



★ Results of FIDIS- research concerning eIDs

Dr. Martin Meints,
ICPP Kiel, Schleswig Holstein, Germany



Project Overview

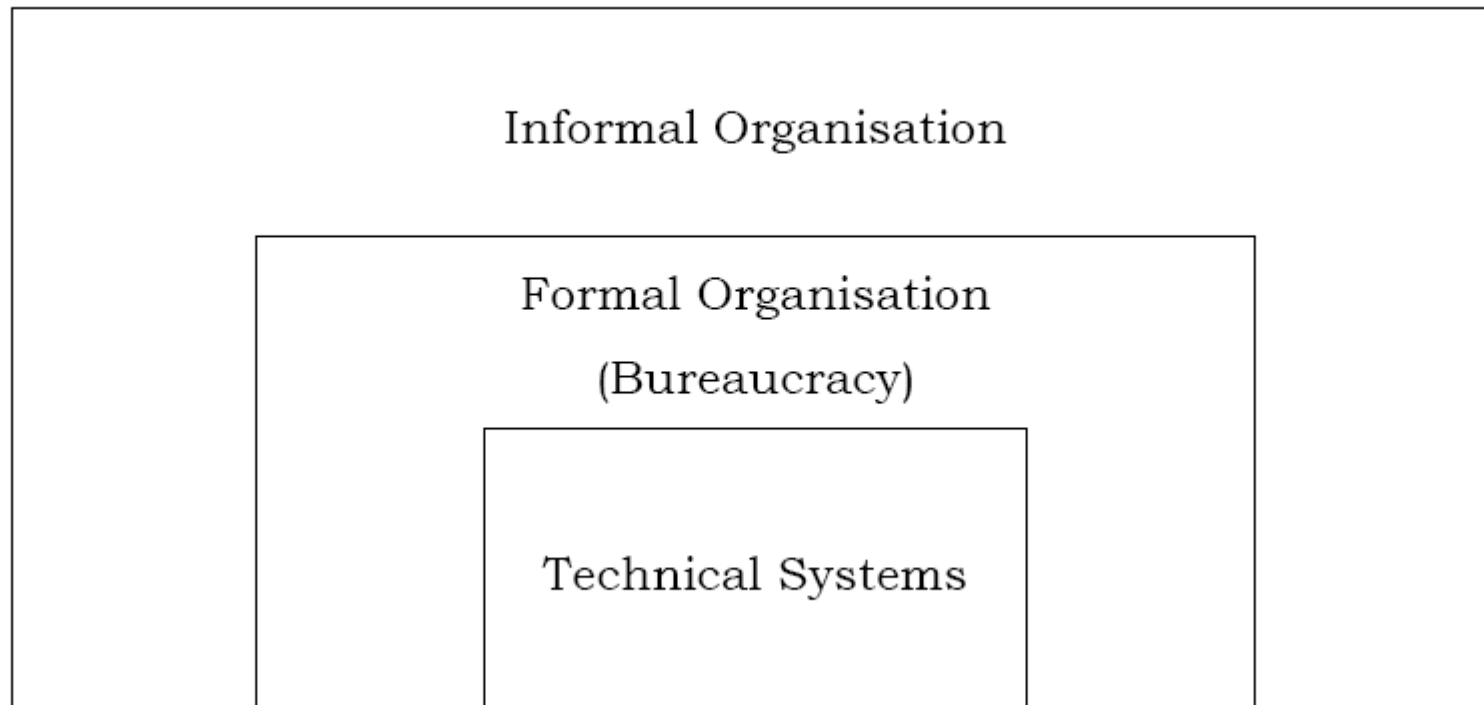
- Future of Identity in the Information Society (FIDIS), Network of Excellence (NoE)
- 24 participants from 12 European countries (including Switzerland)
- Objective: Interdisciplinary research covering social, technical and legal aspects; publication and dissemination of results
- URL: <http://www.fidis.net>



Introductory Statement

- The FIDIS partners well understand that
 - Identity Management in national and pan-European governmental applications is challenging due to
 - The size of identity management systems
 - Requirements of high levels of authentication (namely identification)
 - The need for offline availability in certain application scenarios
 - Differences in cultural and legal grounds

Interoperability Challenges



TFI model, Stamper et al. 2000



Recommendations

- General observation:
 - While technical interoperability can be achieved relatively easy, on the formal and informal layer much more effort is needed.
- Example:
 - Technical interoperability has been demonstrated
 - National concepts of governmental sectors, data handling strategies in these sectors, sector separation and linking strategies and enforcement of borders between governmental sectors differ widely.
 - Risk: interoperability opens "back doors" endangering data security and protection in neighbouring European countries
 - Possible countermeasures:
 - Data handling, security and privacy policies need to be negotiated, implemented / enforced and audited.
 - Harmonisation of governmental sectors in mid and long term



Recommendations

- Concerning Public Key Infrastructure (PKI)
 - PKI is well established in the context of authentication of devices and citizens, and electronic signing.
 - However, interoperable eID schemes should take care not to require verification of citizen's certificates in case of any authentication (risk of tracking at gateways, CAs etc.).



Recommendations

- Biometrics are increasingly used to strengthen the link between an ID document and the document holder.
- With respect to data protection and security the current ICAO standards are far from being state-of-the-art.
- A mid and long term strategy is needed how to:
 - Reduce or avoid additional information in biometric reference data
 - Protect reference data (e.g. applying measures for template protection, revocability or using encapsulated biometrics)
 - Ensure back up procedures in case biometric verification fails

Questions and Answers



Thank you for your attention!
Any questions?



Coordinator:
Prof. Kai Rannenberg
Chair for Mobile Commerce and
Multilateral Security
Goethe-University Frankfurt
60629 Frankfurt, Germany
<http://www.m-chair.net>
kai.rannenberg@m-chair.net

Contact w.r.t. research on eIDs
Dr. Martin Meints
Independent Centre for
Privacy Protection
Holstenstr. 98
24103 Kiel, Germany
ULD61@datenschutzzentrum.de

14.10.2008

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

8

