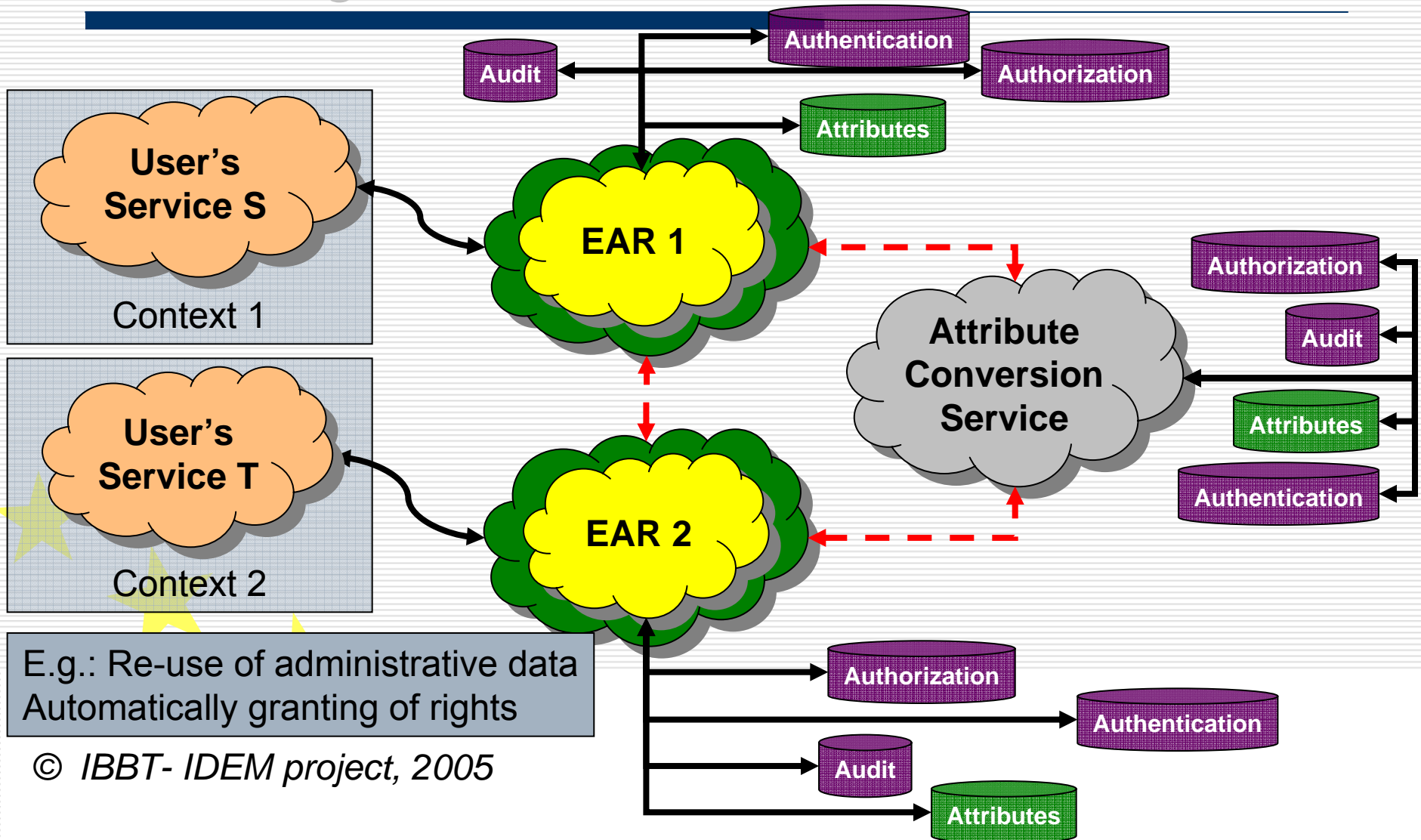
# Privacy and IDM in eGov

- **Pseudonym management** is, for example necessary in eGovernment:
  - because of the privacy sensitivity of certain data
  - because the data processing requires this type of investment
  - health data, judicial data





# Privacy and IDM in eGov



# Privacy and IDM in eGov

---

- However, in all other cases
  - pseudonym management is not necessary
  - the focus could, for example lay on:
    - technical enforcement of authorizations via **privacy policy enforcement** (e.g., extension of XACML)
    - **transparency**, e.g., via monitoring and pushing information about data processing back to the data subject



# Privacy and IDM in eGov

- Arguments for privacy by design developed in the paper:
  - **Objective risk liability** (art. 23 DP Directive) → controller is responsible when processing is not compatible with DP regulation)
  - Obligation to take all **appropriate measures** given state of the art and nature of data, cost data processing (art. 17 DP Directive)
  - **Privacy protection** is part of DP regulation (art. 1 DP Directive)

# Privacy and IDM in eGov

- Own considerations:
  - access control is already being implemented in eGovernment → **extra privacy layer/filtering is not disproportionate**
  - avoiding data processing in other contexts is a minimum-requirement → e.g. Belgian eID – one step to far (!)
  - transparency, monitoring → has to be done anyway, for security purposes → **not disproportionate to require data that relates to the processing of the personal data**, put that info in the logs and push it back to the data subject
    - static: what info about me in “authentic sources”
    - dynamic: what info is being consulted by whom for what purposes?

# BURNING QUESTIONS

TACK!

[e] [xavier.huysmans@law.kuleuven.be](mailto:xavier.huysmans@law.kuleuven.be)

[e] [jos.dumortier@law.kuleuven.be](mailto:jos.dumortier@law.kuleuven.be)

[t] +32 16 32 51 77

[f] +32 16 32 54 38





# Bibliography

- F. ROBBEN, 'Service oriented E-government in the Belgian social sector', available at: <http://www.law.kuleuven.be/icri/frobber/presentations/20050623.ppt>, 23 June 2005, last visited: 12 April 2006.
- F. ROBBEN, 'Naar een dienstgeoriënteerde architectuur en het gemeenschappelijk gebruik van basisdiensten', available at: <http://www.law.kuleuven.be/icri/frobber/presentations/20060704nl.ppt>, 4 July 2006, last visited: 22 October 2006.
- M. MACDONALD, 'Data Registries Comparison Report', available at: <http://www.itsregistry.org.uk/Comparison%20Report%20v3.doc>, March 2003, last visited: 20 August 2006.
- M. MEINTS, 'Fidis D2.3 and D3.1', available at: <http://www.strategiestm.com/conferences/esmart/05/proceedings.htm>, 21-23 September 2005, last visited: 23 September 2005.
- N. WITHERIDGE and E. VULLINGS, 'MAMS Roadshow', available at: [https://mams.melcoe.mq.edu.au/zope/mams/events/roadshow2005\\_Q1/20050309%20MAMS%20Roadshow.ppt/download](https://mams.melcoe.mq.edu.au/zope/mams/events/roadshow2005_Q1/20050309%20MAMS%20Roadshow.ppt/download), 9 March 2005, last visited: 15 May 2006.
- <https://projects.ibbt.be/idem> (mainly presentations by D. De Cock).